

URTEIL DES GERICHTSHOFS (Große Kammer)

8. April 2014

„Elektronische Kommunikation – Richtlinie 2006/24/EG – Öffentlich zugängliche elektronische Kommunikationsdienste oder öffentliche Kommunikationsnetze – Vorratsspeicherung von Daten, die bei der Bereitstellung solcher Dienste erzeugt oder verarbeitet werden – Gültigkeit – Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union“

In den verbundenen Rechtssachen C-293/12 und C-594/12

betreffend Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom High Court (Irland) und vom Verfassungsgerichtshof (Österreich) mit Entscheidungen vom 27. Januar und vom 28. November 2012, beim Gerichtshof eingegangen am 11. Juni und am 19. Dezember 2012, in den Verfahren

**Digital Rights Ireland Ltd (C-293/12)**

gegen

**Minister for Communications, Marine and Natural Resources,**

**Minister for Justice, Equality and Law Reform,**

**Commissioner of the Garda Síochána,**

**Irland,**

**The Attorney General,**

Beteiligte:

**Irish Human Rights Commission,**

und

**Kärntner Landesregierung (C-594/12),**

**Michael Seitlinger,**

**Christof Tschohl u. a.**

erlässt

DER GERICHTSHOF (Große Kammer)

unter Mitwirkung des Präsidenten V. Skouris, des Vizepräsidenten K. Lenaerts, des Kammerpräsidenten A. Tizzano, der Kammerpräsidentin R. Silva de Lapuerta, der Kammerpräsidenten T. von Danwitz (Berichterstatter), E. Juhász, A. Borg Barthet,

C. G. Fernlund und J. L. da Cruz Vilaça, der Richter A. Rosas, G. Arestis, J.-C. Bonichot und A. Arabadjiev, der Richterin C. Toader und des Richters C. Vajda,

Generalanwalt: P. Cruz Villalón,

Kanzler: K. Malacek, Verwaltungsrat,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 9. Juli 2013,

unter Berücksichtigung der Erklärungen

- der Digital Rights Ireland Ltd, vertreten durch F. Callanan, SC, und F. Crehan, BL, beauftragt durch S. McGarr, Solicitor,
- von Herrn Seitlinger, vertreten durch Rechtsanwalt G. Otto,
- von Herrn Tschohl u. a., vertreten durch Rechtsanwalt E. Scheucher,
- der Irish Human Rights Commission, vertreten durch P. Dillon Malone, BL, beauftragt durch S. Lucey, Solicitor,
- Irlands, vertreten durch E. Creedon und D. McGuinness als Bevollmächtigte im Beistand von E. Regan, SC, und D. Fennelly, JC,
- der österreichischen Regierung, vertreten durch G. Hesse und G. Kunnert als Bevollmächtigte,
- der spanischen Regierung, vertreten durch N. Díaz Abad als Bevollmächtigte,
- der französischen Regierung, vertreten durch G. de Bergues, D. Colas und B. Beaupère-Manokha als Bevollmächtigte,
- der italienischen Regierung, vertreten durch G. Palmieri als Bevollmächtigte im Beistand von A. De Stefano, avvocato dello Stato,
- der polnischen Regierung, vertreten durch B. Majczyna und M. Szpunar als Bevollmächtigte,
- der portugiesischen Regierung, vertreten durch L. Inez Fernandes und C. Vieira Guerra als Bevollmächtigte,
- der Regierung des Vereinigten Königreichs, vertreten durch L. Christie als Bevollmächtigten im Beistand von S. Lee, Barrister,
- des Europäischen Parlaments, vertreten durch U. Rösslein, A. Caiola und K. Zejdová als Bevollmächtigte,
- des Rates der Europäischen Union, vertreten durch J. Monteiro, E. Sitbon und I. Šulce als Bevollmächtigte,

– der Europäischen Kommission, vertreten durch D. Maidani, B. Martenczuk und M. Wilderspin als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 12. Dezember 2013

folgendes

## **Urteil**

1 Die Vorabentscheidungsersuchen betreffen die Gültigkeit der 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, S. 54).

2 Das Ersuchen des High Court (Rechtssache C-293/12) ergeht in einem Rechtsstreit der Digital Rights Ireland Ltd (im Folgenden: Digital Rights) gegen den Minister for Communications, Marine and Natural Resources, den Minister for Justice, Equality and Law Reform, den Commissioner of the Garda Síochána, Irland sowie den Attorney General wegen der Rechtmäßigkeit nationaler legislativer und administrativer Maßnahmen zur Vorratsspeicherung von Daten elektronischer Kommunikationsvorgänge.

3 Das Ersuchen des Verfassungsgerichtshofs (Rechtssache C-594/12) bezieht sich auf verfassungsrechtliche Verfahren, die vor diesem Gericht von der Kärntner Landesregierung sowie von Herrn Seitlinger, Herrn Tschohl und 11 128 weiteren Antragstellern wegen der Vereinbarkeit des Gesetzes zur Umsetzung der Richtlinie 2006/24 in österreichisches Recht mit dem Bundes-Verfassungsgesetz anhängig gemacht wurden.

## **Rechtlicher Rahmen**

### *Richtlinie 95/46/EG*

4 Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281, S. 31) soll nach ihrem Art. 1 Abs. 1 den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten gewährleisten.

5 In Bezug auf die Sicherheit der Verarbeitung solcher Daten bestimmt Art. 17 Abs. 1 der Richtlinie:

„Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.“

#### *Richtlinie 2002/58/EG*

6 Die 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, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. L 337, S. 11) geänderten Fassung (im Folgenden: Richtlinie 2002/58) dient nach ihrem Art. 1 Abs. 1 zur Harmonisierung der Vorschriften der Mitgliedstaaten, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Europäischen Union zu gewährleisten. Nach Art. 1 Abs. 2 stellen die Bestimmungen dieser Richtlinie eine Detaillierung und Ergänzung der Richtlinie 95/46 im Hinblick auf die in Abs. 1 genannten Zwecke dar.

7 In Bezug auf die Sicherheit der Verarbeitung sieht Art. 4 der Richtlinie 2002/58 vor:

„(1) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.

(1a) Unbeschadet der Richtlinie 95/46/EG ist durch die in Absatz 1 genannten Maßnahmen zumindest Folgendes zu erreichen:

- Sicherstellung, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten,
- Schutz gespeicherter oder übermittelter personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung oder Verarbeitung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe und
- Sicherstellung der Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten.

Die zuständigen nationalen Behörden haben die Möglichkeit, die von den Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste getroffenen Maßnahmen zu prüfen und Empfehlungen zu bewährten Verfahren im Zusammenhang mit dem mit Hilfe dieser Maßnahmen zu erreichenden Sicherheitsniveau ... abzugeben.

(2) Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes die Teilnehmer über dieses Risiko und – wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt – über mögliche Abhilfen, einschließlich der voraussichtlich entstehenden Kosten, unterrichten.“

8 Hinsichtlich der Vertraulichkeit der Kommunikation und der Verkehrsdaten bestimmt Art. 5 Abs. 1 und 3 der Richtlinie:

„(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Diese Bestimmung steht – unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen.

...

(3) Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.“

9 Art. 6 Abs. 1 der Richtlinie 2002/58 lautet:

„Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.“

10 Art. 15 Abs. 1 der Richtlinie 2002/58 bestimmt:

„Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG 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 in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch

Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.“

#### *Richtlinie 2006/24*

11 Nach einer Anhörung von Vertretern der Strafverfolgungsbehörden und der Branche für elektronische Kommunikation sowie Datenschutzexperten legte die Kommission am 21. September 2005 eine Wirkungsanalyse der politischen Optionen für Regeln zur Vorratsspeicherung von Verkehrsdaten vor (im Folgenden: Wirkungsanalyse). Diese Analyse diente als Grundlage für die Ausarbeitung des am selben Tag vorgelegten Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM[2005] 438 endgültig, im Folgenden: Richtlinienvorschlag), der zum Erlass der auf Art. 95 EG gestützten Richtlinie 2006/24 führte.

12 Der vierte Erwägungsgrund der Richtlinie 2006/24 lautet:

„In Artikel 15 Absatz 1 der Richtlinie 2002/58/EG ist festgelegt, unter welchen Bedingungen die Mitgliedstaaten die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 der genannten Richtlinie beschränken dürfen. Etwaige Beschränkungen müssen zu besonderen Zwecken der Aufrechterhaltung der öffentlichen Ordnung, d. h. für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen, in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sein.“

13 Im ersten Satz des fünften Erwägungsgrundes der Richtlinie 2006/24 wird ausgeführt: „Einige Mitgliedstaaten haben Rechtsvorschriften über eine Vorratsspeicherung von Daten durch Diensteanbieter zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erlassen.“

14 In den Erwägungsgründen 7 bis 11 der Richtlinie 2006/24 heißt es:

„(7) In seinen Schlussfolgerungen vom 19. Dezember 2002 betont der Rat ‚Justiz und Inneres‘, dass die beträchtliche Zunahme der Möglichkeiten bei der elektronischen Kommunikation dazu geführt hat, dass Daten über die Nutzung elektronischer Kommunikation besonders wichtig sind und daher ein wertvolles Mittel bei der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten und insbesondere der organisierten Kriminalität darstellen.

(8) In der vom Europäischen Rat am 25. März 2004 angenommenen Erklärung zum Kampf gegen den Terrorismus wurde der Rat aufgefordert, Vorschläge für Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter zu prüfen.

(9) Gemäß Artikel 8 der [am 4. November 1950 in Rom unterzeichneten] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) hat jede Person

das Recht auf Achtung ihres Privatlebens und ihrer Korrespondenz. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist, unter anderem für die nationale oder öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten oder zum Schutz der Rechte und Freiheiten anderer. Da sich die Vorratsspeicherung von Daten in mehreren Mitgliedstaaten als derart notwendiges und wirksames Ermittlungswerkzeug für die Strafverfolgung, insbesondere in schweren Fällen wie organisierter Kriminalität und Terrorismus, erwiesen hat, muss gewährleistet werden, dass die auf Vorrat gespeicherten Daten den Strafverfolgungsbehörden für einen bestimmten Zeitraum unter den in dieser Richtlinie festgelegten Bedingungen zur Verfügung stehen. ...

(10) Am 13. Juli 2005 hat der Rat in seiner Erklärung, in der die Terroranschläge von London verurteilt wurden, nochmals auf die Notwendigkeit hingewiesen, so rasch wie möglich gemeinsame Maßnahmen zur Vorratsspeicherung von Telekommunikationsdaten zu erlassen.

(11) Da sowohl wissenschaftliche Untersuchungen als auch praktische Erfahrungen in mehreren Mitgliedstaaten gezeigt haben, dass Verkehrs- und Standortdaten für die Ermittlung, Feststellung und Verfolgung von Straftaten von großer Bedeutung sind, muss auf europäischer Ebene sichergestellt werden, dass Daten, die bei der Bereitstellung von Kommunikationsdiensten von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, für einen bestimmten Zeitraum unter den in dieser Richtlinie festgelegten Bedingungen auf Vorrat gespeichert werden.“

15 Die Erwägungsgründe 16, 21 und 22 der Richtlinie lauten:

(16) Die Pflichten von Diensteanbietern hinsichtlich Maßnahmen zur Sicherstellung der Datenqualität, die sich aus Artikel 6 der Richtlinie 95/46/EG ergeben, und ihre Pflichten hinsichtlich Maßnahmen zur Gewährleistung der Vertraulichkeit und der Sicherheit der Datenverarbeitung, die sich aus den Artikeln 16 und 17 der genannten Richtlinie ergeben, gelten uneingeschränkt für Daten, die im Sinne der vorliegenden Richtlinie auf Vorrat gespeichert werden.

(21) Da die Ziele dieser Richtlinie, nämlich die Harmonisierung der Pflichten für Diensteanbieter bzw. Netzbetreiber im Zusammenhang mit der Vorratsspeicherung bestimmter Daten und die Gewährleistung, dass diese Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen, auf Ebene der Mitgliedstaaten nicht ausreichend erreicht werden können und daher wegen des Umfangs und der Wirkungen dieser Richtlinie besser auf Gemeinschaftsebene zu erreichen sind, kann die Gemeinschaft gemäß dem in Artikel 5 des Vertrags niedergelegten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das zur Erreichung dieser Ziele erforderliche Maß hinaus.

(22) Diese Richtlinie wahrt die vor allem mit der Charta der Grundrechte der Europäischen Union anerkannten Grundrechte und Grundsätze. In Verbindung mit der Richtlinie 2002/58/EG ist die vorliegende Richtlinie insbesondere bestrebt, die volle Wahrung der Grundrechte der Bürger auf Achtung des Privatlebens und ihrer Kommunikation sowie auf Schutz personenbezogener Daten gemäß Artikel 7 und 8 der Charta zu gewährleisten.“

16 Die Richtlinie 2006/24 verpflichtet die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder die Betreiber eines öffentlichen Kommunikationsnetzes, bestimmte von ihnen erzeugte oder verarbeitete Daten auf Vorrat zu speichern. Hierzu heißt es in den Art. 1 bis 9, 11 und 13 der Richtlinie:

### *„Artikel 1*

#### Gegenstand und Geltungsbereich

(1) Mit dieser Richtlinie sollen die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter Daten, die von ihnen erzeugt oder verarbeitet werden, harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen.

(2) Diese Richtlinie gilt für Verkehrs- und Standortdaten sowohl von juristischen als auch von natürlichen Personen sowie für alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind. Sie gilt nicht für den Inhalt elektronischer Nachrichtenübermittlungen einschließlich solcher Informationen, die mit Hilfe eines elektronischen Kommunikationsnetzes abgerufen werden.

### *Artikel 2*

#### Begriffsbestimmungen

(1) Für die Zwecke dieser Richtlinie finden die Begriffsbestimmungen der Richtlinie 95/46/EG, der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) ... und der Richtlinie 2002/58/EG Anwendung.

(2) Im Sinne dieser Richtlinie bezeichnet der Ausdruck

a) ‚Daten‘ Verkehrsdaten und Standortdaten sowie alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind;

b) ‚Benutzer‘ jede juristische oder natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

c) ‚Telefondienst‘ Anrufe (einschließlich Sprachtelefonie, Sprachspeicherdienst, Konferenzschaltungen und Datenabrufungen), Zusatzdienste (einschließlich Rufweiterleitung und Rufumleitung) und Mitteilungsdienste und Multimediadienste (einschließlich Kurznachrichtendienste (SMS), erweiterte Nachrichtendienste (EMS) und Multimediadienste (MMS));

d) ‚Benutzerkennung‘ eine eindeutige Kennung, die Personen zugewiesen wird, wenn diese sich bei einem Internetanbieter oder einem Internet-Kommunikationsdienst registrieren lassen oder ein Abonnement abschließen;

e) ‚Standortkennung‘ die Kennung der Funkzelle, von der aus eine Mobilfunkverbindung hergestellt wird bzw. in der sie endet;

f) ‚erfolgloser Anrufversuch‘ einen Telefonanruf, bei dem die Verbindung erfolgreich aufgebaut wurde, der aber unbeantwortet bleibt oder bei dem das Netzwerkmanagement eingegriffen hat.

### *Artikel 3*

#### Vorratsspeicherungspflicht

(1) Abweichend von den Artikeln 5, 6 und 9 der Richtlinie 2002/58/EG tragen die Mitgliedstaaten durch entsprechende Maßnahmen dafür Sorge, dass die in Artikel 5 der vorliegenden Richtlinie genannten Daten, soweit sie im Rahmen ihrer Zuständigkeit im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, gemäß den Bestimmungen der vorliegenden Richtlinie auf Vorrat gespeichert werden.

(2) Die Verpflichtung zur Vorratsspeicherung nach Absatz 1 schließt die Vorratsspeicherung von in Artikel 5 genannten Daten im Zusammenhang mit erfolglosen Anrufversuchen ein, wenn diese Daten von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes im Rahmen der Zuständigkeit des betreffenden Mitgliedstaats im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet und gespeichert (bei Telefoniedaten) oder protokolliert (bei Internetdaten) werden. Nach dieser Richtlinie ist die Vorratsspeicherung von Daten im Zusammenhang mit Anrufen, bei denen keine Verbindung zustande kommt, nicht erforderlich.

### *Artikel 4*

#### Zugang zu Daten

Die Mitgliedstaaten erlassen Maßnahmen, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden. Jeder Mitgliedstaat legt in seinem innerstaatlichen Recht unter Berücksichtigung der einschlägigen Bestimmungen des Rechts der Europäischen Union oder des Völkerrechts, insbesondere der EMRK in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte, das Verfahren und die Bedingungen fest, die für den Zugang zu auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.

### *Artikel 5*

#### Kategorien von auf Vorrat zu speichernden Daten

(1) Die Mitgliedstaaten stellen sicher, dass gemäß dieser Richtlinie die folgenden Datenkategorien auf Vorrat gespeichert werden:

a) zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk:
  - i) die Rufnummer des anrufenden Anschlusses,
  - ii) der Name und die Anschrift des Teilnehmers oder registrierten Benutzers;
2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
  - i) die zugewiesene(n) Benutzerkennung(en),
  - ii) die Benutzerkennung und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden,
  - iii) der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine Internetprotokoll-Adresse (IP-Adresse), Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war;
- b) zur Identifizierung des Adressaten einer Nachricht benötigte Daten:
  1. betreffend Telefonfestnetz und Mobilfunk:
    - i) die angewählte(n) Nummer(n) (die Rufnummer(n) des angerufenen Anschlusses) und bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Nummer(n), an die der Anruf geleitet wird,
    - ii) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer;
  2. betreffend Internet-E-Mail und Internet-Telefonie:
    - i) die Benutzerkennung oder Rufnummer des vorgesehenen Empfängers eines Anrufs mittels Internet-Telefonie,
    - ii) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer und die Benutzerkennung des vorgesehenen Empfängers einer Nachricht;
- c) zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten:
  1. betreffend Telefonfestnetz und Mobilfunk: Datum und Uhrzeit des Beginns und Endes eines Kommunikationsvorgangs;
  2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
    - i) Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers,
    - ii) Datum und Uhrzeit der An- und Abmeldung beim Internet-E-Mail-Dienst oder Internet-Telefonie-Dienst auf der Grundlage einer bestimmten Zeitzone;

- d) zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten:
    - 1. betreffend Telefonfestnetz und Mobilfunk: der in Anspruch genommene Telefondienst;
    - 2. betreffend Internet-E-Mail und Internet-Telefonie: der in Anspruch genommene Internetdienst;
  - e) zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten:
    - 1. betreffend Telefonfestnetz: die Rufnummern des anrufenden und des angerufenen Anschlusses;
    - 2. betreffend Mobilfunk:
      - i) die Rufnummern des anrufenden und des angerufenen Anschlusses,
      - ii) die internationale Mobilteilnehmerkennung (IMSI) des anrufenden Anschlusses,
      - iii) die internationale Mobilfunkgeräteerkennung (IMEI) des anrufenden Anschlusses,
      - iv) die IMSI des angerufenen Anschlusses,
      - v) die IMEI des angerufenen Anschlusses,
      - vi) im Falle vorbezahlter anonymer Dienste: Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID), an dem der Dienst aktiviert wurde;
    - 3. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
      - i) die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss,
      - ii) der digitale Teilnehmeranschluss (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs;
  - f) zur Bestimmung des Standorts mobiler Geräte benötigte Daten:
    - 1. die Standortkennung (Cell-ID) bei Beginn der Verbindung,
    - 2. Daten zur geografischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell-ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt.
- (2) Nach dieser Richtlinie dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden.

## *Artikel 6*

### Speicherungsfristen

Die Mitgliedstaaten sorgen dafür, dass die in Artikel 5 angegebenen Datenkategorien für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden.

#### *Artikel 7*

##### Datenschutz und Datensicherheit

Unbeschadet der zur Umsetzung der Richtlinien 95/46/EG und 2002/58/EG erlassenen Vorschriften stellt jeder Mitgliedstaat sicher, dass Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten bzw. Betreiber eines öffentlichen Kommunikationsnetzes in Bezug auf die nach Maßgabe der vorliegenden Richtlinie auf Vorrat gespeicherten Daten zumindest die folgenden Grundsätze der Datensicherheit einhalten:

- a) Die auf Vorrat gespeicherten Daten sind von der gleichen Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im 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,

und

- d) die Daten werden am Ende der Vorratsspeichungsfrist vernichtet, mit Ausnahme jener Daten, die abgerufen und gesichert worden sind.

#### *Artikel 8*

##### Anforderungen an die Vorratsdatenspeicherung

Die Mitgliedstaaten stellen sicher, dass die in Artikel 5 genannten Daten gemäß den Bestimmungen dieser Richtlinie so gespeichert werden, dass sie und alle sonstigen damit zusammenhängenden erforderlichen Informationen unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können.

#### *Artikel 9*

##### Kontrollteam

- (1) Jeder Mitgliedstaat benennt eine oder mehrere öffentliche Stellen, die für die Kontrolle der Anwendung der von den Mitgliedstaaten zur Umsetzung von Artikel 7 erlassenen Vorschriften bezüglich der Sicherheit der auf Vorrat gespeicherten Daten in seinem Hoheitsgebiet zuständig ist/sind. Diese Stellen können dieselben Stellen sein, auf die in Artikel 28 der Richtlinie 95/46/EG Bezug genommen wird.

(2) Die in Absatz 1 genannten Stellen nehmen die dort genannte Kontrolle in völliger Unabhängigkeit wahr.

...

### *Artikel 11*

#### Änderung der Richtlinie 2002/58/EG

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 ... eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben ist.

...“

### *Artikel 13*

#### Rechtsbehelfe, Haftung und Sanktionen

(1) Jeder Mitgliedstaat ergreift die erforderlichen Maßnahmen, um sicherzustellen, dass die einzelstaatlichen Maßnahmen zur Umsetzung von Kapitel III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen im Hinblick auf die Datenverarbeitung gemäß der vorliegenden Richtlinie in vollem Umfang umgesetzt werden.

(2) Jeder Mitgliedstaat ergreift insbesondere die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche Zugang zu oder die vorsätzliche Übermittlung von gemäß dieser Richtlinie auf Vorrat gespeicherten Daten, der bzw. die nach den zur Umsetzung dieser Richtlinie erlassenen nationalen Rechtsvorschriften nicht zulässig ist, mit Sanktionen, einschließlich verwaltungsrechtlicher und strafrechtlicher Sanktionen, belegt wird, die wirksam, verhältnismäßig und abschreckend sind.“

### **Ausgangsverfahren und Vorlagefragen**

#### *Rechtssache C-293/12*

17 Digital Rights erhob am 11. August 2006 eine Klage vor dem High Court, in deren Rahmen sie angibt, Eigentümerin eines am 3. Juni 2006 registrierten Mobiltelefons zu sein, das sie seit diesem Tag nutze. Sie stellt die Rechtmäßigkeit nationaler legislativer und administrativer Maßnahmen zur Vorratsspeicherung von Daten elektronischer Kommunikationsvorgänge in Abrede und begehrt vom vorlegenden Gericht u. a. die Feststellung der Unwirksamkeit der Richtlinie 2006/24 und des siebten Teils des Gesetzes von 2005 über terroristische Straftaten (Criminal Justice [Terrorist Offences] Act 2005), das die Anbieter von Telekommunikationsdiensten verpflichtete, Verkehrs- und Standortdaten im Bereich der Telekommunikation für einen gesetzlich festgelegten Zeitraum zum Zweck der Verhütung, Feststellung, Ermittlung und Verfolgung von Straftaten sowie des Schutzes der Sicherheit des Staats zu speichern.

18 Da der High Court der Ansicht ist, nicht über die von ihm zu klärenden Fragen des nationalen Rechts entscheiden zu können, ohne dass die Gültigkeit der Richtlinie 2006/24

geprüft wurde, hat er beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Ist die sich aus den Erfordernissen der Art. 3, 4 und 6 der Richtlinie 2006/24 ergebende Beschränkung der Rechte der Klägerin bezüglich der Nutzung des Mobilfunks mit Art. 5 Abs. 4 EUV unvereinbar, weil sie unverhältnismäßig und nicht erforderlich bzw. ungeeignet zur Erreichung der berechtigten Ziele ist, die darin bestehen,

a) sicherzustellen, dass bestimmte Daten zwecks Ermittlung, Feststellung und Verfolgung schwerer Straftaten zur Verfügung stehen,

und/oder

b) sicherzustellen, dass der Binnenmarkt der Europäischen Union reibungslos funktioniert?

2. Insbesondere:

a) Ist die Richtlinie 2006/24 mit dem in Art. 21 AEUV verankerten Recht der Bürger vereinbar, sich im Hoheitsgebiet der Mitgliedstaaten frei zu bewegen und aufzuhalten?

b) Ist die Richtlinie 2006/24 mit dem in Art. 7 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) und in Art. 8 EMRK verankerten Recht auf Privatleben vereinbar?

c) Ist die Richtlinie 2006/24 mit dem in Art. 8 der Charta verankerten Recht auf Schutz personenbezogener Daten vereinbar?

d) Ist die Richtlinie 2006/24 mit dem in Art. 11 der Charta und in Art. 10 EMRK verankerten Recht auf Freiheit der Meinungsäußerung vereinbar?

e) Ist die Richtlinie 2006/24 mit dem in Art. 41 der Charta verankerten Recht auf eine gute Verwaltung vereinbar?

3. Inwieweit hat ein nationales Gericht nach den Verträgen – insbesondere nach dem in Art. 4 Abs. 3 EUV verankerten Grundsatz der loyalen Zusammenarbeit – die Vereinbarkeit der nationalen Maßnahmen zur Umsetzung der Richtlinie 2006/24 mit dem durch die Charta einschließlich deren Art. 7 (in dem der Gedanke des Art. 8 EMRK zum Ausdruck kommt) gewährten Schutz zu prüfen und festzustellen?

*Rechtssache C-594/12*

19 Dem Vorabentscheidungsersuchen des Verfassungsgerichtshofs in der Rechtssache C-594/12 liegen Anträge der Kärntner Landesregierung sowie von Herrn Seitlinger, Herrn Tschohl und 11 128 weiteren Antragstellern auf Nichtigerklärung von § 102a des Telekommunikationsgesetzes 2003 (im Folgenden: TKG 2003) zugrunde, der durch das Bundesgesetz, mit dem das TKG 2003 geändert wird (BGBl. I Nr. 27/2011), zur Umsetzung der Richtlinie 2006/24 in österreichisches Recht in dieses Gesetz eingefügt wurde. Die Antragsteller sind u. a. der Ansicht, dass § 102a TKG 2003 das Grundrecht der Bürger auf Schutz ihrer Daten verletze.

20 Der Verfassungsgerichtshof möchte insbesondere wissen, ob die Richtlinie 2006/24 insofern mit der Charta vereinbar sei, als sie die Speicherung vielfältiger Daten einer unbegrenzten Zahl von Personen für lange Dauer ermögliche. Die Vorratsdatenspeicherung erfasse fast ausschließlich Personen, deren Verhalten die Speicherung der sie betreffenden Daten in keiner Weise rechtfertige. Diese Personen würden einem erhöhten Risiko ausgesetzt, dass die Behörden ihre Daten ermittelten, deren Inhalt zur Kenntnis nähmen und sich über ihr Privatleben informierten und dass diese Daten – in Anbetracht vor allem der nicht überblickbaren Zahl von Personen, die für mindestens sechs Monate Zugriff auf sie hätten – für vielfältige Zwecke verwendet würden. Es bestünden Zweifel, ob sich die Richtlinie zur Erreichung der mit ihr verfolgten Ziele eigne und ob der Eingriff in die betreffenden Grundrechte verhältnismäßig sei.

21 Der Verfassungsgerichtshof hat daher beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Zur Gültigkeit von Handlungen von Organen der Union:

Sind die Art. 3 bis 9 der Richtlinie 2006/24 mit den Art. 7, 8 und 11 der Charta vereinbar?

2. Zur Auslegung der Verträge:

a) Sind im Licht der Erläuterungen zu Art. 8 der Charta, die gemäß Art. 52 Abs. 7 der Charta als Anleitung zur Auslegung der Charta verfasst wurden und vom Verfassungsgerichtshof gebührend zu berücksichtigen sind, die Richtlinie 95/46 und die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. 2001, L 8, S. 1) für die Beurteilung der Zulässigkeit von Eingriffen gleichwertig mit den Bedingungen nach Art. 8 Abs. 2 und Art. 52 Abs. 1 der Charta zu berücksichtigen?

b) In welchem Verhältnis steht das in Art. 52 Abs. 3 letzter Satz der Charta in Bezug genommene „Recht der Union“ zu den Richtlinien im Bereich des Datenschutzrechts?

c) Sind angesichts dessen, dass die Richtlinie 95/46 und die Verordnung Nr. 45/2001 Bedingungen und Beschränkungen für die Wahrnehmung des Datenschutzgrundrechts der Charta enthalten, Änderungen als Folge späteren Sekundärrechts bei der Auslegung des Art. 8 der Charta zu berücksichtigen?

d) Hat unter Berücksichtigung des Art. 52 Abs. 4 der Charta der Grundsatz der Wahrung höherer Schutzniveaus in Art. 53 der Charta zur Konsequenz, dass die nach der Charta maßgeblichen Grenzen für zulässige Einschränkungen durch Sekundärrecht enger zu ziehen sind?

e) Können sich im Hinblick auf Art. 52 Abs. 3 der Charta, Abs. 5 der Präambel und die Erläuterungen zu Art. 7 der Charta, wonach die darin garantierten Rechte den Rechten nach Art. 8 EMRK entsprechen, aus der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Art. 8 EMRK Gesichtspunkte für die Auslegung des Art. 8 der Charta ergeben, die die Auslegung des zuletzt genannten Artikels beeinflussen?

22 Durch Beschluss des Präsidenten des Gerichtshofs vom 11. Juni 2013 sind die Rechtssachen C-293/12 und C-594/12 zu gemeinsamem mündlichen Verfahren und zu gemeinsamer Entscheidung verbunden worden.

### **Zu den Vorlagefragen**

*Zur zweiten Frage, Buchst. b bis d, in der Rechtssache C-293/12 und zur ersten Frage in der Rechtssache C-594/12*

23 Mit der zweiten Frage, Buchst. b bis d, in der Rechtssache C-293/12 und mit der ersten Frage in der Rechtssache C-594/12, die zusammen zu prüfen sind, ersuchen die vorlegenden Gerichte den Gerichtshof um die Prüfung der Gültigkeit der Richtlinie 2006/24 im Licht der Art. 7, 8 und 11 der Charta.

Zur Relevanz der Art. 7, 8 und 11 der Charta für die Frage der Gültigkeit der Richtlinie 2006/24

24 Wie sich aus Art. 1 sowie den Erwägungsgründen 4, 5, 7 bis 11, 21 und 22 der Richtlinie 2006/24 ergibt, sollen mit ihr in erster Linie die Vorschriften der Mitgliedstaaten über die Vorratsspeicherung bestimmter von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes erzeugter oder verarbeiteter Daten harmonisiert werden, um sicherzustellen, dass die Daten, unter Wahrung der in den Art. 7 und 8 der Charta verankerten Rechte, zwecks Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten wie organisierter Kriminalität und Terrorismus zur Verfügung stehen.

25 Die in Art. 3 der Richtlinie 2006/24 vorgesehene Pflicht der Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder der Betreiber eines öffentlichen Kommunikationsnetzes, die in Art. 5 der Richtlinie aufgezählten Daten auf Vorrat zu speichern, um sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, wirft Fragen hinsichtlich des in Art. 7 der Charta verankerten Schutzes sowohl des Privatlebens als auch der Kommunikation, hinsichtlich des von Art. 8 der Charta erfassten Schutzes personenbezogener Daten und hinsichtlich der durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung auf.

26 Hierzu ist festzustellen, dass es sich bei den Daten, die von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes nach den Art. 3 und 5 der Richtlinie 2006/24 auf Vorrat zu speichern sind, u. a. um die zur Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie zur Bestimmung von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte benötigten Daten handelt, zu denen Name und Anschrift des Teilnehmers oder registrierten Benutzers, die Rufnummer des anrufenden Anschlusses und des angerufenen Anschlusses sowie bei Internetdiensten eine IP-Adresse gehören. Aus diesen Daten geht insbesondere hervor, mit welcher Person ein Teilnehmer oder registrierter Benutzer auf welchem Weg kommuniziert hat, wie lange die Kommunikation gedauert hat und von welchem Ort aus sie stattfand. Ferner ist ihnen zu entnehmen, wie häufig der Teilnehmer oder registrierte Benutzer während eines bestimmten Zeitraums mit bestimmten Personen kommuniziert hat.

27 Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren.

28 Unter solchen Umständen ist es – auch wenn die Richtlinie 2006/24, wie sich aus ihren Art. 1 Abs. 2 und 5 Abs. 2 ergibt, keine Vorratsspeicherung des Inhalts einer Nachricht und der mit Hilfe eines elektronischen Kommunikationsnetzes abgerufenen Informationen gestattet – nicht ausgeschlossen, dass die Vorratsspeicherung der fraglichen Daten Auswirkungen auf die Nutzung der von dieser Richtlinie erfassten Kommunikationsmittel durch die Teilnehmer oder registrierten Benutzer und infolgedessen auf deren Ausübung der durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung hat.

29 Die in der Richtlinie 2006/24 vorgesehene Vorratsspeicherung der Daten zu dem Zweck, sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, betrifft unmittelbar und speziell das Privatleben und damit die durch Art. 7 der Charta garantierten Rechte. Eine solche Vorratsspeicherung der Daten fällt zudem unter Art. 8 der Charta, weil sie eine Verarbeitung personenbezogener Daten im Sinne dieses Artikels darstellt und deshalb zwangsläufig die ihm zu entnehmenden Erfordernisse des Datenschutzes erfüllen muss (Urteil Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 47).

30 Zwar werfen die Vorabentscheidungsersuchen in den vorliegenden Rechtssachen insbesondere die grundsätzliche Frage auf, ob die Daten der Teilnehmer und der registrierten Benutzer im Hinblick auf Art. 7 der Charta auf Vorrat gespeichert werden dürfen, doch betreffen sie auch die Frage, ob die Richtlinie 2006/24 den in Art. 8 der Charta aufgestellten Erfordernissen des Schutzes personenbezogener Daten genügt.

31 In Anbetracht der vorstehenden Erwägungen ist zur Beantwortung der zweiten Frage, Buchst. b bis d, in der Rechtssache C-293/12 und der ersten Frage in der Rechtssache C-594/12 die Gültigkeit der Richtlinie anhand der Art. 7 und 8 der Charta zu prüfen.

Zum Vorliegen eines Eingriffs in die Rechte, die in den Art. 7 und 8 der Charta verankert sind

32 Durch die Verpflichtung zur Vorratsspeicherung der in Art. 5 Abs. 1 der Richtlinie 2006/24 aufgeführten Daten und durch die Gestattung des Zugangs der zuständigen nationalen Behörden zu diesen Daten weicht die Richtlinie, wie der Generalanwalt insbesondere in den Nrn. 39 und 40 seiner Schlussanträge ausgeführt hat, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich elektronischer Kommunikationsvorgänge von der durch die Richtlinien 95/46 und 2002/58 geschaffenen Regelung zum Schutz des Rechts auf Achtung der Privatsphäre ab, denn die letztgenannten Richtlinien sehen die Vertraulichkeit der Kommunikation und der Verkehrsdaten sowie die Pflicht vor, diese Daten zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden, ausgenommen die zur Gebührenabrechnung erforderlichen Daten und nur solange diese dafür benötigt werden.

33 Für die Feststellung des Vorliegens eines Eingriffs in das Grundrecht auf Achtung des Privatlebens kommt es nicht darauf an, ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile

erlitten haben könnten (vgl. in diesem Sinne Urteil Österreichischer Rundfunk u. a., C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 75).

34 Daraus folgt, dass die den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste und den Betreibern eines öffentlichen Kommunikationsnetzes durch die Art. 3 und 6 der Richtlinie 2006/24 auferlegte Pflicht, die in Art. 5 dieser Richtlinie aufgeführten Daten über das Privatleben einer Person und ihre Kommunikationsvorgänge während eines bestimmten Zeitraums auf Vorrat zu speichern, als solche einen Eingriff in die durch Art. 7 der Charta garantierten Rechte darstellt.

35 Zudem stellt der Zugang der zuständigen nationalen Behörden zu den Daten einen zusätzlichen Eingriff in dieses Grundrecht dar (vgl., zu Art. 8 EMRK, Urteile des EGMR Leander/Schweden vom 26. März 1987, Serie A, Nr. 116, § 48, Rotaru/Rumänien [GK], Nr. 28341/95, § 46, Rep. 2000-V, sowie Weber und Saravia/Deutschland (Entsch.), Nr. 54934/00, § 79, Rep. 2006-XI). Auch die Art. 4 und 8 der Richtlinie 2006/24, die Regeln für den Zugang der zuständigen nationalen Behörden zu den Daten aufstellen, greifen daher in die durch Art. 7 der Charta garantierten Rechte ein.

36 Desgleichen greift die Richtlinie 2006/24 in das durch Art. 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten ein, da sie eine Verarbeitung personenbezogener Daten vorsieht.

37 Der mit der Richtlinie 2006/24 verbundene Eingriff in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte ist, wie auch der Generalanwalt insbesondere in den Nrn. 77 und 80 seiner Schlussanträge ausgeführt hat, von großem Ausmaß und als besonders schwerwiegend anzusehen. Außerdem ist der Umstand, dass die Vorratsspeicherung der Daten und ihre spätere Nutzung vorgenommen werden, ohne dass der Teilnehmer oder der registrierte Benutzer darüber informiert wird, geeignet, bei den Betroffenen – wie der Generalanwalt in den Nrn. 52 und 72 seiner Schlussanträge ausgeführt hat – das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist.

Zur Rechtfertigung des Eingriffs in die durch Art. 7 und Art. 8 der Charta garantierten Rechte

38 Nach Art. 52 Abs. 1 der Charta muss jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten; unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

39 Zum Wesensgehalt des Grundrechts auf Achtung des Privatlebens und der übrigen in Art. 7 der Charta verankerten Rechte ist festzustellen, dass die nach der Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung von Daten zwar einen besonders schwerwiegenden Eingriff in diese Rechte darstellt, doch nicht geeignet ist, ihren Wesensgehalt anzutasten, da die Richtlinie, wie sich aus ihrem Art. 1 Abs. 2 ergibt, die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet.

40 Die Vorratsspeicherung von Daten ist auch nicht geeignet, den Wesensgehalt des in Art. 8 der Charta verankerten Grundrechts auf den Schutz personenbezogener Daten anzutasten, weil die Richtlinie 2006/24 in ihrem Art. 7 eine Vorschrift zum Datenschutz und zur Datensicherheit enthält, nach der Anbieter von öffentlich zugänglichen elektronischen

Kommunikationsdiensten bzw. Betreiber eines öffentlichen Kommunikationsnetzes, unbeschadet der zur Umsetzung der Richtlinien 95/46 und 2002/58 erlassenen Vorschriften, bestimmte Grundsätze des Datenschutzes und der Datensicherheit einhalten müssen. Nach diesen Grundsätzen stellen die Mitgliedstaaten sicher, dass geeignete technische und organisatorische Maßnahmen getroffen werden, um die Daten gegen zufällige oder unrechtmäßige Zerstörung sowie zufälligen Verlust oder zufällige Änderung zu schützen.

41 Zu der Frage, ob der fragliche Eingriff einer dem Gemeinwohl dienenden Zielsetzung entspricht, ist festzustellen, dass mit der Richtlinie 2006/24 zwar die Vorschriften der Mitgliedstaaten über die Pflichten der genannten Anbieter oder Betreiber im Bereich der Vorratsspeicherung bestimmter von ihnen erzeugter oder verarbeiteter Daten harmonisiert werden sollen, doch besteht das materielle Ziel dieser Richtlinie, wie sich aus ihrem Art. 1 Abs. 1 ergibt, darin, die Verfügbarkeit der Daten zwecks Ermittlung, Feststellung und Verfolgung schwerer Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, sicherzustellen. Materielles Ziel der Richtlinie ist es demnach, zur Bekämpfung schwerer Kriminalität und somit letztlich zur öffentlichen Sicherheit beizutragen.

42 Nach der Rechtsprechung des Gerichtshofs stellt die Bekämpfung des internationalen Terrorismus zur Wahrung des Weltfriedens und der internationalen Sicherheit eine dem Gemeinwohl dienende Zielsetzung der Union dar (vgl. in diesem Sinne Urteile Kadi und Al Barakaat International Foundation/Rat und Kommission, C-402/05 P und C-415/05 P, EU:C:2008:461, Rn. 363, sowie Al-Aqsa/Rat, C-539/10 P und C-550/10 P, EU:C:2012:711, Rn. 130). Das Gleiche gilt für die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit (vgl. in diesem Sinne Urteil Tsakouridis, C-145/09, EU:C:2010:708, Rn. 46 und 47). Im Übrigen ist insoweit festzustellen, dass nach Art. 6 der Charta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat.

43 Hierzu geht aus dem siebten Erwägungsgrund der Richtlinie 2006/24 hervor, dass der Rat „Justiz und Inneres“ am 19. Dezember 2002 wegen der beträchtlichen Zunahme der Möglichkeiten bei der elektronischen Kommunikation die Ansicht vertrat, dass Daten über die Nutzung elektronischer Kommunikation besonders wichtig seien und daher ein nützliches Mittel bei der Verhütung von Straftaten und der Bekämpfung der Kriminalität, insbesondere der organisierten Kriminalität, darstellten.

44 Somit ist festzustellen, dass die durch die Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung von Daten zu dem Zweck, sie gegebenenfalls den zuständigen nationalen Behörden zugänglich machen zu können, eine dem Gemeinwohl dienende Zielsetzung darstellt.

45 Unter diesen Umständen ist die Verhältnismäßigkeit des festgestellten Eingriffs zu prüfen.

46 Insoweit ist darauf hinzuweisen, dass der Grundsatz der Verhältnismäßigkeit nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist (vgl. in diesem Sinne Urteile Afton Chemical, C-343/09, EU:C:2010:419, Rn. 45, Volker und Markus Schecke und Eifert, EU:C:2010:662, Rn. 74, Nelson u. a., C-581/10 und C-629/10, EU:C:2012:657, Rn. 71, Sky Österreich, C-283/11, EU:C:2013:28, Rn. 50, und Schaible, C-101/12, EU:C:2013:661, Rn. 29).

47 Was die gerichtliche Überprüfung der Einhaltung dieser Voraussetzungen anbelangt, kann, da Grundrechtseingriffe in Rede stehen, der Gestaltungsspielraum des Unionsgesetzgebers anhand einer Reihe von Gesichtspunkten eingeschränkt sein; zu ihnen gehören u. a. der betroffene Bereich, das Wesen des fraglichen durch die Charta gewährleisteten Rechts, Art und Schwere des Eingriffs sowie dessen Zweck (vgl. entsprechend, zu Art. 8 EMRK, Urteil des EGMR S und Marper/Vereinigtes Königreich [GK], Nrn. 30562/04 und 30566/04, § 102, Rep. 2008-V).

48 Im vorliegenden Fall ist angesichts der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung des Privatlebens und des Ausmaßes und der Schwere des mit der Richtlinie 2006/24 verbundenen Eingriffs in dieses Recht der Gestaltungsspielraum des Unionsgesetzgebers eingeschränkt, so dass die Richtlinie einer strikten Kontrolle unterliegt.

49 Zu der Frage, ob die Vorratsspeicherung der Daten zur Erreichung des mit der Richtlinie 2006/24 verfolgten Ziels geeignet ist, ist festzustellen, dass angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die nach dieser Richtlinie auf Vorrat zu speichernden Daten den für die Strafverfolgung zuständigen nationalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und insoweit daher ein nützliches Mittel für strafrechtliche Ermittlungen darstellen. Die Vorratsspeicherung solcher Daten kann somit als zur Erreichung des mit der Richtlinie verfolgten Ziels geeignet angesehen werden.

50 Diese Beurteilung kann nicht durch den – insbesondere von Herrn Tschohl und Herrn Seitlinger sowie der portugiesischen Regierung in ihren beim Gerichtshof eingereichten schriftlichen Erklärungen angeführten – Umstand in Frage gestellt werden, dass es mehrere elektronische Kommunikationsweisen gebe, die nicht in den Anwendungsbereich der Richtlinie 2006/24 fielen oder die eine anonyme Kommunikation ermöglichen. Dieser Umstand vermag zwar die Eignung der in der Vorratsspeicherung der Daten bestehenden Maßnahme zur Erreichung des verfolgten Ziels zu begrenzen, führt aber, wie der Generalanwalt in Nr. 137 seiner Schlussanträge ausgeführt hat, nicht zur Ungeeignetheit dieser Maßnahme.

51 Zur Erforderlichkeit der durch die Richtlinie 2006/24 vorgeschriebenen Vorratsspeicherung der Daten ist festzustellen, dass zwar die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit ist und dass ihre Wirksamkeit in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen kann. Eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer Speicherungsmaßnahme – wie sie die Richtlinie 2006/24 vorsieht – für die Kriminalitätsbekämpfung nicht rechtfertigen.

52 Der Schutz des Grundrechts auf Achtung des Privatlebens verlangt nach ständiger Rechtsprechung des Gerichtshofs jedenfalls, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen (Urteil IPI, C-473/12, EU:C:2013:715, Rn. 39 und die dort angeführte Rechtsprechung).

53 Insoweit ist darauf hinzuweisen, dass der Schutz personenbezogener Daten, zu dem Art. 8 Abs. 1 der Charta ausdrücklich verpflichtet, für das in ihrem Art. 7 verankerte Recht auf Achtung des Privatlebens von besonderer Bedeutung ist.

54 Daher muss die fragliche Unionsregelung klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen (vgl. entsprechend, zu Art. 8 EMRK, Urteile des EGMR Liberty u. a./Vereinigtes Königreich vom 1. Juli 2008, Nr. 58243/00, §§ 62 und 63, Rotaru/Rumänien, §§ 57 bis 59, sowie S und Marper/Vereinigtes Königreich, § 99).

55 Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten, wie in der Richtlinie 2006/24 vorgesehen, automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu diesen Daten besteht (vgl. entsprechend, zu Art. 8 EMRK, Urteil des EGMR S und Marper/Vereinigtes Königreich, § 103, sowie M. K./Frankreich vom 18. April 2013, Nr. 19522/09, § 35).

56 Zu der Frage, ob der mit der Richtlinie 2006/24 verbundene Eingriff auf das absolut Notwendige beschränkt ist, ist festzustellen, dass nach Art. 3 dieser Richtlinie in Verbindung mit ihrem Art. 5 Abs. 1 alle Verkehrsdaten betreffend Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie auf Vorrat zu speichern sind. Sie gilt somit für alle elektronischen Kommunikationsmittel, deren Nutzung stark verbreitet und im täglichen Leben jedes Einzelnen von wachsender Bedeutung ist. Außerdem erfasst die Richtlinie nach ihrem Art. 3 alle Teilnehmer und registrierten Benutzer. Sie führt daher zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung.

57 Hierzu ist erstens festzustellen, dass sich die Richtlinie 2006/24 generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckt, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen.

58 Die Richtlinie 2006/24 betrifft nämlich zum einen in umfassender Weise alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keinerlei Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen.

59 Zum anderen soll die Richtlinie zwar zur Bekämpfung schwerer Kriminalität beitragen, verlangt aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit; insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.

60 Zweitens kommt zu diesem generellen Fehlen von Einschränkungen hinzu, dass die Richtlinie 2006/24 kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die

im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen. Die Richtlinie 2006/24 nimmt im Gegenteil in ihrem Art. 1 Abs. 1 lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten schweren Straftaten Bezug.

61 Überdies enthält die Richtlinie 2006/24 keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung. Art. 4 der Richtlinie, der den Zugang dieser Behörden zu den auf Vorrat gespeicherten Daten regelt, bestimmt nicht ausdrücklich, dass der Zugang zu diesen Daten und deren spätere Nutzung strikt auf Zwecke der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung zu beschränken sind, sondern sieht lediglich vor, dass jeder Mitgliedstaat das Verfahren und die Bedingungen festlegt, die für den Zugang zu den auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.

62 Insbesondere sieht die Richtlinie 2006/24 kein objektives Kriterium vor, das es erlaubt, die Zahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späterer Nutzung befugt sind, auf das angesichts des verfolgten Ziels absolut Notwendige zu beschränken. Vor allem unterliegt der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht. Auch sieht die Richtlinie keine präzise Verpflichtung der Mitgliedstaaten vor, solche Beschränkungen zu schaffen.

63 Drittens schreibt die Richtlinie 2006/24 hinsichtlich der Dauer der Vorratsspeicherung in ihrem Art. 6 vor, dass die Daten für einen Zeitraum von mindestens sechs Monaten auf Vorrat zu speichern sind, ohne dass eine Unterscheidung zwischen den in Art. 5 der Richtlinie genannten Datenkategorien nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder anhand der betroffenen Personen getroffen wird.

64 Die Speicherungsfrist liegt zudem zwischen mindestens sechs Monaten und höchstens 24 Monaten, ohne dass ihre Festlegung auf objektiven Kriterien beruhen muss, die gewährleisten, dass sie auf das absolut Notwendige beschränkt wird.

65 Aus dem Vorstehenden folgt, dass die Richtlinie 2006/24 keine klaren und präzisen Regeln zur Tragweite des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte vorsieht. Somit ist festzustellen, dass die Richtlinie einen Eingriff in diese Grundrechte beinhaltet, der in der Rechtsordnung der Union von großem Ausmaß und von besonderer Schwere ist, ohne dass sie Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.

66 Darüber hinaus ist in Bezug auf die Regeln zur Sicherheit und zum Schutz der von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes auf Vorrat gespeicherten Daten festzustellen, dass die Richtlinie 2006/24 keine hinreichenden, den Anforderungen von Art. 8 der Charta entsprechenden Garantien dafür bietet, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder

unberechtigten Nutzung geschützt sind. Erstens sieht Art. 7 der Richtlinie 2006/24 keine speziellen Regeln vor, die der großen nach der Richtlinie auf Vorrat zu speichernden Datenmenge, dem sensiblen Charakter dieser Daten und der Gefahr eines unberechtigten Zugangs zu ihnen angepasst sind. Derartige Regeln müssten namentlich klare und strikte Vorkehrungen für den Schutz und die Sicherheit der fraglichen Daten treffen, damit deren Unversehrtheit und Vertraulichkeit in vollem Umfang gewährleistet sind. Auch sieht die Richtlinie keine präzise Verpflichtung der Mitgliedstaaten vor, solche Regeln zu schaffen.

67 Art. 7 der Richtlinie 2006/24 in Verbindung mit Art. 4 Abs. 1 der Richtlinie 2002/58 und Art. 17 Abs. 1 Unterabs. 2 der Richtlinie 95/46 gewährleistet nicht, dass die genannten Anbieter oder Betreiber durch technische und organisatorische Maßnahmen für ein besonders hohes Schutz- und Sicherheitsniveau sorgen, sondern gestattet es ihnen u. a., bei der Bestimmung des von ihnen angewandten Sicherheitsniveaus wirtschaftliche Erwägungen hinsichtlich der Kosten für die Durchführung der Sicherheitsmaßnahmen zu berücksichtigen. Vor allem gewährleistet die Richtlinie 2006/24 nicht, dass die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich vernichtet werden.

68 Zweitens schreibt die Richtlinie nicht vor, dass die fraglichen Daten im Unionsgebiet auf Vorrat gespeichert werden, so dass es nicht als vollumfänglich gewährleistet angesehen werden kann, dass die Einhaltung der in den beiden vorstehenden Randnummern angesprochenen Erfordernisse des Datenschutzes und der Datensicherheit, wie in Art. 8 Abs. 3 der Charta ausdrücklich gefordert, durch eine unabhängige Stelle überwacht wird. Eine solche Überwachung auf der Grundlage des Unionsrechts ist aber ein wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten (vgl. in diesem Sinne Urteil Kommission/Österreich, C-614/10, EU:C:2012:631, Rn. 37).

69 Aus der Gesamtheit der vorstehenden Erwägungen ist zu schließen, dass der Unionsgesetzgeber beim Erlass der Richtlinie 2006/24 die Grenzen überschritten hat, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta einhalten musste.

70 Unter diesen Umständen ist die Vereinbarkeit der Richtlinie 2006/24 mit Art. 11 der Charta nicht zu prüfen.

71 Infolgedessen ist auf die zweite Frage, Buchst. b bis d, in der Rechtssache C-293/12 und auf die erste Frage in der Rechtssache C-594/12 zu antworten, dass die Richtlinie 2006/24 ungültig ist.

*Zur ersten Frage, zur zweiten Frage, Buchst. a und e, und zur dritten Frage in der Rechtssache C-293/12 sowie zur zweiten Frage in der Rechtssache C-594/12*

72 Aus den Ausführungen in der vorstehenden Randnummer folgt, dass die erste Frage, die zweite Frage, Buchst. a und e, und die dritte Frage in der Rechtssache C-293/12 sowie die zweite Frage in der Rechtssache C-594/12 nicht zu beantworten sind.

## **Kosten**

73 Für die Parteien der Ausgangsverfahren ist das Verfahren ein Zwischenstreit in den bei den vorlegenden Gerichten anhängigen Rechtsstreitigkeiten; die Kostenentscheidung ist daher Sache dieser Gerichte. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

Aus diesen Gründen hat der Gerichtshof (Große Kammer) für Recht erkannt:

**Die 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 ist ungültig.**