EUROPÄISCHE KOMMISSION

Brüssel, den 18.4.2011
KOM(2011) 225 endgültig

BERICHT DER KOMMISSION AN DEN RAT UND DAS EUROPÄISCHE PARLAMENT

Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG)

BERICHT DER KOMMISSION AN DEN RAT UND DAS EUROPÄISCHE PARLAMENT

Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG)

1. EINLEITUNG

Die Richtlinie über die Vorratsdatenspeicherung[1] (nachfolgend die „Richtlinie") sieht vor, dass die Mitgliedstaaten die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze (nachfolgend „Betreiber") dazu verpflichten, Verkehrs- und Standortdaten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten für einen Zeitraum zwischen sechs Monaten und zwei Jahren auf Vorrat zu speichern.

Dieser Bericht der Kommission bewertet im Einklang mit Artikel 14 der Richtlinie ihre Anwendung durch die Mitgliedstaaten sowie ihre Auswirkungen auf die Wirtschaftsbeteiligten und die Verbraucher, um festzustellen, ob ihre Bestimmungen, insbesondere in Bezug auf Datenkategorien und Speicherungsfristen, gegebenenfalls geändert werden müssen, wobei die Kommission die Weiterentwicklung der Technologie der elektronischen Kommunikation und die ihr zur Verfügung gestellten Statistiken berücksichtigt. Ferner untersucht dieser Bericht in Anbetracht der an der Vorratsdatenspeicherung geäußerten grundsätzlichen Kritik auch die Auswirkungen der Richtlinie auf die Grundrechte und prüft, ob die Bedenken im Zusammenhang mit der Verwendung anonymer SIM-Karten zu kriminellen Zwecken[2] Maßnahmen erfordern.

Die Bewertung hat insgesamt gezeigt, dass die Vorratsdatenspeicherung ein wertvolles Instrument für die Strafjustizsysteme und die Strafverfolgung in der EU ist. Der Beitrag der Richtlinie zur Harmonisierung der Vorratsdatenspeicherung war insbesondere im Hinblick auf die Zweckbindung und die Aufbewahrungsfristen sowie die Erstattung der den Betreibern entstehenden Kosten, die nicht in den Anwendungsbereich der Richtlinie fällt, begrenzt. Angesichts der Folgen und Risiken für den Binnenmarkt sowie die Achtung des Rechtes auf Privatsphäre und den Schutz personenbezogener Daten sollte die EU weiterhin durch gemeinsame Regeln gewährleisten, dass gleichbleibend hohe Anforderungen an die Speicherung, den Abruf und die Verwendung von Verkehrs- und Standortdaten gestellt werden. Im Hinblick auf diese Schlussfolgerungen beabsichtigt die Kommission, auf der Grundlage einer Folgenabschätzung Änderungen der Richtlinie vorzuschlagen.

---

1 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13.4.2006, S. 54–63.

2 Schlussfolgerungen des Rates zur Bekämpfung der kriminellen Zwecken dienenden Nutzung der elektronischen Kommunikation und ihrer Anonymität, 2908. Tagung des Rates Justiz und Inneres, Brüssel, 27./28. November 2008.

2. HINTERGRUND DIESER BEWERTUNG

Dieser Bewertungsbericht beruht auf umfangreichen Diskussionen mit den Mitgliedstaaten, Sachverständigen und Interessenvertretern sowie deren Stellungnahmen.

Im Mai 2009 veranstaltete die Kommission die Konferenz „Towards the Evaluation of the Data Retention Directive“, an der Vertreter von Datenschutzbehörden, der Privatwirtschaft, der Zivilgesellschaft und Wissenschaftler teilnahmen. Im September 2009 übersandte die Kommission Interessenvertretern aus diesen Gruppen einen Fragebogen, auf den sie etwa 70 Antworten erhielt.[3] Im Dezember 2010 veranstaltete die Kommission eine zweite Konferenz mit dem Titel „Taking on the Data Retention Directive“ und einem ähnlichen Teilnehmerkreis wie die erste Konferenz. Sie diente dem Austausch vorläufiger Beurteilungen der Richtlinie und der Erörterung künftiger Herausforderungen in diesem Bereich.

Die Kommission kam zwischen Oktober 2009 und März 2010 mit Vertretern der einzelnen Mitgliedstaaten und assoziierten EWR-Staaten zusammen, um Probleme im Zusammenhang mit der Anwendung der Richtlinie weiter zu erörtern. Die Mitgliedstaaten begannen später als erwartet mit der Umsetzung der Richtlinie, insbesondere in Bezug auf Internetdaten. Die verzögerte Umsetzung hatte zur Folge, dass nur neun Mitgliedstaaten in der Lage waren, der Kommission die in Artikel 10 der Richtlinie vorgesehene Statistik für 2008 oder 2009 vollständig zu übermitteln, wenngleich insgesamt 19 Mitgliedstaaten zumindest einige statistische Daten vorlegten (vgl. Abschnitt 4.7). Im Juli 2010 forderte die Kommission die Mitgliedstaaten auf, weitere quantitative und qualitative Angaben zur Notwendigkeit der Vorratsdatenspeicherung für die Strafverfolgung zu übermitteln. Daraufhin machten zehn Mitgliedstaaten[4] Angaben zu konkreten Fällen, für die sich derartige Daten als notwendig erwiesen hatten.

Dieser Bericht stützt sich auf die von der Sachverständigengruppe „Vorratsspeicherung von elektronischen Daten zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten“[5] seit ihrer Einsetzung im Jahr 2008 angenommenen Positionspapiere. Die Kommission hat ferner die Berichte der Artikel-29-Datenschutzgruppe[6], insbesondere ihren Bericht über die zweite Durchsetzungsmaßnahme, in dem sie einschätzt,

---

3 Die Kommission hat die Antworten auf der Website http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm veröffentlicht.

4 Belgien, Litauen, Niederlande, Polen, Slowenien, Tschechische Republik, Ungarn, Vereinigtes Königreich, Zypern. Schweden berichtete ebenfalls über mehrere Fälle bestimmter schwerer Straftaten, in denen historische Verkehrsdaten, die zur Verfügung standen, obwohl keine Pflicht zur Vorratsdatenspeicherung bestand, ausschlaggebend für Verurteilungen waren.

5 Diese Sachverständigengruppe wurde durch den Beschluss 2008/324 EG der Kommission (ABl. L 111 vom 23.4.2008, S. 11–14) eingesetzt. Die Kommission ist mit der Sachverständigengruppe regelmäßig zusammengekommen. Ihre Positionspapiere werden auf der Website http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm veröffentlicht.

6 Die gemäß Artikel 29 der Datenschutzrichtlinie (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) eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten.

wie die Mitgliedstaaten die Datenschutz- und -sicherheitsanforderungen der Richtlinie erfüllen[7], berücksichtigt.

3. VORRATSDATENSPEICHERUNG IN DER EUROPÄISCHEN UNION

3.1. Vorratsdatenspeicherung für die Strafjustiz und die Strafverfolgung

Diensteanbieter und Netzbetreiber (nachfolgend „Betreiber“) verarbeiten im Rahmen ihrer Tätigkeit personenbezogene Daten für die Übermittlung von Nachrichten, die Abrechnung von Gebühren, die Bezahlung von Zusammenschaltungen, Vermarktungszwecke und bestimmte Dienste mit Zusatznutzen. Verarbeitet werden Daten zur Quelle, zum Adressaten, zu Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung sowie zu den Endeinrichtungen der Benutzer und beim Mobilfunk auch zum Standort der Geräte. Nach der Richtlinie 2002/58/EG über den Schutz der Privatsphäre in der elektronischen Kommunikation (nachfolgend „Datenschutzrichtlinie für elektronische Kommunikation“)[8] sind derartige Verkehrsdaten grundsätzlich zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden, außer wenn und nur solange sie für die Gebührenabrechnung benötigt werden oder der Teilnehmer oder Nutzer zuvor eingewilligt hat. Standortdaten dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der betreffende Nutzer eingewilligt hat.

Vor dem Inkrafttreten der Richtlinie verlangten die einzelstaatlichen Behörden unter bestimmten Bedingungen von den Betreibern Zugang zu diesen Daten, um beispielsweise Teilnehmer anhand einer IP-Adresse zu identifizieren, Kommunikationsaktivitäten zu analysieren oder den Standort eines Mobiltelefons zu bestimmen.

Auf EU-Ebene befasste sich die Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation erstmals mit der Vorratsspeicherung und Verwendung von Daten für die Strafverfolgung. Diese Richtlinie sah zum ersten Mal die Möglichkeit vor, dass Mitgliedstaaten gegebenenfalls Rechtsvorschriften zum Schutz der öffentlichen Sicherheit und Ordnung (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten

---

[7] Bericht 01/2010 über die zweite gemeinsame Durchsetzungsmaßnahme: Erfüllung der nach den innerstaatlichen Rechtsvorschriften über die Vorratsspeicherung von Verkehrsdaten aufgrund der Artikel 6 und 9 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der Richtlinie 2006/24/EG (über die Vorratsspeicherung von Daten und zur Änderung der Datenschutzrichtlinie für elektronische Kommunikation) bestehenden Pflichten durch die Telekommunikations-Diensteanbieter und die Internet-Diensteanbieter auf nationaler Ebene (WP 172) vom 13.7.2010, abrufbar unter http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm.

[8] 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) (ABl. L 201 vom 31.7.2002, S. 37–47).

die Sicherheit des Staates berühren), zur Landesverteidigung und zur Anwendung strafrechtlicher Bestimmungen erlassen[9].

Diese Vorschrift wurde in der Datenschutzrichtlinie für elektronische Kommunikation weiterentwickelt. Diese sieht vor, dass die Mitgliedstaaten vom Grundsatz der Vertraulichkeit der Kommunikation abweichende Rechtsvorschriften erlassen können, unter bestimmten Bedingungen auch solche, die die Vorratsspeicherung von sowie den Zugang zu und die Verwendung von Daten für die Strafverfolgung zulassen. Nach Artikel 15 Absatz 1 können die Mitgliedstaaten die Datenschutzrechte und -pflichten unter anderem durch Vorratsdatenspeicherung beschränken, sofern dies „für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen […] notwendig, angemessen und verhältnismäßig ist."

Die Rolle von auf Vorrat gespeicherten Daten in den Strafjustizsystemen und der Strafverfolgung wird in Abschnitt 5 weiter erörtert.

3.2. Ziel und Rechtsgrundlage der Richtlinie über die Vorratsdatenspeicherung

Die Richtlinie 97/66/EG und die Datenschutzrichtlinie für elektronische Kommunikation, die den Mitgliedstaaten den Erlass von Rechtsvorschriften zur Vorratsdatenspeicherung gestatten, führten dazu, dass Betreiber in manchen Mitgliedstaaten für die Vorratsdatenspeicherung Ausrüstungen kaufen und zum Abruf von Daten für Strafverfolgungsbehörden Personal einstellen mussten, während dies in anderen Mitgliedstaaten nicht erforderlich war. Dies hatte Wettbewerbsverzerrungen im Binnenmarkt zur Folge. Darüber hinaus führten Trends bei Geschäftsmodellen und Dienstangeboten wie Flatrate-Tarifen, vorausbezahlten und kostenlosen elektronischen Kommunikationsdiensten dazu, dass die Betreiber immer weniger Verkehrs- und Standortdaten für die Gebührenabrechnung speicherten. Damit standen auch immer weniger derartige Daten für die Strafjustiz und die Strafverfolgung zur Verfügung. Die 2004 in Madrid und 2005 in London verübten Terroranschläge machten die Diskussionen zur Lösung dieser Probleme auf EU-Ebene noch dringlicher.

Vor diesem Hintergrund verpflichtete die Richtlinie über die Vorratsdatenspeicherung Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze, Kommunikationsdaten „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden", auf Vorrat zu speichern, und versuchte, bestimmte damit im Zusammenhang stehende Aspekte EU-weit zu harmonisieren.

Die Richtlinie änderte Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation ab, indem sie ihn für nicht anwendbar auf gemäß der Richtlinie gespeicherte Daten erklärte.[10] Daher können die Mitgliedstaaten (wie in Erwägungsgrund 12 der Richtlinie

---

[9] Artikel 14 Absatz 1 der Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (ABl. L 24 vom 30.1.1998, S. 1).

[10] Artikel 11 der Richtlinie lautet: „In Artikel 15 der Richtlinie 2002/58/EG wird folgender Absatz eingefügt:„(1a) Absatz 1 gilt nicht für Daten, für die in der Richtlinie 2006/24/EG des Europäischen

dargelegt) auch weiterhin vom Grundsatz der Vertraulichkeit der Kommunikation abweichen. Die Richtlinie (über die Vorratsdatenspeicherung) regelt lediglich die Speicherung von Daten für den begrenzten Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten.

Dieses komplexe Rechtsverhältnis zwischen der Richtlinie und der Datenschutzrichtlinie für elektronische Kommunikation erschwert in Verbindung mit der Tatsache, dass der Begriff „schwere Straftat" in keiner der beiden Richtlinien definiert ist, eine Unterscheidung zwischen Maßnahmen der Mitgliedstaaten zur Umsetzung der sich aus der Richtlinie ergebenden Pflichten zur Vorratsdatenspeicherung einerseits und der in den Mitgliedstaaten gängigen und nach Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation zulässigen Vorratsdatenspeicherung andererseits[11]. Weitere Ausführungen dazu enthält Abschnitt 4.

Grundlage der Richtlinie ist Artikel 95 des Vertrags zur Gründung der Europäischen Gemeinschaft (ersetzt durch Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union), welcher die Errichtung und das Funktionieren des Binnenmarkts betrifft. Nach Erlass der Richtlinie wurde ihre Rechtsgrundlage vor dem Europäischen Gerichtshof mit der Begründung angefochten, ihr hauptsächlicher Zweck bestehe in der Ermittlung, Feststellung und Verfolgung schwerer Straftaten. Der Gerichtshof befand, dass die Richtlinie Tätigkeiten regele, die unabhängig von der Durchführung jeder eventuellen Maßnahme polizeilicher oder justizieller Zusammenarbeit in Strafsachen sind, und dass sie weder den Zugang zu den Daten durch die zuständigen nationalen Behörden noch die Verwendung und den Austausch dieser Daten zwischen diesen Behörden harmonisiere. Daraus schloss er, dass die Richtlinie im Wesentlichen die Tätigkeiten der Diensteanbieter im betroffenen Sektor des Binnenmarkts erfasse, und erhielt die Rechtsgrundlage demzufolge aufrecht.[12]

3.3. Datensicherung

Die Datenvorratsspeicherung unterscheidet sich von der Datensicherung (auch als „Quick Freeze" bezeichnet), bei der Betreiber auf gerichtliche Anordnung hin verpflichtet sind, ab dem Datum der Anordnung Daten, die sich auf bestimmte, strafbarer Handlungen verdächtige Personen beziehen, zu sichern. Die Datensicherung ist eines der von den Unterzeichnerstaaten des Übereinkommens über Computerkriminalität des Europarats[13] vorgesehenen und verwendeten Instrumente für strafrechtliche Ermittlungen. Fast alle Unterzeichnerstaaten haben eine Kontaktstelle bestimmt, die bei Ermittlungen oder Verfahren im Zusammenhang mit Computerkriminalität für unverzügliche Unterstützung sorgt. Jedoch scheinen nicht alle

---

Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben ist.'"

11 Die Artikel-29-Datenschutzgruppe hinterfragt, „ob die Richtlinie [über die Vorratsdatenspeicherung] als Ausnahmeregelung zur allgemeinen Pflicht, Verkehrsdaten mit der Beendigung der elektronischen Kommunikation zu löschen, dienen soll, oder vielmehr als Befugnisnorm für die Vorratsspeicherung all jener Daten, zu deren Speicherung die Diensteanbieter bereits für [ihre geschäftlichen] Zwecke ermächtigt wurden."

12 EuGH, Rs. C-301/06 Irland gegen Parlament und Rat, Slg. 2009, S. I-00593.

13 Artikel 16 des Übereinkommens über Computerkriminalität (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

Parteien die notwendigen Maßnahmen zur Datensicherung getroffen zu haben. Zudem wurde noch nicht bewertet, wie wirksam dieses Modell bei der Bekämpfung der Computerkriminalität tatsächlich ist.[14] Kürzlich wurde eine als „Quick Freeze Plus" bezeichnete Art der Datensicherung entwickelt. Dieses Modell geht insoweit über die einfache Datensicherung hinaus, als auf richterliche Anordnung auch Zugang zu Daten gewährt werden kann, die der Betreiber noch nicht gelöscht hat. Ferner besteht eine sehr begrenzte und zeitlich eng befristete gesetzliche Befreiung von der Verpflichtung, bestimmte, normalerweise nicht gespeicherte Kommunikationsdaten wie Standortdaten, Internetverbindungsdaten und dynamische IP-Adressen von Nutzern mit Flatrates oder in Fällen, in denen eine Speicherung zur Gebührenabrechnung nicht notwendig ist, zu löschen.

Befürworter der Datensicherung meinen, dass diese weniger stark in die Privatsphäre eingreife als die Vorratsdatenspeicherung. Doch die meisten Mitgliedstaaten sind nicht der Auffassung, dass Variationen der Datensicherung die Vorratsdatenspeicherung adäquat ersetzen können, und argumentieren, dass im Gegensatz zur Vorratsdatenspeicherung, die zur Folge habe, dass historische Daten verfügbar sind, die Datensicherung nicht gewährleiste, dass Beweisspuren vor dem Datum der gerichtlichen Anordnung gesichert, Ermittlungen ohne bekanntes Ziel geführt oder Beweismittel zu Bewegungen, etwa von Geschädigten oder Zeugen einer Straftat, gesammelt werden können.[15]

4. UMSETZUNG DER RICHTLINIE ÜBER DIE VORRATSDATENSPEICHERUNG

Die Mitgliedstaaten waren verpflichtet, die Richtlinie vor dem 15. September 2007 umzusetzen, und hatten die Möglichkeit, die Umsetzung der Pflichten zur Speicherung von Daten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail bis 15. März 2009 aufzuschieben.

Die folgende Analyse beruht auf den bei der Kommission eingegangenen Mitteilungen der Umsetzungsmaßnahmen von 25 Mitgliedstaaten einschließlich Belgien, das die Richtlinie nur teilweise umgesetzt hat.[16] In Österreich und Schweden werden derzeit Gesetzentwürfe erörtert. In diesen beiden Mitgliedstaaten besteht keine Pflicht zur Vorratsdatenspeicherung, jedoch können Strafverfolgungsbehörden von Betreibern Verkehrsdaten, soweit sie vorliegen, anfragen und einholen und machen von dieser Möglichkeit auch Gebrauch. Nachdem die Tschechische Republik, Deutschland und Rumänien zunächst ihre Umsetzungsmaßnahmen mitgeteilt hatten, erklärten ihre jeweiligen Verfassungsgerichte die betreffenden

---

14 Quelle: Europarat.

15 Dies wurde auch vom deutschen Bundesverfassungsgericht in seinem Urteil zur Nichtigerklärung des deutschen Gesetzes zur Umsetzung der Richtlinie anerkannt (siehe Abschnitt 4.9) (Bundesverfassungsgericht, 1 BvR 256/08 vom 2. März 2010, Randnr. 208).

16 Die 25 Mitgliedstaaten, die der Kommission ihre Maßnahmen zur Umsetzung der Richtlinie mitgeteilt haben, sind Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, die Niederlande, Polen, Portugal, Rumänien, die Slowakei, Slowenien, Spanien, die Tschechische Republik, Ungarn, das Vereinigte Königreich und Zypern. Belgien hat der Kommission mitgeteilt, dass ein Gesetzentwurf zum Abschluss der Umsetzung noch auf dem parlamentarischen Weg ist.

innerstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie für nichtig.[17] Diese Mitgliedstaaten erwägen nun, wie sie die Richtlinie erneut umsetzen können.

Dieser Abschnitt analysiert, wie die Mitgliedstaaten die betreffenden Vorschriften der Richtlinie umgesetzt haben. Ferner wird untersucht, ob sich die Mitgliedstaaten dafür entschieden haben, den Betreibern die durch die Vorratsspeicherung und den Abruf von Daten entstehenden Kosten zu erstatten, da die Richtlinie keine diesbezügliche Regelung enthält, und welche Bedeutung die Urteile der Verfassungsgerichte von Deutschland, Rumänien und der Tschechischen Republik für die Richtlinie haben.

4.1. Zweck der Vorratsdatenspeicherung (Artikel 1)

Die Richtlinie verpflichtet die Mitgliedstaaten, durch entsprechende Maßnahmen dafür Sorge zu tragen, dass Daten auf Vorrat gespeichert werden und zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen. Dennoch werden in den innerstaatlichen Rechtsvorschriften weiterhin unterschiedliche Zwecke für die Vorratsspeicherung von und/oder den Zugang zu Daten genannt. Zehn Mitgliedstaaten (Bulgarien, Estland, Finnland, Griechenland, Irland, Litauen, Luxemburg, die Niederlande, Spanien und Ungarn) haben den Begriff „schwere Straftat“ unter Bezugnahme auf eine Mindestfreiheitsstrafe, auf die Möglichkeit der Verhängung einer Freiheitsstrafe oder auf eine in den innerstaatlichen Rechtsvorschriften an anderer Stelle festgelegte Liste von Straftaten definiert. Acht Mitgliedstaaten (Belgien, Dänemark, Frankreich, Italien, Lettland, Polen, die Slowakei und Slowenien) sehen die Vorratsspeicherung von Daten nicht nur zur Ermittlung, Feststellung und Verfolgung schwerer Straftaten, sondern auch im Zusammenhang mit sämtlichen Straftaten sowie zur Verhütung von Kriminalität oder aus allgemeinen Gründen der nationalen oder staatlichen und/oder öffentlichen Sicherheit vor. In den Rechtsvorschriften von vier Mitgliedstaaten (Malta, Portugal, Vereinigtes Königreich und Zypern) wird auf „schwere Straftaten“ oder „schwere Vergehen“ Bezug genommen, ohne die Begriffe überhaupt zu definieren. Tabelle 1 legt dies im Einzelnen dar.

Tabelle 1: In innerstaatlichen Rechtsvorschriften angegebene Einschränkung des Zwecks der Vorratsdatenspeicherung

Belgien	Zur Ermittlung und Verfolgung von Straftaten, Verfolgung des Missbrauchs von Notdienstrufnummern, Untersuchung des vorsätzlichen Missbrauchs von elektronischen Kommunikationsnetzen oder -diensten sowie für Informationsbeschaffungseinsätze von Geheim- und Sicherheitsdiensten.[18]

[17] Entscheidung Nr. 1258 des rumänischen Verfassungsgerichts vom 8. Oktober 2009, rumänisches Staatsblatt (Monitorul Oficial) 789 vom 23. November 2009; Urteil des Bundesverfassungsgerichts 1 BvR 256/08 vom 2. März 2010, veröffentlicht am 1. April 2011; Urteil des tschechischen Verfassungsgerichts vom 22. März 2011 zu Artikel 97 Absätze 3 und 4 des Gesetzes Nr. 127/2005 über die elektronische Kommunikation und zur Änderung damit zusammenhängender Gesetze sowie zum Erlass Nr. 485/2005 über die Vorratsdatenspeicherung und die Übermittlung an die zuständigen Behörden.

[18] Artikel 126 Absatz 1 des Gesetzes über die elektronische Kommunikation vom 13. Juni 2005. .

Tabelle 1: In innerstaatlichen Rechtsvorschriften angegebene Einschränkung des Zwecks der Vorratsdatenspeicherung	
Bulgarien	Zur Feststellung und Ermittlung von schweren Straftaten und Straftaten nach den Artikeln 319a bis 319f des Strafgesetzbuchs sowie zur Fahndung nach Personen.[19]
Tschechische Republik	Nicht umgesetzt.
Dänemark	Zur Ermittlung und Verfolgung von Straftaten.[20]
Deutschland	Nicht umgesetzt.
Estland	Verwendung zulässig, wenn eine Sammlung von Beweismitteln durch andere Verfahrenshandlungen ausgeschlossen oder besonders schwierig ist und Gegenstand des Strafverfahrens eine Straftat ersten Grades oder eine vorsätzlich begangene und mit mindestens drei Jahren Freiheitsentzug bedrohte Straftat zweiten Grades ist.[21]
Irland	Zur Verhütung schwerer Straftaten (d. h. mit mindestens fünf Jahren Freiheitsentzug bedrohte Straftaten oder eine der im Anhang zum Umsetzungsgesetz aufgeführten Straftaten), zum Schutz der staatlichen Sicherheit oder zur Rettung von Menschenleben.[22]
Griechenland	Zur Aufdeckung von besonders schweren Straftaten.[23]
Spanien	Zur Feststellung, Ermittlung und Verfolgung der im Strafgesetzbuch oder den besonderen Strafgesetzen aufgeführten schweren Straftaten.[24]
Frankreich	Zur Feststellung, Ermittlung und Verfolgung von Straftaten und ausschließlich mit dem Ziel, den Justizbehörden benötigte Informationen zur Verfügung zu stellen, sowie zur Verhinderung von Terroranschlägen und zum Schutz von geistigem Eigentum.[25]
Italien	Zur Ermittlung und Bekämpfung von Straftaten.[26]

19 Artikel 250a Absatz 2 des Gesetzes über die elektronische Kommunikation, geänderte Fassung 2010.

20 Artikel 1 der Verordnung über die Vorratsdatenspeicherung.

21 Artikel 110 Absatz 1 der Strafprozessordnung.

22 Artikel 6 des Communications (Retention of Data) Act 2011 [Gesetz über Kommunikation (Vorratsdatenspeicherung) von 2011].

23 Diese Straftaten sind in Artikel 4 des Gesetzes 2225/1994 definiert; Artikel 1 des Gesetzes 3917/2011.

24 Artikel 1 Absatz 1 des Gesetzes 25/2007.

25 Folgende Rechtsakte regeln die Verwendung von auf Vorrat gespeicherten Daten bei Straftaten, zur Verhinderung von Terroranschlägen bzw. für den Schutz geistigen Eigentums: Artikel L.34-1(II) CPCE, Gesetz Nr. 2006-64 vom 23. Januar 2006 und Gesetz Nr. 2009-669 vom 12. Juni 2009.

26 Artikel 132 Absatz 1 des Datenschutzgesetzbuchs.

Tabelle 1: In innerstaatlichen Rechtsvorschriften angegebene Einschränkung des Zwecks der Vorratsdatenspeicherung	
Zypern	Zur Ermittlung von schweren Vergehen.[27]
Lettland	Zum Schutz der staatlichen und öffentlichen Sicherheit oder zur Ermittlung von Straftaten, zur Strafverfolgung und zur Durchführung gerichtlicher Strafverfahren.[28]
Litauen	Für die Ermittlung, Feststellung und Verfolgung von schweren und sehr schweren Straftaten im Sinne des litauischen Strafgesetzbuchs.[29]
Luxemburg	Zur Feststellung, Ermittlung und Verfolgung von mit mindestens einem Jahr [30]Freiheitsentzug bedrohten Straftaten.
Ungarn	Um den Ermittlungsbehörden, der Staatsanwaltschaft, den Gerichten und nationalen Sicherheitsbehörden die Wahrnehmung ihrer Aufgaben zu ermöglichen und die Polizei sowie das Nationale Steuer- und Zollamt in die Lage zu setzen, bei Straftaten zu ermitteln, die mit mindestens zwei Jahren Freiheitsentzug bedroht sind.[31]
Malta	Zur Ermittlung, Feststellung oder Verfolgung von schweren Straftaten.[32]
Niederlande	*Zur Ermittlung und Verfolgung von mit Freiheitsentzug bedrohten schweren Straftaten.*[33]
Österreich	Nicht umgesetzt.
Polen	Zur Verhütung oder Feststellung von Straftaten, zur Verhütung und Feststellung von Zoll- und Steuervergehen, zur Verwendung durch Staatsanwaltschaften und Gerichte, soweit dies für anhängige Gerichtsverfahren von Bedeutung ist, damit der Inlandsgeheimdienst, der Auslandsgeheimdienst, das Zentrale Antikorruptionsbüro, der Militärische Inlandsgeheimdienst und der Militärische Auslandsgeheimdienst ihre Aufgaben wahrnehmen können.[34]

27 Artikel 4 Absatz 1 des Gesetzes 183(I)/2007.

28 Artikel 71 Absatz 1 des Gesetzes über die elektronische Kommunikation.

29 Artikel 65 des Gesetzes X-1835.

30 Artikel 1 Absatz 1 des Gesetzes vom 24. Juli 2010.

31 Artikel 159/A des Gesetzes C/2003 in der durch das Gesetz CLXXIV/2007 geänderten Fassung; für den Zugang der Polizei: Artikel 68 des Gesetzes XXXIV/1994; für den Zugang des Nationalen Steuer- und Zollamts: Artikel 59 des Gesetzes CXXII/2010.

32 Artikel 20 Absatz 1 der Legal Notice 198/2008.

33 Artikel 126 der Strafprozessordnung.

34 Artikel 180a des Telekommunikationsgesetzes vom 16. Juli 2004 in der durch Artikel 1 des Gesetzes vom 24. April 2009 geänderten Fassung.

Tabelle 1: In innerstaatlichen Rechtsvorschriften angegebene Einschränkung des Zwecks der Vorratsdatenspeicherung	
Portugal	Zur Ermittlung, Feststellung und Verfolgung von schweren Straftaten.[35]
Rumänien	Nicht umgesetzt.
Slowenien	Zur Gewährleistung der nationalen Sicherheit, der verfassungsmäßigen Ordnung sowie der Sicherheitsinteressen, politischen und wirtschaftlichen Interessen des Staates und zum Zwecke der Landesverteidigung.[36]
Slowakei	Zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten.[37]
Finnland	Zur Ermittlung, Feststellung und Verfolgung schwerer Straftaten gemäß Kapitel 5a Artikel 3 Absatz 1 des Gesetzes über Zwangsmaßnahmen.[38]
Schweden	Nicht umgesetzt.
Vereinigtes Königreich	Zur Ermittlung, Feststellung und Verfolgung von schweren Straftaten.[39]

Die meisten Mitgliedstaaten, die die Richtlinie umgesetzt haben, gestatten in ihren innerstaatlichen Rechtsvorschriften den Zugang zu und die Verwendung von gespeicherten Daten zu Zwecken, die über die Zwecke der Richtlinie hinausgehen, etwa zur Verhütung und Bekämpfung der Kriminalität im Allgemeinen und von Gefahren für Leib und Leben. Zwar ist dies nach der Datenschutzrichtlinie für elektronische Kommunikation zulässig, doch haben die EU-Rechtsvorschriften auf diesem Gebiet bislang nur eine begrenzte Harmonisierung erreicht. Unterschiedliche Zwecke der Vorratsdatenspeicherung dürften sich auf Umfang und Häufigkeit der Anfragen und somit auf die durch die Einhaltung der Verpflichtungen nach der Richtlinie entstehenden Kosten auswirken. Zudem beeinträchtigt dies möglicherweise die Vorhersehbarkeit, die für jede gesetzgeberische Maßnahme, die das Recht auf Privatsphäre

35 Artikel 1, Artikel 3 Absatz 1 des Gesetzes 32/2008.

36 Artikel 170a Absatz 1 des Gesetzes über die elektronische Kommunikation.

37 Artikel 59a Absatz 6 des Gesetzes über die elektronische Kommunikation.

38 Artikel 14a Absatz 1 des Gesetzes über die elektronische Kommunikation.

39 The Data Retention (EC Directive) Regulations 2009 (2009 No. 859) [Verordnung über die Vorratsdatenspeicherung (EG-Richtlinie) 2009].

einschränkt, erforderlich ist.[40] Die Kommission wird prüfen, ob in diesem Bereich eine stärkere Harmonisierung erforderlich und wie sie gegebenenfalls zu erreichen ist.[41]

4.2. Pflicht der Betreiber zur Vorratsdatenspeicherung (Artikel 1)

Die Richtlinie betrifft die „Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes“ (Artikel 1 Absatz 1). Zwei Mitgliedstaaten (Finnland und das Vereinigte Königreich) verpflichten kleine Betreiber nicht zur Vorratsspeicherung von Daten, weil, so ihre Begründung, die damit sowohl für die Betreiber als auch für den Staat verbundenen Kosten in keinem Verhältnis zu den Vorteilen für die Strafjustizsysteme und die Strafverfolgung stünden. Vier Mitgliedstaaten (Lettland, Luxemburg, die Niederlande und Polen) berichten, dass sie alternative Verwaltungsregelungen getroffen haben. Während in mehreren Mitgliedstaaten tätige große Betreiber die Kosten aufgrund von Skaleneffekten abfedern können, neigen kleinere Betreiber in einigen Mitgliedstaaten dazu, zur Einsparung von Kosten Jointventures zu gründen oder die Vorratsspeicherung und den Abruf von Daten an darauf spezialisierte Unternehmen auszulagern. Eine derartige Auslagerung technischer Funktionen hat keine Auswirkungen auf die Pflicht der Betreiber, die Verarbeitungsvorgänge genau zu überwachen und für die erforderlichen Sicherheitsmaßnahmen zu sorgen, was sich besonders für kleinere Betreiber als problematisch erweisen kann. Die Kommission wird die Datensicherheitsaspekte möglicher Optionen zur Änderung des Rechtsrahmens für die Vorratsdatenspeicherung und ihre Auswirkungen auf kleine und mittlere Unternehmen prüfen.

4.3. Zugang zu Daten: Behörden, Verfahren und Bedingungen (Artikel 4)

Die Mitgliedstaaten sind verpflichtet, „sicherzustellen, dass die […] auf Vorrat gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden.“ Es wird den Mitgliedstaaten überlassen, in ihrem innerstaatlichen Recht unter Berücksichtigung der einschlägigen Bestimmungen des Rechts der Europäischen Union oder des Völkerrechts, insbesondere der Europäischen Menschenrechtskonvention in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte, das Verfahren und die Bedingungen festzulegen, die für den Zugang zu auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.

In allen Mitgliedstaaten haben die nationale Polizei und – ausgenommen die Common-Law-Staaten (Irland und Vereinigtes Königreich) – die Staatsanwaltschaft Zugang zu auf Vorrat gespeicherten Daten. Vierzehn Mitgliedstaaten führen Sicherheits- oder Geheimdienste oder

---

[40] Urteil des Europäischen Gerichtshofs vom 20. Mai 2003 in den verbundenen Rechtssachen C–465/00, C–138/01 und C–139/01 (Ersuchen um Vorabentscheidung des Verfassungsgerichtshof und des Obersten Gerichtshofs): Rechnungshof (C–465/00) gegen Österreichischer Rundfunk und andere und Christa Neukomm (C–138/01) und Joseph Lauermann (C–139/01) gegen Österreichischer Rundfunk (Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten – Richtlinie 95/46/EG – Schutz der Privatsphäre – Offenlegung der Einkommensdaten von Arbeitnehmern bei Rechtsträgern, die der Kontrolle durch den Rechnungshof unterliegen).

[41] Im Zusammenhang mit dem Erlass der Richtlinie hat die Kommission in einer Erklärung vorgeschlagen, die Liste der Straftaten nach dem Europäischen Haftbefehl zu berücksichtigen. (Rahmenbeschluss 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten).

das Militär als zuständige Behörden auf. Sechs Mitgliedstaaten führen Steuer- und/oder Zollbehörden auf und drei nennen Grenzkontrollbehörden. Ein Mitgliedstaat gestattet anderen Behörden Zugang zu den Daten, sofern sie durch sekundäre Rechtsvorschriften für besondere Zwecke dazu ermächtigt werden. In elf Mitgliedstaaten ist für jede Anfrage nach Zugang zu auf Vorrat gespeicherten Daten eine richterliche Genehmigung erforderlich. In drei Mitgliedstaaten wird in den meisten Fällen eine solche richterliche Genehmigung benötigt. Vier Mitgliedstaaten sehen eine Genehmigung einer vorgesetzten Behörde, nicht jedoch eine richterliche Genehmigung vor. In zwei Mitgliedstaaten scheint die einzige Bedingung darin zu bestehen, dass die Anfrage schriftlich gestellt wird.

Tabelle 2: Zugang zu gespeicherten Telekommunikationsdaten		
	Zuständige nationale Behörden	*Verfahren und Bedingungen*
Belgien	Stelle zur justiziellen Koordinierung, Untersuchungsrichter, Staatsanwaltschaft, Kriminalpolizei.	Für den Zugang ist eine richterliche oder staatsanwaltschaftliche Genehmigung erforderlich. Betreiber müssen auf Anfrage Teilnehmer-, Verkehrs- und Standortdaten für Verbindungen des letzten Monats in „Echtzeit“ zur Verfügung stellen. Daten für ältere Verbindungen sind schnellstmöglich zur Verfügung zu stellen.
Bulgarien[42]	Bestimmte Direktionen und Abteilungen des Nationalen Sicherheitsdienstes, das Innenministerium, der Militärgeheimdienst, die Militärpolizei, der Verteidigungsminister, der Nationale Ermittlungsdienst, das Gericht und Ermittlungsbehörden unter bestimmten Bedingungen.	Zugang nur auf Anordnung des Leiters eines Kreisgerichts möglich.
Tschechische Republik	Nicht umgesetzt.	
Dänemark[43]	Polizei	Für den Zugang ist eine richterliche Genehmigung erforderlich. Gerichtliche Anordnungen werden nur erlassen, wenn der Antrag strenge Kriterien (Verdacht, Notwendigkeit und Verhältnismäßigkeit) erfüllt.
Deutschland	Nicht umgesetzt	
Estland[44]	Das Polizei- und Grenzschutzamt, das Sicherheitspolizeiamt und – für Objekte und elektronische Kommunikation – das Steuer- und Zollamt.	Für den Zugang ist die Genehmigung eines Ermittlungsrichters erforderlich. Die Betreiber müssen auf Vorrat gespeicherte Daten in dringenden Fällen innerhalb von 10 Stunden und in anderen Fällen innerhalb von 10 Arbeitstagen nach Erhalt der Anfrage zur Verfügung stellen.
Irland[45]	Mitglieder der Garda Síochána (Polizei) im Rang eines Chief Superintendent oder höher, Offiziere der Permanent Defence Force (Ständige Streitkräfte) im Rang eines Colonel (Oberst) oder höher, Beamte des Office of the Revenue Commissioners (Finanzverwaltung)	Anfragen bedürfen der Schriftform.

42 Artikel 250b Absatz 1 des Gesetzes über die elektronische Kommunikation, geänderte Fassung 2010 (Behörden), Artikel 250b Absatz 1 und Artikel 250c Absatz 1 des Gesetzes über die elektronische Kommunikation, geänderte Fassung 2010 (Zugang).

43 Kapitel 71 des Rechtspflegegesetzes.

44 Artikel 112 Absätze 2 und 3 der Strafprozessordnung (Behörden und Verfahren), Artikel 111 Absatz 9 des Gesetzes über die elektronische Kommunikation (Bedingungen).

Tabelle 2: Zugang zu gespeicherten Telekommunikationsdaten		
	Zuständige nationale Behörden	*Verfahren und Bedingungen*
	im Rang eines Principal Officer (Hauptfinanzrat) oder höher.	
Griechenland[46]	Justiz-, Militär- oder Polizeibehörden.	Für den Zugang ist ein Gerichtsbeschluss erforderlich, der besagt, dass die Ermittlungen mit anderen Mitteln unmöglich oder extrem schwierig sind.
Spanien[47]	Für die Feststellung, Ermittlung und Verfolgung von schweren Straftaten zuständige Polizeikräfte, der Geheimdienst und die Zollagentur.	Für den Zugang der zuständigen nationalen Behörden ist eine vorherige richterliche Genehmigung erforderlich.
Frankreich[48]	Staatsanwalt, benannte Offiziere der Polizei und Gendarmerie.	Die Polizei muss jede Anfrage nach gespeicherten Daten begründen und dafür die Genehmigung der von der Commission Nationale de Contrôle des Interceptions de Sécurité benannten Person im Innenministerium einholen. Zugangsanfragen werden von einem benannten Mitarbeiter des Betreibers bearbeitet.
Italien[49]	Staatsanwalt, Polizei, der Verteidiger des Angeklagten bzw. der Person, gegen die ermittelt wird.	Für den Zugang ist eine begründete staatsanwaltschaftliche Anordnung erforderlich.
Zypern[50]	Gerichte, Staatsanwaltschaft, Polizei	Für den Zugang ist eine staatsanwaltschaftliche Genehmigung erforderlich, die erteilt wird, wenn sich der Staatsanwalt dadurch die Erlangung von Beweismitteln für schwere Straftaten verspricht. Ein Richter kann eine entsprechende Anordnung erlassen, wenn ein hinreichender Verdacht auf eine schwere Straftat sowie die Wahrscheinlichkeit besteht, dass die Daten damit im Zusammenhang stehen.
Lettland[51]	Ermächtigte Beamte in Ermittlungsbehörden, mit Ermittlungen befasste Personen, ermächtigte Beamte in Staatssicherheitseinrichtungen, die Staatsanwaltschaft, die Gerichte.	Die ermächtigten Beamten, die Staatsanwaltschaft und die Gerichte müssen die Angemessenheit und Relevanz der Anfrage prüfen, die Anfrage dokumentieren und den Schutz der eingeholten Daten gewährleisten. Die ermächtigten Stellen können mit Betreibern Vereinbarungen, etwa über die Verschlüsselung der übermittelten Daten, schließen.
Litauen[52]	Ermittlungsbehörden, die Staatsanwaltschaft, das Gericht (Richter) und Geheimdienstbeamte.	Ermächtigte Behörden müssen auf Vorrat gespeicherte Daten schriftlich anfordern.

45 Artikel 6 des Communications (Retention of Data) Bill 2009 [Gesetzesvorlage zur Kommunikation (Vorratsdatenspeicherung) von 2009].

46 Artikel 3 und 4 des Gesetzes 2225/94.

47 Artikel 6–7 des Gesetzes 25/2007.

48 Artikel 60-1 und 60-2 der Strafprozessordnung (Behörden) und Artikel L.31-1-1 (Bedingungen).

49 Artikel 132 Absatz 3 des Datenschutzgesetzbuchs.

50 Artikel 4 Absätze 2 und 4 des Gesetzes 183(I)/2007.

51 Artikel 71 Absatz 1 des Gesetzes über die elektronische Kommunikation (Behörden). Kabinettsverordnung Nr. 820 (Verfahren).

Tabelle 2: Zugang zu gespeicherten Telekommunikationsdaten		
	Zuständige nationale Behörden	*Verfahren und Bedingungen*
		Für den Zugang im Rahmen von Ermittlungen ist eine richterliche Anordnung erforderlich.
Luxemburg[53]	Justizbehörden (Ermittlungsrichter, Staatsanwaltschaft), für den Schutz der staatlichen Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten zuständige Behörden.	Für den Zugang ist eine richterliche Genehmigung erforderlich.
Ungarn[54]	Polizei, Nationale Steuer- und Zollbehörde, nationale Sicherheitsbehörden, Staatsanwaltschaft, Gerichte.	Die Polizei sowie die Nationale Steuer- und Zollbehörde benötigen eine staatsanwaltschaftliche Genehmigung. Staatsanwaltschaft und nationale Sicherheitsbehörden haben ohne richterliche Anordnung Zugang zu diesen Daten.
Malta[55]	Polizei; Sicherheitsdienst	Anfragen bedürfen der Schriftform.
Niederlande[56]	Ermittlungsbeamte der Polizei	Für den Zugang ist eine richterliche oder staatsanwaltschaftliche Anordnung erforderlich.
Österreich	Nicht umgesetzt	
Polen[57]	Polizei, Grenzschutz, Finanzämter, Inlandsgeheimdienst, Auslandsgeheimdienst, Zentrales Antikorruptionsbüro, Militärischer Inlandsgeheimdienst, Militärischer Auslandsgeheimdienst, Gerichte, Staatsanwaltschaft	Anfragen bedürfen der Schriftform und im Falle der Polizei, des Grenzschutzes oder der Finanzämter der Genehmigung durch einen leitenden Beamten der betreffenden Organisation.
Portugal[58]	Kriminalpolizei, Republikanische Nationalgarde, Büro für öffentliche Sicherheit, Militärische Kriminalpolizei, Einwanderungs- und Grenzbehörde, Wasserschutzpolizei.	Für die Datenübertragung ist eine richterliche Genehmigung mit der Begründung erforderlich, dass der Zugang zu den Daten von entscheidender Bedeutung für die Wahrheitsfindung ist oder Beweismittel auf andere Weise nicht oder nur sehr schwer zu beschaffen wären. Für die richterliche Genehmigung ist ein Nachweis der Notwendigkeit und Verhältnismäßigkeit erforderlich.
Rumänien	Nicht umgesetzt	
Slowenien[59]	Polizei, Geheim- und Sicherheitsdienst sowie für Aufklärungs-, Spionageabwehr- und Sicherheitsmissionen zuständige Verteidigungsagenturen.	Für den Zugang ist eine richterliche Genehmigung erforderlich.

52 Artikel 77 Absätze 1 und 2 des Gesetzes X-1835, mündlicher Bericht an die Kommission.

53 Artikel 5-2 Absatz 1 und Artikel 9 Absatz 2 des Gesetzes vom 24. Juli 2010 (Behörden), Artikel 67-1 des Strafgesetzbuchs (Bedingungen).

54 Artikel 68 Absatz 1 und Artikel 69 Absatz 1 Buchstaben c und d des Gesetzes XXXIV von 1994, Artikel 9/A Absatz 1 des Gesetzes V von 1972, Artikel 71 Absätze 1, 3 und 4, Artikel 178/A Absatz 4, Artikel 200, 201 und 268 Absatz 2 des Gesetzes XIX von 1998, Artikel 40 Absätze 1 und 2, Artikel 53 Absatz 1, Artikel 54 Absatz 1 Buchstabe j des Gesetzes CXXV von 1995.

55 Artikel 20 Absätze 1 und 3 der Legal Notice 198/2008.

56 Artikel 12ni der Strafprozessordnung.

57 Artikel 179 Absatz 3 des Telekommunikationsgesetzes vom 16. Juli 2004 in der durch Artikel 1 des Gesetzes vom 24. April 2009 geänderten Fassung.

58 Artikel 2 Absatz 1, Artikel 3 Absatz 2 und Artikel 9 des Gesetzes 32/2008.

Tabelle 2: Zugang zu gespeicherten Telekommunikationsdaten		
	Zuständige nationale Behörden	*Verfahren und Bedingungen*
Slowakei[60]	Strafverfolgungsbehörden, Gerichte.	Anfragen bedürfen der Schriftform.
Finnland[61]	Polizei, Grenzschutz, Zollbehörden (für auf Vorrat gespeicherte Teilnehmer-, Verkehrs- und Standortdaten). Notfallabwehrzentrum, Seenotrettungszentrum, Unterzentrale für Seenotrettung (für Identifizierungs- und Standortdaten in Notfällen).	Alle zuständigen Behörden haben ohne richterliche Genehmigung Zugang zu Teilnehmerdaten. Für andere Daten ist eine richterliche Anordnung erforderlich.
Schweden	Nicht umgesetzt	
Vereinigtes Königreich[62]	Polizei, Geheimdienste, Steuer- und Zollbehörden, andere in sekundären Rechtsvorschriften festgelegte Behörden.	Für den Zugang, der nur in besonderen Fällen und Situationen zulässig ist, in denen eine Übermittlung der Daten gesetzlich zulässig oder vorgeschrieben ist, ist eine Genehmigung durch eine benannte Person sowie eine Prüfung der Notwendigkeit und Verhältnismäßigkeit erforderlich. Mit den Betreibern wurden konkrete Verfahrensweisen vereinbart.

Die Kommission wird prüfen, ob eine stärkere Harmonisierung im Hinblick darauf, welche Behörden Zugang zu auf Vorrat gespeicherten Daten haben und nach welchem Verfahren ihnen dieser Zugang gewährt wird, erforderlich und wie sie gegebenenfalls zu erreichen ist. Denkbar wären klarer definierte Listen zuständiger Behörden, eine unabhängige und/oder gerichtliche Aufsicht über Datenanfragen und Mindeststandards für Verfahren, nach denen Betreiber den zuständigen Behörden Zugang gewähren.

4.4. Anwendungsbereich der Vorratsdatenspeicherung und Kategorien von Daten (Artikel 1 Absatz 2, Artikel 3 Absatz 2 und Artikel 5)

Die Richtlinie betrifft die Bereiche Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie. Sie bestimmt in Artikel 5 die Kategorien von auf Vorrat zu speichernden Daten. Dies sind insbesondere Daten zur Identifizierung:

(a) der Quelle einer Nachricht,

(b) des Adressaten einer Nachricht,

(c) von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung,

---

59 Artikel 107c des Gesetzes über die elektronische Kommunikation, Artikel 149b der Strafprozessordnung, Artikel 24 Buchstabe b des Gesetzes über den Geheim- und Sicherheitsdienst, Artikel 32 des Gesetzes über die Landesverteidigung.

60 Artikel 59a Absatz 8 des Gesetzes über die elektronische Kommunikation.

61 Artikel 35 Absatz 1 und Artikel 36 des Gesetzes über die elektronische Kommunikation, Artikel 31–33 des Polizeigesetzes, Artikel 41 des Grenzschutzgesetzes.

62 Artikel 25 und Anhang 1 des Regulation of Investigatory Powers Act 2000 (Gesetz zur Regelung von Ermittlungsbefugnissen von 2000), Artikel 7 der Data Retention Regulation (Verordnung über die Vorratsdatenspeicherung). In Artikel 22 Absatz 2 des RIPA wird festgelegt, zu welchen Zwecken diese Behörden Daten einholen können.

(d) der Art einer Nachrichtenübermittlung,

(e) der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern sowie

(f) des Standorts mobiler Geräte.

Sie betrifft ferner erfolglose Anrufversuche, also Telefonanrufe, bei denen die Verbindung erfolgreich aufgebaut wurde, die aber unbeantwortet bleiben oder bei denen das Netzwerkmanagement eingegriffen hat, wenn die betreffenden Daten von den Betreibern erzeugt oder verarbeitet und gespeichert oder protokolliert werden (Artikel 3 Absatz 2). Nach der Richtlinie dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden. Später wurde auch klargestellt, dass Suchanfragen, d. h. von einem Suchmaschinendienst generierte Server-Protokolle, ebenfalls nicht in den Anwendungsbereich der Richtlinie fallen, weil sie nicht als Verkehrsdaten, sondern als Inhaltsdaten zu betrachten sind.[63]

Einundzwanzig Mitgliedstaaten haben in ihren Umsetzungsmaßnahmen die Vorratsspeicherung jeder dieser Datenkategorien vorgesehen. Belgien hat weder für die Arten von Telefoniedaten noch für Internetdaten eine Vorratsspeicherung vorgesehen. Diejenigen Mitgliedstaaten, die den Fragebogen der Kommission beantwortet haben, hielten eine Änderung der auf Vorrat zu speichernden Datenkategorien nicht für erforderlich, obwohl das Europäische Parlament die Kommission in einer Schriftlichen Erklärung aufgefordert hat, den Anwendungsbereich der Richtlinie „auf Suchmaschinen auszudehnen, um schnell […] gegen Kinderpornographie und sexuelle Belästigung im Internet vorgehen zu können“[64]. In ihrem Bericht über die zweite Durchsetzungsmaßnahme vertritt die Artikel-29-Datenschutzgruppe den Standpunkt, dass die in der Richtlinie vorgesehenen Kategorien als erschöpfend anzusehen sind und den Betreibern keine zusätzlichen Pflichten zur Vorratsdatenspeicherung auferlegt werden dürfen. Die Kommission wird die Notwendigkeit all dieser Datenkategorien prüfen.

4.5. Speicherungsfristen (Artikel 6 und Artikel 12)

Die Mitgliedstaaten sollen dafür sorgen, dass die in Artikel 5 angegebenen Datenkategorien für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren auf Vorrat gespeichert werden. Ein Mitgliedstaat kann die maximale Speicherungsfrist verlängern, „wenn besondere Umstände die Verlängerung […] für einen begrenzten Zeitraum rechtfertigen“. Die Verlängerung ist der Kommission anzuzeigen, die innerhalb von sechs Monaten nach der Mitteilung die Verlängerung billigen oder ablehnen kann. Während eine Verlängerung der maximalen Speicherungsfrist möglich ist, ist eine Verkürzung auf weniger als sechs Monate nicht vorgesehen. Bis auf einen Mitgliedstaat wenden alle Mitgliedstaaten, die die Richtlinie umgesetzt haben, eine oder mehrere Speicherungsfristen innerhalb dieser Grenzen an. Der Kommission wurden bislang keine Verlängerungen angezeigt. Dennoch ist die Herangehensweise innerhalb der EU uneinheitlich.

---

63 Stellungnahme der Artikel-29-Datenschutzgruppe zu Datenschutzfragen im Zusammenhang mit Suchmaschinen vom 4. April 2008.

64 Schriftliche Erklärung zur Schaffung eines europäischen Frühwarnsystems gegen Pädophilie und sexuelle Belästigung, eingereicht gemäß Artikel 123 der Geschäftsordnung, 19.4.2010, 0029/2010.

In 15 Mitgliedstaaten gilt für alle Datenkategorien eine einheitliche Speicherungsfrist: In einem Mitgliedstaat (Polen) ist eine Speicherungsfrist von zwei Jahren, in einem weiteren (Lettland) eine Speicherungsfrist von 1,5 Jahren, in zehn Mitgliedstaaten (Bulgarien, Dänemark, Estland, Finnland, Frankreich, Griechenland, den Niederlanden, Portugal, Spanien und dem Vereinigten Königreich) eine Speicherungsfrist von einem Jahr und in drei Mitgliedstaaten (Litauen, Luxemburg und Zypern) eine Speicherungsfrist von sechs Monaten vorgesehen. In fünf Mitgliedstaaten gelten für verschiedene Datenkategorien unterschiedliche Speicherungsfristen: Zwei Mitgliedstaaten (Irland und Italien) sehen zwei Jahre für Daten aus dem Telefonfestnetz und dem Mobilfunk und ein Jahr für Daten zu Internetzugang, Internet-E-Mail und Internet-Telefonie vor, ein Mitgliedstaat Slowenien) hat 14 Monate für Telefoniedaten und acht Monate für Internetdaten festgelegt, in einem Mitgliedstaat (Slowakei) sind ein Jahr für Telefonfestnetz- und Mobilfunkdaten und sechs Monate für Internetdaten und in einem weiteren Mitgliedstaat (Malta) ein Jahr für Telefonfestnetz-, Mobilfunk- und Internet-Telefonie-Daten und sechs Monate für Daten zu Internetzugang und Internet-E-Mail vorgesehen. Ein Mitgliedstaat (Ungarn) speichert sämtliche Daten ein Jahr lang, ausgenommen Daten zu erfolglosen Anrufversuchen, die lediglich sechs Monate lang gespeichert werden. Ein Mitgliedstaat (Belgien) hat keine Speicherfrist für die in der Richtlinie aufgeführten Datenkategorien festgelegt. Einzelheiten sind der Tabelle 3 zu entnehmen.

Tabelle 3: Speicherungsfristen in innerstaatlichen Rechtsvorschriften	
Belgien[65]	Zwischen 1 Jahr und 36 Monaten für öffentlich zugängliche Telefondienste. Keine Festlegung für Internetdaten.
Bulgarien	1 Jahr. Daten, zu denen Zugang gewährt wurde, können auf Verlangen weitere sechs Monate gespeichert werden.
Tschechische Republik	Nicht umgesetzt.
Dänemark	1 Jahr
Deutschland	Nicht umgesetzt
Estland	1 Jahr
Irland	2 Jahre für Daten aus dem Telefonfestnetz und dem Mobilfunk, 1 Jahr für Daten zu Internetzugang, Internet-E-Mail und Internet-Telefonie
Griechenland	1 Jahr
Spanien	1 Jahr
Frankreich	1 Jahr
Italien	2 Jahre für Daten aus dem Telefonfestnetz und dem Mobilfunk, 1 Jahr für Daten zu Internetzugang, Internet-E-Mail und Internet-Telefonie
Zypern	6 Monate
Lettland	18 Monate
Litauen	6 Monate
Luxemburg	6 Monate
Ungarn	6 Monate für erfolglose Anrufversuche und 1 Jahr für alle anderen Daten
Malta	1 Jahr für Telefonfestnetz-, Mobilfunk- und Internet-Telefonie-Daten, 6 Monate für Daten zu Internetzugang und Internet-E-Mail
Niederlande	1 Jahr
Österreich	Nicht umgesetzt
Polen	2 Jahre
Portugal	1 Jahr
Rumänien	Nicht umgesetzt (6 Monate nach dem für nichtig erklärten Umsetzungsgesetz)

[65] Artikel 126 Absatz 2 des Gesetzes über die elektronische Kommunikation vom 13. Juni 2005.

Tabelle 3: Speicherungsfristen in innerstaatlichen Rechtsvorschriften	
Slowenien	14 Monate für Telefoniedaten und 8 Monate für internetbezogene Daten
Slowakei	1 Jahr für Daten aus dem Telefonfestnetz und dem Mobilfunk, 6 Monate für Daten zu Internetzugang, Internet-E-Mail und Internet-Telefonie
Finnland	1 Jahr
Schweden	Nicht umgesetzt
Vereinigtes Königreich	1 Jahr

Die Richtlinie lässt derart unterschiedliche Ansätze zwar zu, jedoch folgt daraus, dass sie in mehr als einem Mitgliedstaat tätigen Betreibern sowie Bürgern, deren Kommunikationsdaten in verschiedenen Mitgliedstaaten gespeichert sind, EU-weit nur begrenzt Rechtssicherheit und Vorhersehbarkeit bietet. Angesichts der zunehmenden Internationalisierung der Datenverarbeitung und ausgelagerter Datenspeicherung sollten Möglichkeiten für eine weitere EU-weite Harmonisierung der Speicherungsfristen in Erwägung gezogen werden. Um dem Grundsatz der Verhältnismäßigkeit Rechnung zu tragen, sowie im Hinblick auf die quantitativen und qualitativen Angaben zu den gespeicherten Daten in den Mitgliedstaaten und die Trends in der Kommunikation, die Entwicklung der Technik sowie Tendenzen in der Kriminalität und beim Terrorismus wird die Kommission die Anwendung unterschiedlicher Speicherungsfristen für verschiedene Datenkategorien oder verschiedene Kategorien schwerer Straftaten oder eine Kombination aus beiden prüfen.[66] Aus den bisher vorgelegten quantitativen Angaben der Mitgliedstaaten über das Alter von gespeicherten Daten geht hervor, dass bei der (ersten) Anfrage einer Strafverfolgungsbehörde auf Zugang rund 90 Prozent der Daten nicht älter als sechs Monate waren. Rund 70 Prozent waren nicht älter als drei Monate (siehe Abschnitt 5.2).

4.6. Datenschutz und Datensicherheit sowie Kontrollstellen (Artikel 7 und 9)

Nach der Richtlinie stellen die Mitgliedstaaten sicher, dass Betreiber zumindest die folgenden vier Grundsätze der Datensicherheit einhalten:

(a) Die Daten sind von der gleichen Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im [öffentlichen Kommunikations-]Netz vorhandenen Daten.

(b) In Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen.

(c) In Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist. sowie

[66] In dem Vorschlag der Kommission für eine Richtlinie über die Vorratsspeicherung von Daten aus dem Jahr 2005 war eine Speicherungsfrist von einem Jahr für Telefoniedaten und von sechs Monaten für Internetdaten vorgesehen.

(d) Die Daten werden am Ende der Vorratsspeicherungsfrist vernichtet, mit Ausnahme jener Daten, die [zu dem in der Richtlinie festgelegten Zweck] abgerufen und gesichert worden sind.

Den Betreibern ist es im Einklang mit der Datenschutzrichtlinie und der Datenschutzrichtlinie für elektronische Kommunikation untersagt, nach der Richtlinie auf Vorrat gespeicherte Daten zu anderen Zwecken zu verarbeiten, es sei denn, die Daten wären auch aus anderen Gründen auf Vorrat gespeichert worden.[67] Die Mitgliedstaaten sollen eine öffentliche Stelle benennen, die „in völliger Unabhängigkeit" für die Kontrolle der Anwendung dieser Grundsätze zuständig ist, wobei es sich dabei um dieselben Stellen handeln kann, die nach der Datenschutzrichtlinie[68] vorgesehen sind.

Fünfzehn Mitgliedstaaten haben alle diese Grundsätze in ihren einschlägigen Rechtsvorschriften umgesetzt. Vier Mitgliedstaaten (Belgien, Estland, Lettland und Spanien) haben zwei oder drei dieser Grundsätze umgesetzt, sehen jedoch nicht ausdrücklich die Vernichtung der Daten am Ende der Speicherungsfrist vor. Zwei Mitgliedstaaten (Italien und Finnland) sehen zwar die Vernichtung von Daten vor, unklar ist jedoch, welche konkreten technischen und organisatorischen Sicherheitsmaßnahmen wie etwa strenge Authentifizierung und Management von detaillierten Zugriffsprotokollen (Logs)[69] sie getroffen haben. In 22 Mitgliedstaaten besteht eine für die Überwachung der Anwendung der Grundsätze zuständige Kontrollstelle. In den meisten Fällen handelt es sich um die Datenschutzbehörde. Einzelheiten sind der Tabelle 4 zu entnehmen.

Tabelle 4: Datenschutz und Datensicherheit sowie Kontrollstellen

Mitgliedstaat	*Datenschutz- und Datensicherheitsvorschriften im innerstaatlichen Recht*	*Kontrollstelle*
Belgien	Betreiber müssen sicherstellen, dass Datenübertragungen nicht von Dritten abgefangen werden können und den ETSI-Normen für die Sicherheit der Datenübermittlung und die rechtmäßige Überwachung entsprechen.[70] Der Grundsatz der obligatorischen Vernichtung von Daten am Ende der Speicherungsfrist scheint nicht umgesetzt zu sein.	Belgisches Institut für Postdienste und Telekommunikation
Bulgarien	Die Umsetzungsmaßnahme enthält Vorschriften zur Umsetzung der vier Grundsätze.[71]	Die Kommission für den Schutz personenbezogener Daten überwacht die Verarbeitung und Speicherung von Daten und die Einhaltung der Verpflichtungen; eine parlamentarische Kommission der Nationalversammlung überwacht die Genehmigungsverfahren und den Zugang zu den Daten.

67 Artikel 13 Absatz 1 der Richtlinie 95/46/EG.

68 Artikel 28 der Richtlinie 95/46/EG.

69 Strenge Authentifizierung umfasst doppelte Authentifizierungsmechanismen wie etwa Passwort plus biometrische Daten oder Passwort plus Token, um die körperliche Anwesenheit der für die Verarbeitung der Verkehrsdaten verantwortlichen Person sicherzustellen. Management von detaillierten Logs umfasst die detailgenaue Rückverfolgung der Arbeitsgänge bei Zugriff und Verarbeitung im Wege der Vorratsspeicherung von Logs, die zumindest die Benutzeridentität, die Zugriffszeit und die vom Zugriff betroffenen Dateien aufzeichnen.

70 Artikel 6 des Königlichen Erlasses vom 9. Januar 2003.

71 Artikel 4 Absatz 1 des Gesetzes über die elektronische Kommunikation, geänderte Fassung 2010.

Tabelle 4: Datenschutz und Datensicherheit sowie Kontrollstellen		
Mitgliedstaat	*Datenschutz- und Datensicherheitsvorschriften im innerstaatlichen Recht*	*Kontrollstelle*
Tschechische Republik[72] .	Nicht umgesetzt.	
Dänemark	In den Rechtsvorschriften sind die vier Grundsätze verankert. [73].	Die National IT and Telecom Agency (Telestyrelsen) überwacht, wie die Anbieter elektronischer Kommunikationsnetze und -dienste gemäß ihrer Verpflichtung sicherstellen, dass die technischen Ausrüstungen und Systeme den Zugang der Polizei zu Telekommunikations-Verkehrsdaten ermöglichen.
Deutschland	Nicht umgesetzt.	
Estland	In der Umsetzungsmaßnahme sind drei der vier Grundsätze verankert. Keine ausdrückliche Regelung zum vierten Grundsatz, allerdings kann jeder, dessen Privatsphäre durch Überwachungstätigkeit verletzt wurde, eine gerichtliche Entscheidung zur Vernichtung der Daten beantragen[74].	Zuständige Behörde ist die Technical Surveillance Authority (Tehnilise Järelevalve Amet).
Irland[75]	Die Umsetzungsmaßnahme enthält Vorschriften zur Umsetzung der vier Grundsätze.	Ein benannter Richter ist befugt, die Einhaltung der Umsetzungsmaßnahme durch die nationalen Behörden zu prüfen und darüber Bericht zu erstatten.
Griechenland[76]	In der Umsetzungsmaßnahme sind die vier Grundsätze verankert. Zudem müssen Betreiber einen Plan zur Einhaltung dieser Vorschriften erarbeiten und für dessen Anwendung einen Datensicherheitsmanager benennen.	Personal Data Protection Authority und Privacy of Communications Authority.
Spanien[77]	In den Datensicherheitsvorschriften sind drei der vier Grundsätze verankert (Qualität und Sicherheit von auf Vorrat gespeicherten Daten, Zugang durch befugte Personen und Schutz vor unbefugter Verarbeitung).	Zuständige Behörde ist die Agencia Española de Protección de Datos (AEPD).
Frankreich[78]	Die Umsetzungsmaßnahme enthält Vorschriften zur Umsetzung der vier Grundsätze.	Die Commission Nationale de l'Informatique et des Libertés überwacht die Einhaltung der Verpflichtungen.

[72] Artikel 87 Absatz 3 und Artikel 88 des Gesetzes 127/2005 in der durch das Gesetz 247/2008 geänderten Fassung, Artikel 2 des Gesetzes 336/2005, Artikel 3 Absatz 4 des Gesetzes 485/2005, Artikel 28 Absatz 1 des Gesetzes 101/2000.

[73] Gesetz über die Verarbeitung personenbezogener Daten; Durchführungsverordnung Nr. 714 über die Bereitstellung elektronischer Kommunikationsnetze und -dienste vom 26. Juni 2008.

[74] Artikel 111 Absatz 9 des Gesetzes über die elektronische Kommunikation, Artikel 122 Absatz 2 der Strafprozessordnung.

[75] Artikel 4, 11 und 12 des Communications (Retention of Data) Bill 2009 [Gesetzesvorlagen zur Kommunikation (Vorratsdatenspeicherung) von 2009].

[76] Artikel 6 des Gesetzes 3917/2011.

[77] Artikel 8 des Gesetzes 25/2007, Artikel 38 Absatz 3 des Allgemeinen Telekommunikationsgesetzes. Das Gesetz (Art. 9) verweist auf die Ausnahmeregelung für Zugangs- und Widerrufsrechte nach dem Organgesetz 15/1999 zum Schutz personenbezogener Daten (Art. 22 und 23).

Tabelle 4: Datenschutz und Datensicherheit sowie Kontrollstellen		
Mitgliedstaat	*Datenschutz- und Datensicherheitsvorschriften im innerstaatlichen Recht*	*Kontrollstelle*
Italien	Keine ausdrücklichen Vorschriften zur Sicherheit von auf Vorrat gespeicherten Daten, jedoch besteht grundsätzlich die Pflicht zur Vernichtung oder Anonymisierung von Verkehrsdaten und zur Einholung der Einwilligung für die Verarbeitung von Standortdaten[79].	Die Datenschutzbehörde überwacht die Einhaltung der Richtlinie durch die Betreiber.
Zypern[80]	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.	Der Commissioner for Personal Data Protection überwacht die Anwendung der Umsetzungsmaßnahme.
Lettland[81]	In der Umsetzungsmaßnahme sind zwei der vier Grundsätze verankert: die Vertraulichkeit von und der autorisierte Zugang zu auf Vorrat gespeicherten Daten sowie die Vernichtung der Daten am Ende der Speicherungsfrist.	Die Staatliche Dateninspektion (Datu valsts inspekcija) überwacht den Schutz personenbezogener Daten im Bereich der elektronische Kommunikation, nicht jedoch den Zugang zu und die Verarbeitung von auf Vorrat gespeicherten Daten.
Litauen[82]	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.	Die Staatliche Datenschutzinspektion (Valstybinė duomenų apsaugos inspekcija) überwacht die Durchführung der Umsetzungsmaßnahme und ist für die Übermittlung der Statistik an die Europäische Kommission zuständig.
Luxemburg[83]	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.	Datenschutzbehörde
Ungarn[84]	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.	Parliamentary Commissioner for Data Protection and Freedom of Information (Adatvédelmi Biztos)
Malta[85]	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.	Data Protection Commissioner
Niederlande[86]	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.	Die Agentschap Telecom überwacht die Einhaltung der Verpflichtungen durch Internet- und Telefonanbieter. Die Datenschutzbehörde überwacht die allgemeine Verarbeitung personenbezogener Daten. Die Zusammenarbeit zwischen beiden Behörden ist durch ein Protokoll geregelt.
Österreich	Nicht umgesetzt.	

78 Artikel D.98-5 CPCE; Artikel L-34-1(V) CPCE, Artikel 34 des Gesetzes Nr. 78-17, Artikel 34-1 CPCE, Artikel 11 des Gesetzes Nr. 78-17 vom 6. Januar 1978.

79 Artikel 123 und 126 des Datenschutzgesetzbuchs.

80 Artikel 14 und 15 des Gesetzes 183(I)/2007.

81 Artikel 4 Absatz 4 und Artikel 71 Absätze 6–8 des Gesetzes über die elektronische Kommunikation.

82 Artikel 12 Absatz 5, Artikel 66 Absätze 8 und 9 des Gesetzes über die elektronische Kommunikation in der Fassung vom 14. November 2009.

83 Artikel 1 Absatz 5 des Gesetzes vom 24. Juli 2010.

84 Artikel 157 des Gesetzes C/2003 in der durch das Gesetz CLXXIV/2007 geänderten Fassung, Artikel 2 der Verordnung 226/2003 und Gesetz LXIII/1992 über den Datenschutz.

85 Artikel 24 und 25 der Legal Notice 198/2008, Artikel 40 Buchstabe b des Datenschutzgesetzes (Kap. 440).

86 Artikel 13 Absatz 5 des Telekommunikationsgesetzes; der ausführliche Titel des Kooperationsprotokolls lautet *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens*.

Tabelle 4: Datenschutz und Datensicherheit sowie Kontrollstellen		
Mitgliedstaat	*Datenschutz- und Datensicherheitsvorschriften im innerstaatlichen Recht*	*Kontrollstelle*
Polen	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.[87]	Datenschutzbehörde
Portugal	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.[88]	Portugiesische Datenschutzbehörde
Rumänien	Nicht umgesetzt.	
Slowenien[89]	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.	Information Commissioner (Informacijski Pooblaščenec)
Slowakei[90]	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.	Die nationale Regulierungs- und Preisbildungsbehörde im Bereich der elektronischen Kommunikation überwacht den Schutz personenbezogener Daten.
Finnland	In der Umsetzungsmaßnahme ist lediglich ausdrücklich vorgesehen, dass die Daten am Ende der Speicherungsfrist zu vernichten sind.[91]	Die Finish Communications Regulatory Authority (Viestintävirasto) überwacht die Einhaltung der Vorschriften zur Vorratsdatenspeicherung durch die Betreiber. Der Datenschutzombudsmann überwacht die allgemeine Rechtmäßigkeit der Verarbeitung personenbezogener Daten.
Schweden	Nicht umgesetzt.	
Vereinigtes Königreich	In der Umsetzungsmaßnahme sind alle vier Grundsätze verankert.[92]	Der Information Commissioner überwacht die Vorratsspeicherung und/oder Verarbeitung von Kommunikationsdaten (und anderen personenbezogenen Daten) und hat die Aufsicht über angemessene Datenschutzkontrollen. Der Interception Officer (ein leitender Richter im Amt oder im Ruhestand) überwacht die behördliche Einholung von Kommunikationsdaten im Rahmen des RIPA. Das Investigatory Powers Tribunal untersucht Datenmissbrauchsbeschwerden, sofern die Daten aufgrund der Umsetzungsmaßnahme (RIPA) eingeholt wurden.

Artikel 7 wurde uneinheitlich umgesetzt. Bei auf Vorrat gespeicherten Daten handelt es sich um potenziell sehr persönliche und sensible Daten, für deren Verarbeitung, Speicherung, Abfrage und Verwendung durchweg hohe Datenschutz- und -sicherheitsstandards einheitlich und transparent anzuwenden sind, um die Gefahr einer Verletzung der Privatsphäre auf ein Minimum zu reduzieren und das Vertrauen der Bürger zu erhalten. Die Kommission wird Optionen zur Verbesserung von Datensicherheits- und Datenschutzstandards einschließlich Lösungen mit eingebautem Datenschutz (Privacy by Design) prüfen, um dafür zu sorgen, dass diese Standards sowohl bei der Speicherung als auch bei der Übertragung erfüllt werden. Sie

87 Artikel 180a und 180e des Telekommunikationsgesetzes.

88 Artikel 7 Absätze 1 und 5 und Artikel 11 des Gesetzes 32/2008, Artikel 53 und 54 des Gesetzes über den Schutz personenbezogener Daten.

89 Artikel 107a Absatz 6 und Artikel 107c des Gesetzes über die elektronische Kommunikation.

90 Artikel 59a des Gesetzes über die elektronische Kommunikation, Artikel S33 des Gesetzes Nr. 428/2002 über den Schutz personenbezogener Daten.

91 Artikel 16 Absatz 3 des Gesetzes über die elektronische Kommunikation.

92 Artikel 6 der Verordnung über die Vorratsdatenspeicherung.

wird dabei auch die in dem Bericht der Artikel-29-Datenschutzgruppe über die zweite Durchsetzungsmaßnahme[93] enthaltenen Empfehlungen zu Mindestschutzvorkehrungen sowie technischen und organisatorischen Sicherheitsmaßnahmen berücksichtigen.

4.7. Statistiken (Artikel 10)

Die Mitgliedstaaten sollen der Kommission jährliche Statistiken über die Vorratsdatenspeicherung übermitteln, aus denen hervorgeht:

– in welchen Fällen im Einklang mit dem innerstaatlichen Recht Daten an die zuständigen Behörden weitergegeben worden sind,

– wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der zuständigen Behörde angefragt wurden, vergangen ist (d. h. das Alter der Daten) sowie

– in welchen Fällen die Anfragen nach Daten ergebnislos geblieben sind.

Die Kommission hat nach diesem Artikel Statistiken von den Mitgliedstaaten angefordert und sie dabei ersucht, Angaben zu Fällen von einzelnen Datenanfragen zu machen. Dennoch weichen die übermittelten Statistiken in Umfang und Einzelheiten voneinander ab: Manche Mitgliedstaaten unterscheiden in ihren Antworten zwischen verschiedenen Arten der Nachrichtenübermittlung, manche geben das Alter der Daten zum Zeitpunkt der Anfrage an, andere wiederum haben nur unaufgeschlüsselte jährliche Statistiken übermittelt. Neunzehn Mitgliedstaaten[94] übermittelten statistische Daten zur Zahl der Datenanforderungen für 2009 und/oder 2008. Dazu zählten Irland, Griechenland und Österreich, wo Daten angefragt werden, obwohl bislang keine Umsetzungsmaßnahmen erlassen worden sind, sowie Deutschland und die Tschechische Republik, deren Gesetze zur Vorratsdatenspeicherung für nichtig erklärt wurden. Sieben Mitgliedstaaten, die die Richtlinie umgesetzt haben, haben keine Statistiken übermittelt, wenngleich Belgien eine Schätzung der Zahl der jährlichen Anfragen nach Telefoniedaten (300 000) übermittelt hat.

Zuverlässige quantitative und qualitative Daten sind für den Nachweis der Notwendigkeit und des Wertes von Sicherheitsmaßnahmen wie der Vorratsdatenspeicherung unerlässlich. Dies wurde 2006 in dem Aktionsplan zur Messung von Kriminalität und Strafverfolgung[95] anerkannt, der als Zielsetzung die Entwicklung von Methoden zur regelmäßigen Datenerfassung im Rahmen der Richtlinie und die Aufnahme der statistischen Daten in die Eurostat-Datenbank (sofern sie die Qualitätsstandards erfüllen) vorsah. Dieses Ziel konnte bislang nicht erfüllt werden, weil die meisten Mitgliedstaaten die Richtlinie erst in den vergangenen zwei Jahren vollständig umgesetzt und zudem die Quellen der statistischen Daten unterschiedlich ausgelegt haben. Die Kommission beabsichtigt, in ihrem künftigen Vorschlag zur Überarbeitung des Rechtsrahmens für die Vorratsdatenspeicherung neben der Überprüfung des Aktionsplans über Statistiken praktikable Mess- und Berichtsverfahren zu

---

93 Artikel-29-Datenschutzgruppe, Stellungnahme 2/2006 (WP 119), Bericht 01/2010.

94 Dänemark, Deutschland, Estland, Finnland, Griechenland, Frankreich, Irland, Lettland, Litauen, Malta, Niederlande, Österreich, Polen, Slowakei, Slowenien, Spanien, Tschechische Republik, Vereinigtes Königreich, Zypern.

95 Mitteilung der Kommission KOM(2006)437, Entwicklung einer umfassenden und kohärenten EU-Strategie zur Messung von Kriminalität und Strafverfolgung: EU-Aktionsplan 2006-2010.

unterbreiten, die eine transparente und aufschlussreiche Überwachung der Vorratsdatenspeicherung ermöglichen, ohne die Strafjustizsysteme und die Strafverfolgungsbehörden unzumutbar zu belasten.

4.8. Umsetzung in den EWR-Ländern

Rechtsvorschriften zur Vorratsdatenspeicherung existieren in Island, Liechtenstein und Norwegen[96].

4.9. Entscheidungen von Verfassungsgerichten zu Umsetzungsmaßnahmen

Das rumänische Verfassungsgericht, das deutsche Bundesverfassungsgericht und das tschechische Verfassungsgericht haben im Oktober 2009, März 2010 bzw. März 2011 die Gesetze zur Umsetzung der Richtlinie in ihren jeweiligen Staaten für verfassungswidrig und damit nichtig erklärt. Das rumänische Verfassungsgericht[97] hielt Eingriffe in Grundrechte für zulässig, wenn bestimmte Regeln respektiert werden und angemessene und ausreichende Garantien gegen potenzielle staatliche Willkür vorhanden sind. Jedoch befand es unter Berufung auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte[98] den Anwendungsbereich und Zweck der Umsetzungsmaßnahme für missverständlich, die Garantien für unzureichend und eine dauerhafte rechtliche Verpflichtung, sämtliche Verkehrsdaten sechs Monate lang auf Vorrat zu speichern, für nicht vereinbar mit den Rechten auf Privatsphäre und freie Meinungsäußerung nach Artikel 8 der Europäischen Menschenrechtskonvention.

Das deutsche Bundesverfassungsgericht[99] meint ebenfalls, die Vorratsdatenspeicherung rufe ein Gefühl des Überwachtwerdens hervor und könne die freie Ausübung der Grundrechte beeinträchtigen. Es erkennt zwar ausdrücklich an, dass die Vorratsdatenspeicherung für streng begrenzte Zwecke bei ausreichend hoher Datensicherheit nicht zwangsläufig gegen das deutsche Grundgesetz verstoße, betont jedoch, dass sie einen schwerwiegenden Eingriff in die Privatsphäre darstelle und daher nur unter besonders strengen Voraussetzungen zulässig sei, und dass eine Speicherungsfrist von sechs Monaten an der Obergrenze dessen liege, was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig sei (Randnr. 215). Daten sollten nur angefragt werden, wenn bereits ein Verdacht auf eine schwere Straftat bestehe oder Beweise für eine Gefährdung der öffentlichen Sicherheit vorlägen, während der Abruf von Daten für bestimmte Nachrichten (etwa im Zusammenhang mit seelischen oder sozialen Notlagen), die auf Vertraulichkeit angewiesen seien, ganz untersagt bleiben sollte. Zudem sollten die Daten verschlüsselt und ihre Verwendung transparent überwacht werden.

Das tschechische Verfassungsgericht[100] erklärte die Umsetzungsmaßnahmen mit der Begründung für nichtig, dass diese für Maßnahmen, die Grundrechte einschränken, nicht präzise und klar genug formuliert waren. Das Gericht kritisierte die Zweckbindung als unzureichend in Anbetracht des Ausmaßes und der Reichweite der Pflicht zur

---

96 In Island wurde die Richtlinie durch das Telekommunikationsgesetz 81/2003 (in der Fassung von April 2005) umgesetzt, in Liechtenstein durch das Telekommunikationsgesetz 2006. In Norwegen wurde das Umsetzungsgesetz am 5. April 2011 verabschiedet und liegt zur Königlichen Genehmigung vor.

97 Entscheidung Nr. 1258 des rumänischen Verfassungsgerichts vom 8. Oktober 2009.

98 EGMR, Rotaru gegen Rumänien, 2000, Sunday Times gegen Vereinigtes Königreich, 1979 und Fürst Hans-Adam von Liechtenstein gegen Rumänien, 2001.

99 Bundesverfassungsgericht, 1 BvR 256/08, Randnrn. 1–345.

100 Urteil des tschechischen Verfassungsgerichts vom 22. März 2011 zu Gesetz Nr. 127/2005 und Erlass Nr. 485/2005, siehe insbesondere Randnrn. 45-48, 50-51 und 56.

Vorratsdatenspeicherung. Darüber hinaus stellte es fest, dass die Definition der zuständigen Behörden, denen der Zugang zu und die Verwendung von gespeicherten Daten gestattet ist, sowie die Zugangs- und Verwendungsverfahren in den Umsetzungsvorschriften nicht klar genug waren, um die Integrität und Vertraulichkeit der Daten garantieren zu können. Der einzelne Bürger hätte dadurch keine ausreichende Gewähr und keinen ausreichenden Schutz vor einen Machtmissbrauch der öffentlichen Behörden. Das Gericht brachte keine Einwände gegen die Richtlinie selbst vor. Es erklärte, dass die Tschechische Republik ausreichenden Ermessensspielraum gehabt hätte, um die Richtlinie verfassungskonform umzusetzen. Allerdings bezweifelte es in einem *obiter dictum* die Notwendigkeit, Wirksamkeit und Angemessenheit der Speicherung von Verkehrsdaten angesichts der neuen kriminellen Methoden, beispielsweise der Verwendung anonymer SIM-Karten.

Die drei Mitgliedstaaten erwägen nun, wie sie die Richtlinie erneut umsetzen können. Mit der Vorratsdatenspeicherung befassten bzw. befassen sich auch die Verfassungsgerichte Bulgariens, das eine Überarbeitung der Umsetzungsmaßnahme für notwendig befand, Zyperns, das richterliche Anordnungen im Rahmen der Umsetzungsmaßnahme für verfassungswidrig erklärte, und Ungarns, wo eine Verfassungsbeschwerde wegen der fehlenden Zweckbegrenzung der Datenverarbeitung in der Umsetzungsmaßnahme anhängig ist.[101]

Die Kommission wird die durch die einzelstaatliche Rechtsprechung aufgeworfenen Fragen in ihrem künftigen Vorschlag zur Überarbeitung des Rechtsrahmens für die Vorratsdatenspeicherung berücksichtigen.

4.10. Durchsetzung der Richtlinie

Die Kommission erwartet, dass die Mitgliedstaaten, die die Richtlinie noch nicht vollständig umgesetzt haben bzw. ihre vom Verfassungsgericht für nichtig erklärten Umsetzungsmaßnahmen noch nicht ersetzt haben, dies so bald wie möglich tun werden. Andernfalls behält sich die Kommission das Recht vor, von ihren Befugnissen nach den EU-Verträgen Gebrauch zu machen. Der Gerichtshof hat in Urteilen gegen zwei Mitgliedstaaten, die die Richtlinie bisher nicht umgesetzt haben (Österreich und Schweden), festgestellt, dass diese gegen ihre Verpflichtungen aus dem EU-Recht verstoßen haben[102]. Im April 2011 beschloss die Kommission, erneut gegen Schweden vor Gericht Klage zu erheben, weil das Land dem Urteil in der Rechtssache C-185/09 nicht nachgekommen ist, und beantragte die Verhängung eines Zwangsgeldes gemäß Artikel 260 des Vertrags über die Arbeitsweise der Europäischen Union, nachdem das schwedische Parlament die Verabschiedung der Umsetzungsvorschriften um 12 Monate aufgeschoben hatte. Die Kommission verfolgt die Lage in Österreich aufmerksam. Das Land hat die baldige Verabschiedung von Umsetzungsmaßnahmen angekündigt.

---

101 Oberstes Verwaltungsgericht Bulgariens, Entscheidung Nr. 13627 vom 11. Dezember 2008; Oberster Gerichtshof Zyperns in den Beschwerdesachen Nr. 65/2009, 78/2009, 82/2009 und 15/2010-22/2010, 1. Februar 2011; die ungarische Verfassungsbeschwerde wurde von der Hungarian Civil Liberties Union (Társaság a Szabadságjogokér) am 2. Juni 2008 eingereicht.

102 Rechtssache C-189/09 bzw. Rechtssache C-185/09.

5. DIE ROLLE VON AUF VORRAT GESPEICHERTEN DATEN IN DER STRAFJUSTIZ UND DER STRAFVERFOLGUNG

In diesem Abschnitt sind die von den Mitgliedstaaten in ihren Beiträgen zur Bewertung beschriebenen Funktionen von gespeicherten Daten zusammengefasst.

5.1. Menge der gespeicherten Daten, zu denen zuständige nationale Behörden Zugang hatten

Sowohl das Volumen des Fernmeldeverkehrs als auch das der Zugangsanfragen für Verkehrsdaten nehmen zu. Aus den von 19 Mitgliedstaaten für 2008 und/oder 2009 übermittelten Statistiken geht hervor, dass EU-weit jährlich über 2 Millionen Zugangsanfragen für Daten eingingen, wobei zwischen den Mitgliedstaaten erhebliche Unterschiede bestehen, die von weniger als 100 pro Jahr (Zypern) bis zu über 1 Million (Polen) reichen. Nach den von zwölf Mitgliedstaaten für 2008 oder 2009 übermittelten Angaben zur Art der angefragten Daten stellten Mobilfunkdaten die am häufigsten angefragte Datenart dar (vgl. Tabellen 5, 8 und 12). Aus den Statistiken geht nicht der genaue Zweck der einzelnen Anfragen hervor. Die Tschechische Republik, Lettland und Polen erklärten, im Falle von Mobilfunkdaten müssten die zuständigen Behörden dieselbe Anfrage an jeden der großen Mobilfunkbetreiber richten, weshalb die tatsächliche Zahl der Anfragen pro Fall wesentlich niedriger sei, als die Statistiken vermuten ließen.

Für diese Abweichungen gibt es keine offensichtliche Erklärung, wenngleich die Einwohnerzahl, die Trends in der Entwicklung der Kriminalität, Zweckbindungen und Bedingungen für den Zugang sowie die Kosten des Datenerwerbs gewisse Einflussfaktoren darstellen.

5.2. Alter von gespeicherten Daten, zu denen Zugang gewährt wurde

Die von neun Mitgliedstaaten[103] für 2008 übermittelten Statistiken (siehe Zusammenfassung in Tabelle 5 und weitere Einzelheiten im Anhang) zeigen, dass rund 90 Prozent der Daten, zu denen die zuständigen Behörden Zugang hatten, bei der (ersten) Anfrage höchstens sechs Monate und rund 70 Prozent höchstens drei Monate alt waren.

Tabelle 5: Übersicht über das Alter von gespeicherten Daten, zu denen in neun Mitgliedstaaten, die Statistiken übermittelt haben, Zugang gewährt wurde, aufgeschlüsselt nach Art der Daten, 2008

Alter	*Telefonfestnetz*	*Mobilfunk*	*Internetdaten*	*Aggregat*
weniger als 3 Monate alt	61%	70%	56%	67%
3–6 Monate alt	28%	18%	19%	19%
6–12 Monate alt	8%	11%	18%	12%
über 1 Jahr alt	3%	1%	7%	2%

[103] Dänemark, Estland, Irland, Lettland, Malta, Spanien, Tschechische Republik, Vereinigtes Königreich und Zypern.

Den meisten Mitgliedstaaten zufolge werden gespeicherte Daten, die älter als drei oder gar sechs Monate sind, seltener verwendet, können aber entscheidend sein, wobei tendenziell drei Kategorien zu unterscheiden sind. Erstens werden internetbezogene Daten in strafrechtlichen Ermittlungen in der Regel später angefordert als andere Formen von Beweismitteln. Aus der Analyse von Festnetz- und Mobilfunkdaten ergeben sich häufig Hinweise, die zu weiteren Anfragen nach älteren Daten führen. Wird etwa bei einer Ermittlung ein Name aufgrund von Festnetz- oder Mobilfunkdaten festgestellt, möchten die Ermittler möglicherweise die Internetprotokoll-Adresse (IP-Adresse), die diese Person benutzt, identifizieren, um anhand dieser IP-Adresse zu ermitteln, zu wem die Person in einem bestimmten Zeitraum Kontakt hatte. In einem solchen Szenario fragen die Ermittler wahrscheinlich Daten an, anhand derer auch der Nachrichtenverkehr mit anderen IP-Adressen zurückverfolgt werden kann und die Personen, die diese IP-Adressen verwendet haben, identifiziert werden können.

Zweitens stützen sich die Ermittlungen bei besonders schweren Straftaten, Serienstraftaten, organisierter Kriminalität und Terroranschlägen oft auf ältere Daten, aus denen hervorgeht, wie lange die Straftaten vorbereitet wurden, um kriminelle Verhaltensmuster und die Beziehungen zwischen Tatbeteiligten zu erkennen und den Tatvorsatz festzustellen. Aktivitäten im Zusammenhang mit komplexen Finanzdelikten werden häufig erst nach mehreren Monaten aufgedeckt. Drittens haben die Mitgliedstaaten in Ausnahmefällen auch Telekommunikationsdaten angefragt, die in anderen Mitgliedstaaten gespeichert sind, die diese Daten in der Regel nur mit richterlicher Genehmigung im Rahmen eines von einem Richter des anfragenden Mitgliedstaats übermittelten Rechtshilfeersuchens freigeben können. Diese Art der Rechtshilfe kann sich als langwierig erweisen, was wiederum erklärt, weshalb einige der angefragten Daten in diesen Fällen über sechs Monate alt waren.

5.3. Grenzüberschreitende Anfragen nach gespeicherten Daten

Bei strafrechtlichen Ermittlungen und Strafverfolgungsmaßnahmen kann es um Beweismittel oder Zeugen aus mehr als einem Mitgliedstaat oder um Vorkommnisse gehen, die sich in mehr als einem Mitgliedstaat ereignet haben. Nach den von den Mitgliedstaaten übermittelten Statistiken betraf weniger als 1 % aller Anfragen Daten, die in einem anderen Mitgliedstaat gespeichert waren. Die Strafverfolgungsbehörden gaben an, dass sie lieber Anfragen an inländische Betreiber richten, die die benötigten Daten möglicherweise gespeichert haben, als ein unter Umständen zeitaufwendiges Rechtshilfeersuchen einzuleiten, bei dem nicht garantiert ist, dass Zugang zu den Daten gewährt wird. Der Rahmenbeschluss 2006/960/JI über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten[104], in dem die Fristen für die Bereitstellung von Informationen auf Ersuchen eines anderen Mitgliedstaats festgelegt sind, ist hier nicht anwendbar, weil auf Vorrat gespeicherte Daten als durch Zwangsmaßnahmen erlangte Information gelten und somit nicht in den Anwendungsbereich des Beschlusses fallen. Allerdings haben weder ein Mitgliedstaat noch eine Strafverfolgungsbehörde eine weitere Erleichterung dieses grenzüberschreitenden Austauschs gefordert.

---

[104] Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, ABl. L 386 vom 29.12.2006, S. 89–100 und ABl. L 200 vom 1.8.2007, S. 637–648.

5.4. Wert von gespeicherten Daten für strafrechtliche Ermittlungen und Strafverfolgungsmaßnahmen

Wenngleich die absolute Zahl der gemeldeten Datenanfragen nicht unbedingt den Wert der Daten in den einzelnen strafrechtlichen Ermittlungen widerspiegelt, haben die Mitgliedstaaten im Allgemeinen berichtet, dass die Vorratsdatenspeicherung zur Verhütung und Bekämpfung von Kriminalität einschließlich des Opferschutzes und des Freispruchs von Unschuldigen in Strafverfahren zumindest wertvoll, in manchen Fällen sogar unverzichtbar sei.[105] Verurteilungen stützen sich auf Geständnisse, Zeugenaussagen oder forensische Beweise. Den Berichten zufolge haben sich auf Vorrat gespeicherte Verkehrsdaten als notwendig für die Kontaktaufnahme zu Zeugen, die andernfalls nicht identifiziert worden wären, sowie den Beweis von bzw. Hinweise auf Mittäterschaft bei Straftaten erwiesen. Einige Mitgliedstaaten[106] haben ferner angegeben, die Verwendung gespeicherter Daten habe dazu beigetragen, verdächtige Personen zu entlasten, ohne auf andere Überwachungsmethoden wie das Abhören von Telefongesprächen und Hausdurchsuchungen, die stärker in die Rechte der Betroffenen eingreifen, zurückgreifen zu müssen.

Es gibt keine EU-weite allgemeine Definition des Begriffs „schwere Straftat“ und dementsprechend auch keine EU-Statistiken zur Häufigkeit von schweren Straftaten oder von Ermittlungen oder Strafverfolgungsmaßnahmen im Zusammenhang mit schweren Straftaten, obwohl Daten über Kriminalität und die Justiz regelmäßig veröffentlicht werden. Aus den Berichten von den 19 Mitgliedstaaten, die für die Jahre 2009 und/oder 2008 Daten übermittelt haben, geht hervor, dass insgesamt etwa 2,6 Millionen Anfragen nach gespeicherten Daten gestellt wurden. Legt man die jüngsten verfügbaren Statistiken zur Kriminalität und Strafverfolgung in diesen 19 Mitgliedstaaten zugrunde, die sich nicht nur auf schwere Straftaten, sondern auf alle angezeigten Straftaten beziehen, so ergibt sich, dass im Durchschnitt jeder Polizeibeamte pro Jahr nur etwas mehr als zwei Anfragen stellt oder dass pro 100 registrierten Straftaten etwa 11 Anfragen gestellt werden.[107]

Aus den übermittelten Statistiken und Beispielen, in denen die Verwendung gespeicherter historischer Kommunikationsdaten mit der Zahl der Verurteilungen, Freisprüche, Verfahrenseinstellungen, und verhüteten Straftaten verknüpft wird, lässt sich eine Reihe von Schlüssen zur Rolle und zum Wert der gespeicherten Daten für strafrechtliche Ermittlungen ziehen.

Entwicklung von Beweisspuren

---

105 Die Tschechische Republik betrachtet die Vorratsdatenspeicherung Daten als in einer Vielzahl von Fällen völlig unverzichtbar; Ungarn meint, sie sei unverzichtbar für die reguläre Tätigkeit der Strafverfolgungsbehörden; Slowenien erklärt, ohne auf Vorrat gespeicherte Daten käme die Tätigkeit der Strafverfolgungsbehörden zum Erliegen; eine Polizeibehörde des Vereinigten Königreichs bezeichnete die Verfügbarkeit von Verkehrsdaten als absolut entscheidend für die Untersuchung der Bedrohungen durch Terrorismus und Schwerkriminalität.

106 Deutschland, Polen, Slowenien und das Vereinigte Königreich.

107 Im Jahr 2007 gab es in der EU-27 1,7 Millionen Polizeibeamte, davon 1,2 Millionen in den 19 Mitgliedstaaten, die Statistiken über Anfragen nach gespeicherten Daten übermittelt haben. Ferner registrierte die Polizei 2007 in der EU 29,2 Millionen Straftaten, davon 24 Millionen in den 19 Mitgliedstaaten, die Statistiken übermittelt haben (Quelle: Eurostat 2009).

Erstens ermöglichen auf Vorrat gespeicherte Daten die Entwicklung von Beweisspuren, die zu einer Straftat führen. Sie dienen dazu, die Aktivitäten und Verbindungen zwischen Verdächtigen zu erkennen oder andere Arten von Beweismitteln zu untermauern. Strafverfolgungsbehörden wie auch Angeklagte verwendeten vor allem Standortdaten, um die Anwesenheit von Verdächtigen an Tatorten auszuschließen und Alibis zu belegen. Dieses Beweismittel kann also bewirken, dass gegen Personen nicht weiter ermittelt wird und somit Nachforschungen, die stärker in die Rechte der Betroffenen eingreifen, überflüssig werden, oder zu Freisprüchen im Prozess führen. Belgien führt die Verurteilung im Fall des Tiger-Kidnappings eines Angestellten des Antwerpener Strafgerichts im Jahr 2008 an, bei der Standortdaten, die die Aktivitäten der Täter in drei verschiedenen Städten miteinander in Verbindung brachten, ausschlaggebend dafür waren, die Geschworenen von ihrer Täterschaft zu überzeugen. In einem anderen Fall, einem Mord im Zusammenhang mit einer Motorradgang im Jahr 2007, bewiesen Standortdaten der Handys der Täter, dass sie sich in Tatortgegend aufgehalten hatten, und führten zu einem Teilgeständnis.[108] Belgien, Irland und dem Vereinigten Königreich zufolge können bestimmte Straftaten im Zusammenhang mit der Kommunikation über das Internet nur unter Nutzung der Vorratsdatenspeicherung untersucht werden. So hinterlassen etwa Gewaltandrohungen in Chatrooms häufig keine anderen Spuren als die Verkehrsdaten im Cyberspace. Ähnliches gilt für über das Telefon begangene Straftaten. Ungarn und Polen führen einen Fall von Betrug zum Nachteil älterer Menschen an, bei dem sich die Täter Ende 2009 / Anfang 2010 telefonisch als kreditbedürftige Familienangehörige ausgaben und nur durch gespeicherte Telefoniedaten identifiziert werden konnten.

Einleitung strafrechtlicher Ermittlungen

Zweitens hat es Fälle gegeben, in denen forensische Beweise oder Augenzeugen fehlten und die einzige Möglichkeit zur Einleitung strafrechtlicher Ermittlungen im Rückgriff auf gespeicherte Daten bestand. Deutschland führt als Beispiel den Mord an einem Polizeibeamten an, bei dem der Angreifer im Fahrzeug des Opfers flüchtete und dieses dann stehen ließ. Es konnte festgestellt werden, dass er sich anschließend telefonisch ein anderes Fahrzeug besorgt hatte. Es gab weder forensische Beweise noch Augenzeugen, um den Mörder zu identifizieren. Die Behörden waren daher, um ermitteln zu können, auf die Verfügbarkeit dieser Verkehrsdaten angewiesen. In Fällen von sexuellem Missbrauch von Kindern über das Internet ist die Vorratsdatenspeicherung für erfolgreiche Ermittlungen unentbehrlich. Im Zusammenspiel mit anderen Ermittlungsmethoden ermöglichen gespeicherte Daten die Identifizierung der Nutzer von Inhalten, die Kindesmissbrauch darstellen[109], und unterstützen die Identifizierung und Rettung von minderjährigen Opfern. Die Tschechische Republik berichtet, ohne Zugang zu gespeicherten Internetdaten wäre es unmöglich gewesen, Ermittlungen im Rahmen der „Operation Vilma“ in einem Netzwerk von Nutzern und Verbreitern von Kinderpornografie aufzunehmen. Auf EU-Ebene wurde die Wirksamkeit der von Europol geführten Operation Rescue zum Schutz von Kindern vor Missbrauch dadurch beeinträchtigt, dass einige Mitgliedstaaten aufgrund fehlender Umsetzungsmaßnahmen zur Vorratsdatenspeicherung bei den Ermittlungen gegen Mitglieder

---

108 National Policing Improvement Agency (Vereinigtes Königreich), The Journal of Homicide and Major Incident Investigation, Band 5, Ausgabe 1, Frühjahr 2009, S. 39–51.

109 Durch das Projekt „Measurement and Analysis of P2P Activity Against Paedophile Content“ im Rahmen des Programms Safer Internet wurden genaue Informationen über pädophile Aktivitäten im Peer-to-Peer-System eDonkey gesammelt, mit deren Hilfe 178 000 Nutzer (von 89 Millionen überprüften Nutzern), die pädophile Inhalte angefordert hatten, identifiziert werden konnten.

eines umfangreichen internationalen Pädophilen-Netzwerks keine IP-Adressen, die unter Umständen bis zu einem Jahr alt sind, verwenden können.

Bei Ermittlungen im Bereich der Computerkriminalität ist eine IP-Adresse oft der erste Anhaltspunkt. Die Strafverfolgungsbehörden können durch den Abruf von Verkehrsdaten den einer IP-Adresse zuzuordnenden Teilnehmer ermitteln, bevor Sie entscheiden, ob strafrechtliche Ermittlungen einzuleiten sind. IP-Adressen können die Polizei außerdem in die Lage versetzen, potenzielle Opfer von Cyberangriffen zu warnen: Wenn es der Polizei gelungen ist, einen von Botnet-Betreibern benutzten Command-and-Control-Server zu beschlagnahmen, sind zunächst nur die mit diesem Server verknüpften IP-Adressen feststellbar. Durch Zugriff auf gespeicherte Daten kann die Polizei jedoch potenzielle Opfer, denen diese IP-Adressen zuzuordnen sind, identifizieren und warnen.

Auf Vorrat gespeicherte Daten als wesentlicher Bestandteil von Strafermittlungen

Drittens sind, obwohl die Strafverfolgungsbehörden und Gerichte in den meisten Mitgliedstaaten keine Statistiken darüber führen, welche Art von Beweismitteln für Verurteilungen oder Freisprüche ausschlaggebend waren, gespeicherte Daten wesentlicher Bestandteil der Strafermittlungen und Strafverfolgung in der EU. Einige Mitgliedstaaten erklären, dass sie nicht immer abgrenzen könnten, wie sich gespeicherte Daten auf den Erfolg von Ermittlungen und Strafverfolgungsmaßnahmen auswirken, weil die Gerichte alle vorgelegten Beweismittel in ihrer Gesamtheit würdigen und nur selten ein einzelnes Beweismittel für ausschlaggebend erachten.[110] Die Niederlande berichten, von Januar bis Juli 2010 seien historische Verkehrsdaten für 24 Gerichtsurteile von entscheidender Bedeutung gewesen. Finnland berichtet, dass sich in 56 % der 3405 Zugangsanfragen gespeicherte Daten als wichtig oder wesentlich für die Aufdeckung und/oder Verfolgung von Straftaten erwiesen haben. Das Vereinigte Königreich hat Daten übermittelt, die die Auswirkungen der Vorratsdatenspeicherung auf die Strafverfolgung zu quantifizieren versuchen, und berichtet, drei der Strafverfolgungsbehörden des Vereinigten Königreichs würden gespeicherte Daten in den meisten, wenn nicht gar in allen Ermittlungen, die zu einer Strafverfolgung oder Verurteilung führen, verwenden.

5.5. Technischer Fortschritt und der Einsatz von vorausbezahlten SIM-Karten

Die Strafverfolgung muss mit den technischen Entwicklungen Schritt halten, die benutzt werden, um Straftaten zu begehen oder Beihilfe dazu zu leisten. Die Vorratsdatenspeicherung zählt zu den Ermittlungswerkzeugen, die die Strafverfolgungsbehörden befähigen, Vielfalt, Umfang und Tempo der Herausforderungen der Kriminalität von heute auf überschaubare und kosteneffiziente Weise zu bewältigen. Eine Reihe immer gebräuchlicherer Formen der Kommunikation fällt nicht in den Anwendungsbereich der Richtlinie. So ermöglichen etwa Virtual Private Networks (VPNs) in Universitäten oder Großunternehmen, dass mehrere Benutzer gleichzeitig über ein einziges Gateway unter Verwendung derselben IP-Adresse auf das Internet zugreifen können. Allerdings wird gegenwärtig eine neue Technologie eingeführt, die zulässt, dass einzelnen VPN-Nutzern IP-Adressen zugeordnet werden.

[110] Belgien, Litauen und die Tschechische Republik.

Der Anteil der Mobilfunkbenutzer, die vorausbezahlte Dienste nutzen, schwankt innerhalb der EU. Einige Mitgliedstaaten haben angeführt, dass anonyme vorausbezahlte SIM-Karten, insbesondere wenn sie in einem anderen Mitgliedstaat erworben wurden, auch von in kriminelle Aktivitäten verwickelten Personen benutzt werden können, um eine Identifizierung in strafrechtlichen Ermittlungen zu vermeiden.[111] Sechs Mitgliedstaaten (Bulgarien, Dänemark, Griechenland, Italien, die Slowakei und Spanien) haben Maßnahmen getroffen, die eine Registrierung von vorausbezahlten SIM-Karten vorsehen. Diese und andere Mitgliedstaaten (Polen, Zypern und Litauen) haben sich für eine EU-weite Maßnahme eingesetzt, wonach die Nutzer von vorausbezahlten Diensten obligatorisch registriert werden sollen. Bislang wurden keine Nachweise für die Wirksamkeit der einzelstaatlichen Maßnahmen vorgelegt. Es wurde auf mögliche Einschränkungen hingewiesen, etwa in Fällen von Identitätsdiebstahl, beim Kauf von SIM-Karten durch Dritte oder beim Roaming mit in einem Drittland erworbenen SIM-Karten. Insgesamt ist die Kommission nicht davon überzeugt, dass in diesem Bereich auf EU-Ebene akuter Handlungsbedarf besteht.

6. AUSWIRKUNGEN DER VORRATSDATENSPEICHERUNG AUF BETREIBER UND VERBRAUCHER

6.1. Betreiber und Verbraucher

In einer an die Kommission gerichteten gemeinsamen Erklärung bezeichneten fünf große Branchenverbände die wirtschaftlichen Auswirkungen der Richtlinie auf kleinere Betreiber als erheblich oder enorm, weil die Richtlinie breiten Spielraum lasse.[112] Acht Betreiber übermittelten stark voneinander abweichende Schätzungen der mit der Einhaltung der Richtlinie verbundenen Investitions- und Betriebskosten. Die Angaben von vier Mitgliedstaaten zur Höhe der Kostenerstattungen für Betreiber (siehe Tabelle 6) bestätigen dies möglicherweise.

Einer vor der Umsetzung der Richtlinie in den meisten Mitgliedstaaten durchgeführten Studie zufolge belaufen sich die einem Internetprovider mit einer halben Million Kunden entstehenden Kosten für die Einrichtung eines Systems zur Vorratsdatenspeicherung im ersten Jahr auf schätzungsweise 375 240 EUR und die anschließenden monatlichen Betriebskosten auf 9 870 EUR[113], während die Kosten für die Einrichtung eines Datenabrufsystems auf 131 190 EUR und seine monatlichen Betriebskosten auf 28 960 EUR veranschlagt wurden. Allerdings befand das deutsche Bundesverfassungsgericht in seinem Urteil vom 2. März 2010, dass die Auferlegung der Speicherungspflicht „gegenüber den betroffenen Diensteanbietern typischerweise nicht übermäßig belastend“[114] wirke und auch nicht unverhältnismäßig in Bezug auf die finanziellen Lasten sei, die den Unternehmen durch die Speicherungspflicht erwachsen. Die Stückkosten der Vorratsdatenspeicherung sind umgekehrt proportional zur Größe des Betreibers und zum Normungsgrad der Interaktion mit den Betreibern im jeweiligen Mitgliedstaat.[115]

---

111 Schlussfolgerungen des Rates zur Bekämpfung der kriminellen Zwecken dienenden Nutzung der elektronischen Kommunikation und ihrer Anonymität.

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF

113 Wilfried Gansterer & Michael Ilger, Data Retention – The EU Directive 2006/24/EC from a Technological Perspective, Wien: Verlag Medien und Recht, 2008.

114 Bundesverfassungsgericht, 1 BvR 256/08 vom 2. März 2010, Randnr. 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx

Die meisten Betreiber konnten in ihrer Antwort zum Fragebogen der Kommission die Auswirkungen der Richtlinie auf den Wettbewerb, die Endverbraucherpreise oder Investitionen in neue Infrastrukturen und Dienste nicht quantifizieren.

Es gibt keine Hinweise auf quantifizierbare oder wesentliche Auswirkungen der Richtlinie auf die Verbraucherpreise für elektronische Kommunikationsdienste. Zu der im Jahr 2009 durchgeführten öffentliche Anhörung gab es keine Beiträge von Vertretern der Verbraucher. Aus einer in Deutschland im Auftrag einer Organisation der Zivilgesellschaft durchgeführten Umfrage geht hervor, dass Verbraucher unter bestimmten Umständen ihr Kommunikationsverhalten ändern und die Nutzung elektronischer Kommunikationsdienste vermeiden wollen[116], jedoch gibt es keine Bestätigung dafür, dass eine Verhaltensänderung in einem Mitgliedstaat oder in der EU tatsächlich stattgefunden hat.

Die Kommission beabsichtigt, die Auswirkungen künftiger Änderungen der Richtlinie auf die Wirtschaft und die Verbraucher zu bewerten, möglicherweise auch durch eine spezielle Eurobarometer-Umfrage zur öffentlichen Wahrnehmung.

6.2. Kostenerstattung

Die Richtlinie regelt nicht die Erstattung der Kosten, die den Betreibern infolge der Pflicht zur Vorratsdatenspeicherung entstehen. Diese Kosten lassen sich einstufen als:

(a) *Betriebsausgaben*, also Betriebskosten oder fortlaufende Ausgaben, die mit dem Betrieb eines Unternehmens oder einer Vorrichtung, eines Bauteils, eines Ausrüstungsgegenstands oder einer Anlage zusammenhängen, sowie

(b) *Investitionskosten*, also Aufwendungen, die zukünftige Nutzeffekte schaffen, oder die Kosten der Entwicklung und Bereitstellung nicht verbrauchbarer Bestandteile des Produkts oder Systems, die auch Personalkosten und Ausgaben für Anlagen wie Miete/Pacht und Versorgungsdienstleistungen einschließen können.

Alle Mitgliedstaaten erstatten in irgendeiner Form Kosten, wenn Daten im Rahmen eines gerichtlichen Strafverfahrens angefragt werden. Zwei Mitgliedstaaten berichteten, dass sie sowohl Betriebsausgaben als auch Investitionskosten erstatten. Sechs Mitgliedstaaten erstatten nur Betriebsausgaben. Andere Erstattungsregelungen wurden der Kommission nicht mitgeteilt. Einzelheiten sind der Tabelle 6 zu entnehmen.

Tabelle 6: Mitgliedstaaten, die Kosten erstatten

Mitgliedstaat	Betriebsausgaben	Investitionskosten	Jährliche Kostenerstattung (Mio. EUR)
Belgien	Ja	Nein	22 (2008)

[116] Die Umfrage wurde von Forsa im Auftrag des AK Vorratsdatenspeicherung durchgeführt. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

Bulgarien	Nein	Nein	-
Tschechische Republik	Nicht umgesetzt[117]		
Dänemark	Ja	Nein	-
Deutschland	Nicht umgesetzt		
Estland	Ja	Nein	-
Irland	Nein	Nein	-
Griechenland	Nein	Nein	-
Spanien	Nein	Nein	-
Frankreich	Ja	Nein	-
Italien	-	-	-
Zypern	Nein	Nein	-
Lettland	Nein	Nein	-
Litauen	Ja, auf begründeten Antrag.	Nein	-
Luxemburg	Nein	Nein	-
Ungarn	Nein	Nein	-
Malta	Nein	Nein	-
Niederlande	Ja	Nein	-
Österreich	Nicht umgesetzt		
Polen	Nein	Nein	-
Portugal	Nein	Nein	-
Rumänien	Nicht umgesetzt		
Slowenien	Nein	Nein	-
Slowakei	Nein	Nein	-
Finnland	Ja	Ja	1
Schweden	Nicht umgesetzt		
Vereinigtes Königreich	Ja	Ja	55 (gesamte Erstattung für die im Laufe von drei Jahren entstandenen Kosten)

Die vorstehende Tabelle lässt den Schluss zu, dass die Richtlinie ihr Ziel, gleiche Wettbewerbsbedingungen für Betreiber in der EU zu schaffen, nicht in vollem Umfang erreicht hat. Die Kommission wird unter besonderer Berücksichtigung kleiner und mittlerer Betreiber prüfen, wie eine einheitliche Erstattung der den Betreibern durch die Vorschriften zur Vorratsdatenspeicherung entstehenden Kosten erreicht werden kann, um die Hindernisse für das Funktionieren des Binnenmarktes auf ein Minimum zu reduzieren.

7. AUSWIRKUNGEN DER VORRATSDATENSPEICHERUNG AUF DIE GRUNDRECHTE

7.1. Das Grundrecht auf Privatsphäre und den Schutz personenbezogener Daten

Die Vorratsdatenspeicherung schränkt das Recht auf Privatleben und den Schutz personenbezogener Daten, die in der EU Grundrechte sind[118], ein. Eine solche Einschränkung

[117] Vor der Nichtigerklärung der tschechischen Umsetzungsmaßnahmen erstattete die Tschechische Republik sowohl die Betriebs- als auch die Investitionskosten. Nach Angaben der Tschechischen Republik wurden 2009 dafür insgesamt 6,8 Mio. EUR aufgewendet.

muss nach Artikel 52 Absatz 1 der Charta der Grundrechte „gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten“ unter Wahrung des Grundsatzes der Verhältnismäßigkeit achten sowie erforderlich sein und den von der EU anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer entsprechen. In der Praxis bedeutet dies, dass jede Einschränkung:[119]

(a) präzise und vorausschauend formuliert sein,

(b) zur Verwirklichung eines Ziels von allgemeinem Interesse oder zum Schutz der Rechte und Freiheiten Dritter erforderlich sein,

(c) in einem angemessenen Verhältnis zu dem angestrebten Ziel stehen sowie

(d) dem Wesensgehalt der einschlägigen Grundrechte Rechnung tragen muss.

Artikel 8 Absatz 2 der Europäischen Menschenrechtskonvention erkennt ebenfalls an, dass ein Eingriff einer Behörde in die Ausübung des Rechts auf Privatsphäre als notwendig für die nationale oder öffentliche Sicherheit oder zur Verhütung von Straftaten gerechtfertigt sein kann.[120] Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation und die Erwägungsgründe der Richtlinie über die Vorratsdatenspeicherung bekräftigen diese Grundsätze und untermauern den Ansatz der EU zur Vorratsdatenspeicherung.

Im Anschluss daran haben der Europäische Gerichtshof und der Europäische Gerichtshof für Menschenrechte in ihrer Rechtsprechung die Bedingungen entwickelt, die bei jeder Einschränkung des Rechts auf Privatsphäre erfüllt sein müssen. Diese Urteile sind für die Frage von Belang, ob die Richtlinie, insbesondere im Hinblick auf die Bedingungen für den Zugang zu und die Verwendung von auf Vorrat gespeicherten Daten, geändert werden muss.

Einschränkungen des Rechts auf Privatsphäre müssen präzise formuliert sein und Vorhersehbarkeit ermöglichen

In der Rechtssache Österreichischer Rundfunk urteilte der Europäische Gerichtshof, dass jeder gesetzlich vorgesehene Eingriff in die Privatsphäre so genau formuliert sein muss, „dass die Adressaten des Gesetzes ihr Verhalten einrichten können, … damit [er] dem Erfordernis der Vorhersehbarkeit genügt.“

Einschränkungen des Rechts auf Privatsphäre müssen notwendig sein und ein Mindestmaß an Garantien bieten

In der Rechtssache Copland gegen das Vereinigte Königreich, in der es um die staatliche Überwachung von Telefongesprächen, E-Mail Korrespondenz und Internetnutzung einer

---

118 Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union (ABl. C 83 vom 30.3.2010, S. 389) garantieren das Recht aller auf „Schutz der sie betreffenden personenbezogenen Daten“. Auch in Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (ABl. C 83 vom 30.3.2010, S. 1) ist das Recht aller auf „Schutz der sie betreffenden personenbezogenen Daten“ verankert.

119 Siehe die Grundrechts-Checkliste der Kommission für alle Legislativvorschläge in der Mitteilung der Kommission KOM(2010) 573/4, „Strategie zur wirksamen Umsetzung der Charta der Grundrechte durch die Europäische Union.“

120 Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (ETS Nr. 5), Europarat, 4.11.1950.

Person ging, befand der Europäische Gerichtshof für Menschenrechte, dass eine solche Einschränkung des Rechts auf Privatsphäre nur dann für notwendig erachtet werden könne, wenn sie auf einschlägigen innerstaatlichen Rechtsvorschriften beruhe.[121] In der Rechtssache S. und Marper gegen das Vereinigte Königreich, die die Speicherung von DNA-Profilen und Fingerabdrücken von Personen nach Freispruch oder Einstellung des Strafverfahrens vor einer Verurteilung betraf, entschied der EGMR, dass eine solche Einschränkung des Rechts auf Privatsphäre nur dann gerechtfertigt sein könne, wenn sie gesellschaftlich dringend notwendig sei, wenn sie im Verhältnis zu dem verfolgten Ziel stehe und wenn die von der betreffenden Behörde vorgebrachten Gründe relevant und ausreichend seien.[122] Nach den Grundprinzipien des Datenschutzes müsse die Vorratsdatenspeicherung in einem angemessenen Verhältnis zum Zweck der Datensammlung stehen und die Speicherdauer zeitlich begrenzt sein.[123] Für das Abhören von Telefongesprächen, die heimliche Überwachung und die verdeckte Informationssammlung seien klare und detaillierte Vorschriften über den Umfang und die Anwendung der Maßnahmen sowie ein Mindestmaß an Garantien, insbesondere in Bezug auf Dauer, Lagerung, Verwendung, Zugang Dritter, Verfahren zur Wahrung von Integrität und Vertraulichkeit der Daten und Verfahren für ihre Vernichtung, von zentraler Bedeutung, um einen ausreichenden Schutz gegen die Gefahr des Missbrauchs und der Willkür zu gewährleisten.

Einschränkungen des Rechts auf Privatsphäre müssen in einem angemessenen Verhältnis zum Gemeinwohl stehen

Ebenso befand der Europäische Gerichtshof in seinem Urteil in der Rechtssache Schecke & Eifert betreffend die Veröffentlichung aller Empfänger von Agrarbeihilfen im Internet[124], dass der EU-Gesetzgeber offenbar keine angemessenen Maßnahmen getroffen habe, um eine ausgewogene Gewichtung zwischen der Achtung des Wesensgehalts des Rechts auf Privatsphäre und der von der EU anerkannten dem Gemeinwohl dienenden Zielsetzung (Transparenz) zu erreichen. Insbesondere stellte der Gerichtshof fest, dass der Gesetzgeber keine anderen Modalitäten erwogen habe, die im Einklang mit dem Zweck gestanden, zugleich aber weniger stark in das Recht der Empfänger auf Achtung ihres Privatlebens und auf Schutz ihrer personenbezogenen Daten eingegriffen hätten. Der Gerichtshof entschied folglich, der Gesetzgeber habe die Grenzen der Verhältnismäßigkeit überschritten, da sich „Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das absolut Notwendige beschränken müssen."

7.2. Kritik am Prinzip der Vorratsdatenspeicherung

Eine Reihe von Organisationen der Zivilgesellschaft hat gegenüber der Kommission schriftlich den Standpunkt vertreten, die Vorratsdatenspeicherung sei im Prinzip eine ungerechtfertigte und unnötige Einschränkung des Rechtes des Einzelnen auf Privatsphäre. Sie betrachten die „generelle und wahllose" Vorratsspeicherung von Telekommunikations-Verkehrs-, Standort- und Teilnehmerdaten Einzelner ohne deren Einwilligung als unzulässige Einschränkung von Grundrechten. In einem Rechtsstreit einer Bürgerrechtsorganisation vor

---

121 Copland gegen das Vereinigte Königreich, Urteil des Europäischen Gerichtshofs für Menschenrechte, Straßburg, 3.4.2007, S. 9.

122 Marper gegen Vereinigtes Königreich, Urteil des Europäischen Gerichtshofs für Menschenrechte, Straßburg, 4.12.2008, S. 31.

123 Marper, S. 30.

124 Rechtssache C–92/09 Volker und Markus Schecke GbR gegen Land Hessen und C–93/09 Eifert gegen Land Hessen und Bundesanstalt für Landwirtschaft und Ernährung, 9.11.2010.

den Gerichten eines Mitgliedstaats (Irland) ist davon auszugehen, dass die Frage der Rechtmäßigkeit der Richtlinie dem Europäischen Gerichtshof vorgelegt wird.[125] Auch der Europäische Datenschutzbeauftragte hat Zweifel an der Notwendigkeit der Maßnahme geäußert.

7.3. Forderungen nach mehr Datensicherheit und strengeren Datenschutzvorschriften

Die Artikel-29-Datenschutzgruppe argumentiert in ihrem Bericht über die zweite Durchsetzungsmaßnahme, dass die Speicherung von Verkehrsdaten an sich die Gefahr von Verletzungen der Vertraulichkeit der Kommunikation und des Rechtes auf freie Meinungsäußerung berge. Sie kritisiert bestimmte Aspekte der Umsetzung in den Mitgliedstaaten, insbesondere die Datenaufzeichnung, die Speicherungsfristen, die Art der gespeicherten Daten und die Maßnahmen zur Datensicherheit. Die Datenschutzgruppe berichtet von Fällen, in denen außerhalb des Anwendungsbereichs der Richtlinie liegende Einzelheiten über den Inhalt von über das Internet übermittelten Nachrichten, etwa die IP-Adresse des Adressaten und die URL-Internetadresse von Websites, die Kopfzeilen von E-Mail-Mitteilungen oder die Liste aller Empfänger in der „cc"-Zeile, gespeichert wurden. Sie fordert daher eine Klarstellung, dass die in der Richtlinie vorgesehenen Datenkategorien als erschöpfend anzusehen sind und den Betreibern keine zusätzlichen Pflichten zur Vorratsdatenspeicherung auferlegt werden dürfen.

Der Europäische Datenschutzbeauftragte hat erklärt, die Richtlinie habe „die Harmonisierung der nationalen Rechtsvorschriften verfehlt" und die Verwendung der auf Vorrat gespeicherten Daten sei nicht strikt auf die Bekämpfung von schweren Straftaten begrenzt.[126] Nach seiner Auffassung sollte ein EU-Rechtsinstrument, das Vorschriften zur obligatorischen Vorratsspeicherung von Daten enthält und dessen Notwendigkeit nachgewiesen wurde, auch Vorschriften über den Zugang und die Weiterverwendung von Daten durch die Strafverfolgungsbehörden enthalten. Er hat die EU aufgerufen, einen umfassenden Rechtsrahmen zu verabschieden, der nicht nur den Betreibern Verpflichtungen zur Vorratsspeicherung von Daten auferlegt, sondern auch regelt, wie die Mitgliedstaaten die Daten für die Strafverfolgung verwenden, um so „Rechtssicherheit für die Bürger" zu schaffen.

Die Datenschutzbehörden haben generell argumentiert, dass die Vorratsdatenspeicherung an sich die Gefahr einer möglichen Verletzung der Privatsphäre berge, der die Richtlinie nicht auf EU-Ebene begegne. Stattdessen verpflichte sie die Mitgliedstaaten, die Einhaltung der innerstaatlichen Datenschutzvorschriften zu gewährleisten. Wenngleich es keine konkreten Beispiele für schwere Verletzungen der Privatsphäre gibt, bleibt das Risiko von Verstößen gegen die Datensicherheit bestehen und kann im Zuge des technischen Fortschritts und neuer Trends bei den Kommunikationsformen – unabhängig davon, ob Daten zu geschäftlichen Zwecken oder zu Sicherheitszwecken, innerhalb oder außerhalb der EU gespeichert werden – noch zunehmen, wenn keine weiteren Sicherheitsvorkehrungen getroffen werden.

---

125 Am 5. Mai 2010 entsprach der irische High Court dem Antrag von Digital Rights Ireland Limited, den Europäischen Gerichtshof nach Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union um Vorabentscheidung zu ersuchen.

126 Rede von Peter Hustinx auf der Konferenz „Taking on the Data Retention Directive", 3. Dezember 2010.

8. SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

In diesem Bericht wurde eine Reihe von Vorteilen und Schwächen des in der EU bestehenden Systems zur Vorratsdatenspeicherung hervorgehoben. Die EU hat die Richtlinie zu einer Zeit, in der verstärkt vor drohenden Terroranschlägen gewarnt wurde, erlassen. Die von der Kommission geplante Folgenabschätzung bietet die Gelegenheit, die Vorratsdatenspeicherung in der EU auf ihre Notwendigkeit und Verhältnismäßigkeit zu prüfen und sie unter Berücksichtigung und im Interesse der inneren Sicherheit, des reibungslosen Funktionierens des Binnenmarktes sowie der Achtung der Privatsphäre und des Grundrechtes auf Schutz personenbezogener Daten zu überarbeiten. In dem Vorschlag der Kommission zur Überarbeitung des Rechtsrahmens für die Vorratsdatenspeicherung sollten die folgenden Schlussfolgerungen und Empfehlungen berücksichtigt werden.

8.1. Die EU sollte die Vorratsdatenspeicherung als Sicherheitsmaßnahme unterstützen und regeln

Most Member States take the view that EU rules on data retention remain necessary as a tool for law enforcement, the protection of victims and the criminal justice systems. The evidence, in the form of statistics and examples, provided by Member States is limited in some respects but nevertheless attests to the very important role of retained data for criminal investigation. These data provide valuable leads and evidence in the prevention and prosecution of crime and ensuring criminal justice. Their use has resulted in convictions for criminal offences which, without data retention, might never have been solved. It has also resulted in acquittals of innocent persons. Harmonised rules in this area should ensure that data retention is an effective tool in combating crime, that industry has legal certainty in a smoothly functioning internal market, and that the high levels of respect for privacy and the protection of personal data are applied consistently throughout the EU.

8.2. Transposition has been uneven

Die meisten Mitgliedstaaten halten die EU-Rechtsvorschriften zur Vorratsdatenspeicherung nach wie vor für ein notwendiges Instrument für die Strafverfolgung, den Opferschutz und die Strafjustiz. Die Belege in Form der von den Mitgliedstaaten übermittelten Statistiken und Beispiele sind zwar in mancher Hinsicht unzulänglich, bestätigen aber dennoch die äußerst wichtige Rolle von auf Vorrat gespeicherten Daten für strafrechtliche Ermittlungen. Diese Daten liefern wertvolle Anhaltspunkte und Beweismittel für die Verhütung und Verfolgung von Straftaten und die Strafjustiz. Ihre Verwendung hat zu Verurteilungen von Straftätern bei Straftaten geführt, die ohne die Vorratsdatenspeicherung möglicherweise nie aufgeklärt worden wären. Sie hat außerdem zu Freisprüchen von Unschuldigen geführt. Harmonisierte Vorschriften in diesem Bereich sollten gewährleisten, dass die Vorratsdatenspeicherung ein wirksames Instrument zur Bekämpfung von Kriminalität ist, dass für die Wirtschaft in einem reibungslos funktionierenden Binnenmarkt Rechtssicherheit besteht und dass die strengen Vorgaben zur Achtung der Privatsphäre und zum Schutz personenbezogener Daten EU-weit einheitlich angewandt werden.

8.3. Die Umsetzung erfolgte uneinheitlich

In 22 Mitgliedstaaten sind Umsetzungsmaßnahmen in Kraft. Der erhebliche Spielraum, den die Mitgliedstaaten nach Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation für den Erlass von Rechtsvorschriften zur Vorratsdatenspeicherung haben, macht die Bewertung der Richtlinie über die Vorratsdatenspeicherung höchst problematisch.

Zwischen den Umsetzungsmaßnahmen bestehen beträchtliche Unterschiede im Hinblick auf die Zweckbindung, den Zugang zu Daten, die Speicherungsfristen, den Datenschutz und die Datensicherheit sowie die Statistiken. Drei Mitgliedstaaten verstoßen gegen die Richtlinie, seit ihre Umsetzungsmaßnahmen von ihren jeweiligen Verfassungsgerichten für nichtig erklärt wurden. In zwei weiteren Mitgliedstaaten steht die Umsetzung noch aus. Die Kommission wird nach wie vor alle Mitgliedstaaten bei der wirksamen Umsetzung der Richtlinie unterstützen. Gleichzeitig wird sie auch weiterhin ihrer Aufgabe nachkommen, EU-Rechtsvorschriften – nötigenfalls durch Vertragsverletzungsverfahren als letztes Mittel – durchzusetzen.

8.4. Die Richtlinie hat weder die Herangehensweise an die Vorratsdatenspeicherung vollständig harmonisiert noch gleiche Wettbewerbsbedingungen für Betreiber geschaffen

Die Richtlinie hat dafür gesorgt, dass inzwischen in den meisten Mitgliedstaaten Daten auf Vorrat gespeichert werden. Sie garantiert selbst nicht, dass auf Vorrat gespeicherte Daten in voller Übereinstimmung mit dem Recht auf Privatsphäre und Schutz personenbezogener Daten gespeichert, abgerufen und verwendet werden. Es obliegt den Mitgliedstaaten, diese Rechte auch weiterhin aufrechtzuerhalten. Ziel der Richtlinie war lediglich eine teilweise Harmonisierung der Herangehensweise an die Vorratsdatenspeicherung. Daher ist das Fehlen eines gemeinsamen Ansatzes – sei es in Bezug auf konkrete Vorschriften der Richtlinie wie etwa die Zweckbindung oder Speicherungsfristen oder in Bezug auf Aspekte außerhalb ihres Anwendungsbereichs wie die Kostenerstattung – nicht verwunderlich. Doch auch über die von der Richtlinie ausdrücklich vorgesehenen Abweichmöglichkeiten hinaus hat die unterschiedliche Anwendung der Vorratsdatenspeicherung in den Mitgliedstaaten die Betreiber vor erhebliche Schwierigkeiten gestellt.

8.5. Die Kostenerstattung für Betreiber bedarf einer Vereinheitlichung

Es besteht nach wie vor keine Rechtssicherheit für die Wirtschaft. Die Pflicht zur Vorratsspeicherung und zum Abruf von Daten stellt vor allem für kleinere Betreiber einen erheblichen Kostenfaktor dar. Zudem sind die Betreiber in den einzelnen Mitgliedstaaten in unterschiedlichem Maße davon betroffen, auch im Hinblick auf die Kostenerstattung, wenngleich es keine Anzeichen dafür gibt, dass der Telekommunikationssektor insgesamt durch die Richtlinie beeinträchtigt worden ist. Die Kommission wird Möglichkeiten für eine einheitliche Kostenerstattung für die Betreiber erwägen.

8.6. Gewährleistung der Verhältnismäßigkeit des gesamten Prozesses von Speicherung, Abruf und Verwendung der Daten

Die Kommission wird sicherstellen, dass jeder künftige Vorschlag zur Vorratsdatenspeicherung dem Grundsatz der Verhältnismäßigkeit Rechnung trägt, dem Ziel der Bekämpfung von schwerer Kriminalität und Terrorismus entspricht und nicht über das dazu Erforderliche hinausgeht. Sie wird respektieren, dass sich Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das Notwendige beschränken müssen. Sie wird sorgfältig prüfen, wie sich eine strengere Regulierung der Speicherung und Verwendung von Verkehrsdaten sowie des Zugangs zu ihnen auf die Wirksamkeit und Effizienz des Strafjustizsystems und der Strafverfolgung, die Privatsphäre und die Kosten der öffentlichen Verwaltung und der Betreiber auswirkt. Insbesondere sollten bei der Folgenabschätzung folgende Bereiche untersucht werden:

- Vereinheitlichung der Zweckbindung der Vorratsdatenspeicherung sowie der Arten von Straftaten, bei denen der Zugang zu und die Verwendung von gespeicherten Daten zulässig sind

- stärkere Harmonisierung und gegebenenfalls Verkürzung der obligatorischen Speicherungsfristen

- Gewährleistung einer unabhängigen Überwachung von Zugangsanfragen und der in allen Mitgliedstaaten geltenden Vorratsspeicherungs- und Zugangsregelung

- Festlegung, welche Behörden Zugang zu Daten haben dürfen

- Verringerung der Zahl der Kategorien von auf Vorrat zu speichernden Daten

- Anleitung im Hinblick auf technische und organisatorische Sicherheitsmaßnahmen für den Zugang zu Daten einschließlich der Übergabeverfahren

- Anleitung zur Verwendung von Daten einschließlich der Verhütung von Data Mining sowie

- Entwicklung praktikabler Mess- und Berichtsverfahren, um Anwendungsvergleiche und die Bewertung eines künftigen Rechtsakts zu erleichtern.

Die Kommission wird auch prüfen, ob – und falls ja, wie – ein EU-weites Konzept für die Datensicherung die Vorratsdatenspeicherung ergänzen könnte.

Mit Blick auf die Grundrechts-Checkliste und den Ansatz für das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht[127] wird die Kommission jeden dieser Bereiche nach dem Grundsätzen der Verhältnismäßigkeit und dem Erfordernis der Vorhersehbarkeit prüfen. Sie wird auch die Kohärenz mit der laufenden Überprüfung des EU-Rahmens für den Datenschutz[128] gewährleisten.

8.7. Weitere Schritte

Die Kommission wird in Anbetracht dieser Bewertung eine Überarbeitung des derzeitigen Rechtsrahmens für die Vorratsdatenspeicherung vorschlagen. Sie wird in Abstimmung mit den Strafverfolgungsbehörden, der Justiz, Wirtschafts- und Verbraucherverbänden, Datenschutzbehörden und Organisationen der Zivilgesellschaft eine Reihe von Optionen erarbeiten. Sie wird die öffentliche Wahrnehmung der Vorratsdatenspeicherung und ihre Auswirkungen auf das Verhalten weiter untersuchen. Diese Ergebnisse werden in eine Folgenabschätzung für die erkannten politischen Optionen, die die Grundlage für den Vorschlag der Kommission bilden werden, einfließen.

---

127 Siehe den obigen Verweis auf die Mitteilung zur Umsetzung der Charta der Grundrechte; „Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht“, KOM(2010)385 vom 20.7.2010.

128 KOM(2010) 609 vom 4.11.2010.

Anhang: Weitere Statistiken zur Vorratsspeicherung von Verkehrsdaten

Hinweise zum Anhang:

1. Alter der Daten bezeichnet den Zeitraum zwischen dem Tag, an dem die Daten gespeichert wurden, und dem Tag, an dem die zuständige Behörde um Übermittlung der Daten ersucht hat.

2. Internetdaten sind Daten über Internetzugang, Internet-E-Mail- und Internettelefonie.

3. Die Statistiken für die Tschechische Republik, Lettland und Polen stehen unter Vorbehalt (siehe Abschnitt 5.1).

Von den Mitgliedstaaten für 2008 übermittelte Statistiken

Tabelle 7: Anfragen nach gespeicherten Verkehrsdaten nach Alter, 2008									
Alter der angefragten Daten (Monate) / Mitgliedstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Gesamt**
Belgien	Keine Angaben übermittelt								
Bulgarien	Keine Angaben übermittelt								
Tschechische Republik	102691	18440	10110	319	0	0	0	0	131560
Dänemark	2669	672	185	37	23	2	7	4	3599
Deutschland	9363	2336	985	0	0	0	0	0	12684
Estland	2773	733	157	827	0	0	0	0	4490
Irland	8981	2016	936	1855	90	85	78	54	14095
Griechenland	Keine Aufschlüsselung nach Alter übermittelt								584
Spanien	22629	15868	10298	4783	0	0	0	0	53578
Frankreich	Keine Aufschlüsselung nach Alter übermittelt								**503437**
Italien	Keine Angaben übermittelt								
Zypern	30	4	0	0	0	0	0	0	34
Lettland	10539	2739	1368	1211	597	438	0	0	16892
Litauen	55735	23817	5251	512	0	0	0	0	85315
Luxemburg	Keine Angaben übermittelt								
Ungarn	Keine Angaben übermittelt								
Malta	810	59	0	0	0	0	0	0	869
Niederlande	Keine Aufschlüsselung nach Alter übermittelt								85000
Österreich	Keine Aufschlüsselung nach Alter übermittelt								3093
Polen	Keine Angaben übermittelt								
Portugal	Keine Angaben übermittelt								
Rumänien	Keine Angaben übermittelt								
Slowenien	Keine Aufschlüsselung nach Alter übermittelt								2821
Slowakei	Keine Angaben übermittelt								
Finnland	9134	1144	448	214	268				4008
Schweden	Keine Angaben übermittelt								
Vereinigtes Königreich	315350	88339	34665	19398	6385	2973	1536	1576	470222
Gesamt	**533504**	**156167**	**64403**	**29156**	**7095***	**3230***	**1353***	**1366***	**1392281**

* Ausgenommen Finnland

Tabelle 8: Anfragen nach gespeicherten Verkehrsdaten nach Art der Daten, 2008 (in Klammern Zahl der Anfragen, auf die keine Daten übermittelt werden konnten – sofern übermittelt)				
Art der Daten / Mitgliedstaat	**Telefonfestnetz**	**Mobilfunk**	**Internet**	**Gesamt**
Belgien	Keine Angaben übermittelt			
Bulgarien	Keine Angaben übermittelt			
Tschechische Republik	**4983 (131)**	**125040 (2276)**	**1537 (83)**	**131560 (2490)**
Dänemark	**192 (0)**	**3273 (5)**	**134 (0)**	**3599 (5)**
Deutschland	Keine Aufschlüsselung nach Art der Daten übermittelt			**12684 (931)**
Estland	**4114 (1519)**	**376 (7)**	Keine Angaben übermittelt	**4490 (1526)**
Irland	**5317 (16)**	**5873 (48)**	**2905 (33)**	**14095 (97)**
Griechenland	Keine Aufschlüsselung nach Art der Daten übermittelt			**584**
Spanien	**4448 (0)**	**40013 (0)**	**9117 (0)**	**53578 (0)**
Frankreich	Keine Aufschlüsselung nach Art der Daten übermittelt			**503437**
Italien	Keine Angaben übermittelt			
Zypern	**3 (0)**	**31 (5)**	**0 (0)**	**34 (5)**
Lettland	**1602 (90)**	**14238 (530)**	**1052 (76)**	**16892 (696)**
Litauen	**765 (72)**	**84550 (5657)**	Keine Angaben übermittelt	**85315 (5729)**
Luxemburg	Keine Angaben übermittelt			
Ungarn	Keine Angaben übermittelt			
Malta	**29 (0)**	**748 (120)**	**92 (13)**	**869 (133)**
Niederlande	Keine Aufschlüsselung nach Art der Daten übermittelt			**85000**
Österreich	Keine Aufschlüsselung nach Art der Daten übermittelt			**3093**
Polen	Keine Angaben übermittelt			
Portugal	Keine Angaben übermittelt			
Rumänien	Keine Angaben übermittelt			
Slowenien	Keine Aufschlüsselung nach Art der Daten übermittelt			**2821**
Slowakei	Keine Angaben übermittelt			
Finnland	Keine Aufschlüsselung nach Art der Daten übermittelt			**4008**
Schweden	Keine Angaben übermittelt			
Vereinigtes Königreich	**90747 (0)**	**329421 (0)**	**50054 (0)**	**470222 (0)**
Gesamt				**1392281**

Tabelle 9: Anfragen nach gespeicherten *Telefonfestnetz*-Verkehrsdaten, die übermittelt wurden, nach Alter, 2008									
Alter der angefragten Daten (Monate) / Mitgliedstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Gesamt**
Belgien	Keine Angaben übermittelt								
Bulgarien	Keine Angaben übermittelt								
Tschechische Republik	3669	916	143	124	0	0	0	0	4852
Dänemark	133	28	31	0	0	0	0	0	192
Deutschland	Keine Angaben übermittelt								
Estland	1876	161	74	484	0	0	0	0	2595
Irland	4118	712	197	182	32	21	23	16	5301
Griechenland	Keine Angaben übermittelt								
Spanien	1948	1431	741	328	0	0	0	0	4448
Frankreich	Keine Angaben übermittelt								
Italien	Keine Angaben übermittelt								
Zypern	3	0	0	0	0	0	0	0	3
Lettland	698	213	167	193	104	137	0	0	1512
Litauen	251	442	0	0	0	0	0	0	693
Luxemburg	Keine Angaben übermittelt								
Ungarn	Keine Angaben übermittelt								
Malta	28	1	0	0	0	0	0	0	29
Niederlande	Keine Angaben übermittelt								
Österreich	Keine Angaben übermittelt								
Polen	Keine Angaben übermittelt								
Portugal	Keine Angaben übermittelt								
Rumänien	Keine Angaben übermittelt								
Slowenien	Keine Angaben übermittelt								
Slowakei	Keine Angaben übermittelt								
Finnland	Keine Angaben übermittelt								
Schweden	Keine Angaben übermittelt								
Vereinigtes Königreich	54805	27052	5340	753	1135	437	1050	175	90747
Gesamt	**67529**	**30956**	**6693**	**2064**	**1271**	**595**	**1073**	**191**	**110372**

Tabelle 10: Anfragen nach gespeicherten *Mobilfunk*-Verkehrsdaten, die übermittelt wurden, nach Alter, 2008									
Alter der angefragten Daten (Monate) / Mitgliedstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Gesamt**
Belgien	Keine Angaben übermittelt								
Bulgarien	Keine Angaben übermittelt								
Tschechische Republik	98232	17013	7518	1	0	0	0	0	122764
Dänemark	2433	628	143	33	20	1	7	3	3268
Deutschland	Keine Angaben übermittelt								
Estland	248	58	35	28	0	0	0	0	369
Irland	4326	820	230	240	57	63	52	37	5825
Griechenland	Keine Angaben übermittelt								
Spanien	17403	12114	7444	3052	0	0	0	0	40013
Frankreich	Keine Angaben übermittelt								
Italien	Keine Angaben übermittelt								
Zypern	23	3	0	0	0	0	0	0	26
Lettland	8928	2298	1085	746	394	257	0	0	13708
Litauen	55484	23375	14	20	0	0	0	0	78893
Luxemburg	Keine Angaben übermittelt								
Ungarn	Keine Angaben übermittelt								
Malta	575	53	0	0	0	0	0	0	628
Niederlande	Keine Angaben übermittelt								
Österreich	Keine Angaben übermittelt								
Polen	Keine Angaben übermittelt								
Portugal	Keine Angaben übermittelt								
Rumänien	Keine Angaben übermittelt								
Slowenien	Keine Angaben übermittelt								
Slowakei	Keine Angaben übermittelt								
Finnland	Keine Angaben übermittelt								
Schweden	Keine Angaben übermittelt								
Vereinigtes Königreich	229375	52241	26228	16040	3333	521	339	1344	329421
Gesamt	**417027**	**108603**	**42697**	**20160**	**3804**	**842**	**398**	**1384**	**594915**

Tabelle 11: Anfragen nach gespeicherten *Internet*-Verkehrsdaten, die übermittelt wurden, nach Alter, 2008									
Alter der angefragten Daten (Monate) / Mitgliedstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Gesamt**
Belgien	Keine Angaben übermittelt								
Bulgarien	Keine Angaben übermittelt								
Tschechische Republik	737	412	137	168	0	0	0	0	1454
Dänemark	102	14	11	2	3	1	0	1	134
Deutschland	Keine Angaben übermittelt								
Estland	Keine Angaben übermittelt								
Irland	492	460	498	1422	0	0	0	0	2872
Griechenland	Keine Angaben übermittelt								
Spanien	3278	2323	2113	1403	0	0	0	0	9117
Frankreich	Keine Angaben übermittelt								
Italien	Keine Angaben übermittelt								
Zypern	0	0	0	0	0	0	0	0	0
Lettland	424	150	75	219	74	34	0	0	976
Litauen	Keine Angaben übermittelt								
Luxemburg	Keine Angaben übermittelt								
Ungarn	Keine Angaben übermittelt								
Malta	76	3	0	0	0	0	0	0	79
Niederlande	Keine Angaben übermittelt								
Österreich	Keine Angaben übermittelt								
Polen	Keine Angaben übermittelt								
Portugal	Keine Angaben übermittelt								
Rumänien	Keine Angaben übermittelt								
Slowenien	Keine Angaben übermittelt								
Slowakei	Keine Angaben übermittelt								
Finnland	Keine Angaben übermittelt								
Schweden	Keine Angaben übermittelt								
Vereinigtes Königreich	31170	9046	3097	2605	1917	2015	147	57	50054
Gesamt	**36279**	**12408**	**5931**	**5819**	**1994**	**2050**	**147**	**58**	**64686**

Von den Mitgliedstaaten für 2009 übermittelte Statistiken

Tabelle 12: Anfragen nach gespeicherten Daten nach Alter, 2009									
Alter der angefragten Daten (Monate) / Mitgliedstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Gesamt**
Belgien	Keine Angaben übermittelt								
Bulgarien	Keine Angaben übermittelt								
Tschechische Republik	210975	56623	11620	1053	0	0	0	0	280271
Dänemark	2980	685	179	104	54	38	12	14	4066
Deutschland	Keine Angaben übermittelt								
Estland	4299	1836	1210	1065	0	0	0	0	8410
Irland	8117	1652	805	297	168	134	69	41	11283
Griechenland	Keine Angaben übermittelt								
Spanien	29775	19346	13999	6970	0	0	0	0	70090
Frankreich	Keine Aufschlüsselung nach Alter übermittelt								514813
Italien	Keine Angaben übermittelt								
Zypern	31	8	1	0	0	0	0	0	40
Lettland	20758	2414	1088	796	565	475	0	0	26096
Litauen	30247	35456	5886	884	0	0	0	0	72473
Luxemburg	Keine Angaben übermittelt								
Ungarn	Keine Angaben übermittelt								
Malta	3336	362	151	174	0	0	0	0	4023
Niederlande	Keine Angaben übermittelt								
Österreich	Keine Angaben übermittelt								
Portugal	Keine Angaben übermittelt								
Rumänien	Keine Angaben übermittelt								
Polen	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Slowenien	Keine Aufschlüsselung nach Alter übermittelt								1918
Slowakei	Keine Aufschlüsselung nach Alter übermittelt								5214
Finnland	2000	1310	532	152	76	0	0	0	4070
Schweden	Keine Angaben übermittelt								
Vereinigtes Königreich	Keine Angaben übermittelt								
Gesamt	**954845**	**297998**	**110996**	**64021**	**27961**	**24571**	**14065**	**34683**	**2051085**

Tabelle 13: Anfragen nach gespeicherten Daten nach Art der Daten, 2009 (in Klammern Zahl der Anfragen, auf die keine Daten übermittelt werden konnten – sofern übermittelt)				
Art der Daten / Mitgliedstaat	**Telefonfestnetz**	**Mobilfunk**	**Internet**	**Gesamt**
Belgien	Keine Angaben übermittelt			
Bulgarien	Keine Angaben übermittelt			
Tschechische Republik	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Dänemark	133 (0)	3771 (10)	162 (1)	4066 (11)
Deutschland	Keine Angaben übermittelt			
Estland	6422 (2279)	902 (21)	1086 (468)	8410 (2768)
Irland	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Griechenland	Keine Angaben übermittelt			
Spanien	5055 (0)	56133 (0)	8902 (0)	70090 (0)
Frankreich	Keine Aufschlüsselung nach Art der Daten übermittelt			**514813**
Italien	Keine Angaben übermittelt			
Zypern	0 (0)	23 (3)	14 (0)	40 (3)
Lettland	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Litauen	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Luxemburg	Keine Angaben übermittelt			
Ungarn	Keine Angaben übermittelt			
Malta	156 (10)	3693 (882)	174 (10)	4023 (902)
Niederlande	Keine Angaben übermittelt			
Österreich	Keine Angaben übermittelt			
Polen	Keine Aufschlüsselung nach Art der Daten übermittelt			**1048318**
Portugal	Keine Angaben übermittelt			
Rumänien	Keine Angaben übermittelt			
Slowenien	Keine Aufschlüsselung nach Art der Daten übermittelt			**1918 (48)**
Slowakei	Keine Aufschlüsselung nach Art der Daten übermittelt			**5214 (157)**
Finnland	Keine Aufschlüsselung nach Art der Daten übermittelt			**4070**
Schweden	Keine Angaben übermittelt			
Vereinigtes Königreich	Keine Angaben übermittelt			
Gesamt				**2051082 (1069885)**

Tabelle 14: Anfragen nach gespeicherten *Telefonfestnetz*-Daten, die übermittelt wurden, nach Alter, 2009									
Alter der angefragten Daten (Monate) / Mitgliedstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Gesamt**
Belgien	Keine Angaben übermittelt								
Bulgarien	Keine Angaben übermittelt								
Tschechische Republik	9919	2907	47	36	0	0	0	0	12909
Dänemark	105	19	7	2	0	0	0	0	133
Deutschland	Keine Angaben übermittelt								
Estland	2254	866	599	424	0	0	0	0	4143
Irland	3934	337	69	70	50	39	16	11	4526
Griechenland	Keine Angaben übermittelt								
Spanien	2371	1492	844	348	0	0	0	0	5055
Frankreich	Keine Angaben übermittelt								
Italien	Keine Angaben übermittelt								
Zypern	0	0	0	0	0	0	0	0	0
Lettland	744	253	157	143	68	89	0	0	1454
Litauen	469	773	73	6	0	0	0	0	1321
Luxemburg	Keine Angaben übermittelt								
Ungarn	Keine Angaben übermittelt								
Malta	83	25	18	20	0	0	0	0	146
Niederlande	Keine Angaben übermittelt								
Österreich	Keine Angaben übermittelt								
Polen	Keine Angaben übermittelt								
Portugal	Keine Angaben übermittelt								
Rumänien	Keine Angaben übermittelt								
Slowenien	Keine Angaben übermittelt								
Slowakei	Keine Angaben übermittelt								
Finnland	Keine Angaben übermittelt								
Schweden	Keine Angaben übermittelt								
Vereinigtes Königreich	Keine Angaben übermittelt								
Gesamt	**19879**	**6672**	**1814**	**1049**	**118**	**128**	**16**	**11**	**29687**

Tabelle 15: Anfragen nach gespeicherten *Mobilfunk*-Daten, die übermittelt wurden, nach Alter, 2009									
Alter der angefragten Daten (Monate) / Mitgliedstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Gesamt**
Belgien	Keine Angaben übermittelt								
Bulgarien	Keine Angaben übermittelt								
Tschechische Republik	197620	48841	472	0	0	0	0	0	246933
Dänemark	2777	639	162	98	47	19	12	7	3761
Deutschland	Keine Angaben übermittelt								
Estland	318	397	96	70	0	0	0	0	881
Irland	3669	835	220	210	115	92	50	28	5219
Griechenland	Keine Angaben übermittelt								
Spanien	24065	15648	11147	5273	0	0	0	0	56133
Frankreich	Keine Angaben übermittelt								
Italien	Keine Angaben übermittelt								
Zypern	17	16	0	0	0	0	0	0	23
Lettland	18832	1912	778	515	394	263	0	0	22694
Litauen	25713	19595	28	0	0	0	0	0	45336
Luxemburg	Keine Angaben übermittelt								
Ungarn	Keine Angaben übermittelt								
Malta	2332	246	111	122	0	0	0	0	2811
Niederlande	Keine Angaben übermittelt								
Österreich	Keine Angaben übermittelt								
Polen	Keine Angaben übermittelt								
Portugal	Keine Angaben übermittelt								
Rumänien	Keine Angaben übermittelt								
Slowenien	Keine Angaben übermittelt								
Slowakei	Keine Angaben übermittelt								
Finnland	Keine Angaben übermittelt								
Schweden	Keine Angaben übermittelt								
Vereinigtes Königreich	Keine Angaben übermittelt								
Gesamt	**275343**	**88119**	**13014**	**6288**	**556**	**374**	**62**	**35**	**383791**

Tabelle 16: Anfragen nach gespeicherten *Internet*-Daten, die übermittelt wurden, nach Alter, 2009									
Alter der angefragten Daten (Monate) / Mitgliedstaat	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Gesamt**
Belgien	Keine Angaben übermittelt								
Bulgarien	Keine Angaben übermittelt								
Tschechische Republik	3369	4811	861	942	0	0	0	0	9983
Dänemark	98	27	10	4	4	7	0	1	151
Deutschland	Keine Angaben übermittelt								
Estland	315	145	56	102	0	0	0	0	618
Irland	489	455	502	0	0	0	0	0	1446
Griechenland	Keine Angaben übermittelt								
Spanien	3339	2206	2008	1349	0	0	0	0	8902
Frankreich	Keine Angaben übermittelt								
Italien	Keine Angaben übermittelt								
Zypern	12	2	0	0	0	0	0	0	14
Lettland	852	198	74	90	88	86	0	0	1388
Litauen	4060	15087	1	88	0	0	0	0	19236
Luxemburg	Keine Angaben übermittelt								
Ungarn	Keine Angaben übermittelt								
Malta	150	14	0	0	0	0	0	0	164
Niederlande	Keine Angaben übermittelt								
Österreich	Keine Angaben übermittelt								
Polen	Keine Angaben übermittelt								
Portugal	Keine Angaben übermittelt								
Rumänien	Keine Angaben übermittelt								
Slowenien	Keine Angaben übermittelt								
Slowakei	Keine Angaben übermittelt								
Finnland	Keine Angaben übermittelt								
Schweden	Keine Angaben übermittelt								
Vereinigtes Königreich	Keine Angaben übermittelt								
Gesamt	**12684**	**22945**	**3512**	**2575**	**92**	**93**	**0**	**1**	**41902**