GERICHTSHOF
DER EUROPÄISCHEN UNION

DIREKTION WISSENSCHAFTLICHER
DIENST UND DOKUMENTATION

Thematische Übersicht

SCHUTZ PERSONENBEZOGENER DATEN

Das Recht auf Schutz personenbezogener Daten ist ein Grundrecht, dessen Wahrung ein wichtiges Ziel der Europäischen Union ist.

Dieses Recht ist in der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) verankert, die in Art. 8 vorsieht:

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

Dieses Grundrecht ist ferner eng mit dem in Art. 7 der Charta verbürgten Recht auf Achtung des Privat- und Familienlebens verbunden.

Das Recht auf Schutz personenbezogener Daten ist außerdem in Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) verankert, der Nachfolgebestimmung von Art. 286 EG.

Was das Sekundärrecht angeht, so hat sich die Europäische Gemeinschaft ab Mitte der 1990er Jahre verschiedene Instrumente gegeben, mit denen der Schutz personenbezogener Daten sichergestellt werden soll. Der wichtigste Rechtsakt der Union auf diesem Gebiet ist die auf der Grundlage von Art. 100a EG erlassene Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1]. Sie legt die allgemeinen Bedingungen, unter denen die Verarbeitung dieser Daten rechtmäßig ist, und die Rechte der betroffenen Personen fest und sieht u. a. die Errichtung unabhängiger Kontrollbehörden in den Mitgliedstaaten vor.

1 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), konsolidierte Fassung vom 20.11.2003, aufgehoben zum 25. Mai 2018 (siehe Fn. 5).

Die Richtlinie 2002/58/EG[2] wurde sodann durch die Richtlinie 95/46/EG ergänzt, mit der die Vorschriften der Mitgliedstaaten zum Schutz des Rechts auf Privatsphäre insbesondere in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation harmonisiert wurden[3].

Auf dem Gebiet des Raums der Freiheit, der Sicherheit und des Rechts (früher Art. 30 und 31 EUV) regelt der Rahmenbeschluss 2008/977/JI[4] (bis Mai 2018) den Schutz personenbezogener Daten im Zusammenhang mit der justiziellen Zusammenarbeit in Straf- und Polizeisachen.

Die Europäische Union hat kürzlich einen neuen umfassenden datenschutzrechtlichen Rahmen erarbeitet. Zu diesem Zweck hat sie 2016 die Verordnung (EU) 2016/679[5] zum Datenschutz erlassen, die die Richtlinie 95/46/EG aufhebt und ab dem 25. Mai 2018 unmittelbar anwendbar sein wird, sowie die Richtlinie (EU) 2016/680[6] zum Schutz personenbezogener Daten in Strafsachen, die den Rahmenbeschluss 2008/977/JI aufhebt und von den Mitgliedstaaten bis zum 6. Mai 2018 umzusetzen ist.

Schließlich ist der Schutz personenbezogener Daten im Zusammenhang mit ihrer Verarbeitung durch die Organe und Einrichtungen der EU durch die Verordnung (EG) Nr. 45/2001[7] gewährleistet. Aufgrund dieser Verordnung wurde u. a. 2004 der Europäische Datenschutzbeauftragte berufen. Im Januar 2017 hat die Kommission einen Vorschlag[8] für eine neue Verordnung zur Aufhebung der Verordnung Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG vorgelegt, um die datenschutzrechtlichen Vorschriften zu modernisieren und an die neue, mit der Verordnung (EU) 2016/679 eingeführte Regelung anzupassen.

2 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), konsolidierte Fassung vom 19.12.2009.

3 Die Richtlinie 2002/58/EG wurde durch 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 (ABl. L 105 vom 13.4.2006, S. 54) geändert. Diese Richtlinie wurde vom Gerichtshof im Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u. a. (C-293/12 und C-594/12, EU:C:2014:238), mit der Begründung für ungültig erklärt, dass sie erheblich in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten eingreift (vgl. Abschnitt I.1. „Vereinbarkeit des abgeleiteten Unionsrechts mit dem Recht auf Schutz personenbezogener Daten" des vorliegenden Überblicks).

4 Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60), aufgehoben mit Wirkung vom 6. Mai 2018 (siehe Fn. 6).

5 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1), anwendbar ab dem 25. Mai 2018.

6 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

7 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. L 8 vom 12.1.2001, S. 1).

8 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (COM[2017] 8 final).

I. Das in der Charta der Grundrechte der Europäischen Union anerkannte Recht auf Schutz personenbezogener Daten

1. Vereinbarkeit des abgeleiteten Unionsrechts mit dem Recht auf Schutz personenbezogener Daten

Urteil vom 9. November 2010 (Große Kammer), Volker und Markus Schecke und Eifert (C-92/09 und C-93/09, EU:C:2010:662)[9]

In dieser Rechtssache standen sich in den Ausgangsrechtsstreitigkeiten Inhaber landwirtschaftlicher Betriebe und das Land Hessen wegen der Veröffentlichung personenbezogener Daten auf der Website der Bundesanstalt für Landwirtschaft und Ernährung gegenüber, die die Landwirte als Empfänger von Mitteln aus dem Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) betrafen. Die Landwirte widersprachen dieser Veröffentlichung und machten insbesondere geltend, dass sie nicht durch überwiegende Allgemeininteressen gerechtfertigt sei. Das Land Hessen war dagegen der Auffassung, dass sich die Veröffentlichung dieser Daten aus den Verordnungen (EG) Nr. 1290/2005[10] und 259/2008[11] ergebe, die die Finanzierung der gemeinsamen Agrarpolitik regeln und eine Veröffentlichung von Informationen über die Empfänger von EGFL- und ELER-Mitteln vorschreiben.

In diesem Zusammenhang legte das Verwaltungsgericht Wiesbaden dem Gerichtshof mehrere Fragen zur Gültigkeit bestimmter Vorschriften der Verordnung (EG) Nr. 1290/2005 und zur Gültigkeit der Verordnung (EG) Nr. 259/2008 vor, nach denen diese Informationen der Öffentlichkeit insbesondere über die Websites der nationalen Behörden zugänglich gemacht werden müssen.

Der Gerichtshof hat zur Abwägung zwischen dem in der Charta anerkannten Recht auf Schutz personenbezogener Daten und dem für die europäischen Fonds geltenden Transparenzgebot ausgeführt, dass die Veröffentlichung von Daten mit den Namen dieser Empfänger und den Beträgen, die sie erhalten haben, auf einer Internetseite einen Eingriff in ihr Recht auf Achtung ihres Privatlebens im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen darstellt, da Dritte Zugang zu diesen Daten erhalten (Rn. 56-64).

Dieser Eingriff ist nur gerechtfertigt, wenn er gesetzlich vorgesehen ist, den Wesensgehalt dieser Rechte achtet, gemäß dem Grundsatz der Verhältnismäßigkeit erforderlich ist und von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen tatsächlich entspricht, wobei sich die Ausnahmen und Einschränkungen in Bezug auf diese Rechte auf das absolut Notwendige beschränken müssen (Rn. 65). Hierzu hat der Gerichtshof ausgeführt, dass die Steuerzahler in einer demokratischen Gesellschaft zwar einen Anspruch darauf haben, über die Verwendung der öffentlichen Gelder informiert zu werden, dass der Rat und die Kommission jedoch eine ausgewogene Gewichtung der verschiedenen beteiligten Interessen vorzunehmen hatten. Vor dem Erlass der angefochtenen Bestimmungen war daher zu

9 Dieses Urteil wurde im Jahresbericht 2010, S. 11, dargestellt.

10 Verordnung (EG) Nr. 1290/2005 des Rates vom 21. Juni 2005 über die Finanzierung der Gemeinsamen Agrarpolitik (ABl. L 209 vom 11.8.2005, S. 1), aufgehoben durch die Verordnung (EU) Nr. 1306/2013 des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über die Finanzierung, die Verwaltung und das Kontrollsystem der Gemeinsamen Agrarpolitik (ABl. L 347 vom 20.12.2013, S. 549).

11 Verordnung (EG) Nr. 259/2008 der Kommission vom 18. März 2008 mit Durchführungsbestimmungen zur Verordnung Nr. 1290/2005 hinsichtlich der Veröffentlichung von Informationen über die Empfänger von Mitteln aus dem Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) (ABl. L 76 vom 19.3.2008, S. 28), aufgehoben durch die Durchführungsverordnung (EU) Nr. 908/2014 der Kommission vom 6. August 2014 mit Durchführungsbestimmungen zur Verordnung (EU) Nr. 1306/2013 des Europäischen Parlaments und des Rates hinsichtlich der Zahlstellen und anderen Einrichtungen, der Mittelverwaltung, des Rechnungsabschlusses und der Bestimmungen für Kontrollen, Sicherheiten und Transparenz (ABl. L 255 vom 28.8.2014, S. 59).

überprüfen, ob die Veröffentlichung dieser Daten durch den Mitgliedstaat auf einer Website nicht über das hinausgeht, was zur Erreichung der verfolgten berechtigten Ziele erforderlich ist (Rn. 77, 79, 85, 86).

Der Gerichtshof hat daher bestimmte Vorschriften der Verordnung (EG) Nr. 1290/2005 sowie die Verordnung (EG) Nr. 259/2008 insgesamt für ungültig erklärt, soweit diese Bestimmungen bei natürlichen Personen, die Empfänger von EGFL- und ELER-Mitteln sind, die Veröffentlichung personenbezogener Daten hinsichtlich aller Empfänger vorschreiben, ohne nach einschlägigen Kriterien wie den Zeiträumen, während deren sie solche Beihilfen erhalten haben, der Häufigkeit oder auch Art und Umfang dieser Beihilfen zu unterscheiden (Rn. 92, Tenor 1). Er hat allerdings nicht die Wirkungen der Veröffentlichung der Listen von Empfängern von EGFL- und ELER-Mitteln in Frage gestellt, die die nationalen Behörden in der Zeit vor dem Tag der Verkündung des Urteils vorgenommen haben (Urteil 94, Tenor 2).

Urteil vom 17. Oktober 2013, Schwarz (C-291/12, EU:C:2013:670)

Herr Schwarz hatte bei der Stadt Bochum (Deutschland) die Erteilung eines Reisepasses beantragt, die Erfassung seiner Fingerabdrücke jedoch verweigert. Da die Stadt seinen Antrag ablehnte, erhob Herr Schwarz beim Verwaltungsgericht Gelsenkirchen (Deutschland) eine Klage mit dem Begehren, die Stadt Bochum zu verpflichten, ihm einen Reisepass zu erteilen, ohne seine Fingerabdrücke zu erfassen. Er berief sich dabei auf die Ungültigkeit der Verordnung (EG) Nr. 2252/2004[12], mit der die Pflicht zur Erfassung der Fingerabdrücke der einen Reisepass beantragenden Personen eingeführt worden war, und machte u. a. geltend, dass diese Verordnung gegen das Recht auf Schutz personenbezogener Daten und das Recht auf Achtung des Privatlebens verstoße

In diesem Zusammenhang legte das Verwaltungsgericht Gelsenkirchen dem Gerichtshof ein Vorabentscheidungsersuchen vor, um zu klären, ob die Verordnung, soweit sie die einen Reisepass beantragende Personen verpflichtet, ihre Fingerabdrücke abzugeben, und deren Speicherung im Reisepass vorsieht, insbesondere im Hinblick auf die Charta gültig ist.

Der Gerichtshof hat dies bejaht. Er hat entschieden, dass die in Art. 1 Abs. 2 der Verordnung (EG) Nr. 2252/2004 geregelte Erfassung und Speicherung von Fingerabdrücken durch die nationalen Behörden zwar einen Eingriff in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen, dass dieser Eingriff jedoch durch das Ziel, zu verhindern, dass Reisepässe betrügerisch verwendet werden, gerechtfertigt ist.

Zunächst wird mit einer solchen gesetzlich vorgesehenen Einschränkung eine von der Union anerkannte dem Gemeinwohl dienende Zielsetzung verfolgt, da insbesondere die illegale Einreise von Personen in das Unionsgebiet verhindert werden soll (Rn. 35-38). Sodann sind die Erfassung und Speicherung der Fingerabdrücke zur Erreichung dieses Ziels geeignet. Denn zum einen ist die Methode zur Überprüfung der Identität anhand von Fingerabdrücken zwar nicht völlig zuverlässig, sie vermindert die Gefahr einer Akzeptanz unbefugter Personen jedoch erheblich. Zum anderen bedeutet die mangelnde Übereinstimmung der Fingerabdrücke des Reisepassinhabers mit den in den Pass aufgenommenen Daten nicht, dass ihm die Einreise in das Unionsgebiet automatisch verweigert würde, sondern nur, dass eine eingehende Überprüfung vorgenommen wird, um seine Identität endgültig zu klären (Rn. 42-45).

12 Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (ABl. L 385 vom 29.12.2004, S. 1) in der durch die Verordnung (EG) Nr. 444/2009 des Europäischen Parlaments und des Rates vom 6. Mai 2009 (ABl. L 142 vom 6.6.2009, S. 1) geänderten Fassung.

Schließlich wurden, was die Erforderlichkeit einer solchen Verarbeitung betrifft, dem Gerichtshof keine hinreichend wirksamen Maßnahmen zur Kenntnis gebracht, die weniger schwerwiegend in die durch die Art. 7 und 8 der Charta anerkannten Rechte eingriffen als das auf den Fingerabdrücken beruhende Verfahren (Rn. 53). Art. 1 Abs. 2 der Verordnung (EG) Nr. 2252/2004 bringt keine Verarbeitung erfasster Fingerabdrücke mit sich, die über das zur Erreichung des verfolgten Ziels Erforderliche hinausgeht. Denn nach der Verordnung dürfen die Fingerabdrücke nur zu dem Zweck verwendet werden, die Authentizität des Passes und die Identität seines Inhabers zu überprüfen. Außerdem bietet Art. 1 Abs. 2 der Verordnung einen Schutz vor der Gefahr, dass Fingerabdruckdaten von Unbefugten gelesen werden, und sieht die Speicherung der Fingerabdrücke nur im Pass selbst vor, der im ausschließlichen Besitz seines Inhabers bleibt (Rn. 54-57, 60, 63).

Urteil vom 8. April 2014 (Große Kammer), Digital Rights Ireland und Seitlinger u. a. (Rechtssachen C-293/12 und C-594/12, EU:C:2014:238)[13]

Diesem Urteil lagen Anträge auf Überprüfung der Gültigkeit der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten anhand der Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten zugrunde, die im Rahmen innerstaatlicher Rechtsstreitigkeiten vor einem irischen und einem österreichischen Gericht gestellt worden waren. In der Rechtssache C-293/12 war der High Court (Hohes Gericht, Irland) mit einem Rechtsstreit zwischen dem Unternehmen Digital Rights und den irischen Behörden über die Rechtmäßigkeit nationaler Maßnahmen zur Vorratsspeicherung von Daten elektronischer Kommunikationsvorgänge befasst worden. In der Rechtssache C-594/12 war der Verfassungsgerichtshof (Österreich) mit mehreren Anträgen auf Nichtigerklärung der nationalen Bestimmung zur Umsetzung der Richtlinie 2006/24/EG in das österreichische Recht befasst worden.

Mit ihren Vorabentscheidungsersuchen befragten das irische und das österreichische Gericht den Gerichtshof zur Gültigkeit der Richtlinie 2006/24/EG im Hinblick auf die Art. 7, 8 und 11 der Charta. Sie wollten insbesondere wissen, ob die nach der Richtlinie den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste und den Betreibern eines öffentlichen Kommunikationsnetzes obliegende Pflicht, Daten über das Privatleben einer Person und ihre Kommunikationsvorgänge während eines bestimmten Zeitraums auf Vorrat zu speichern und den zuständigen nationalen Behörden Zugang zu gewähren, einen ungerechtfertigten Eingriff in die genannten Grundrechte darstellen. Dabei geht es 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, 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.

Der Gerichtshof hat zunächst entschieden, dass die Bestimmungen der Richtlinie 2006/24/EG dadurch, dass sie diesen Anbietern und Betreibern solche Verpflichtungen auferlegen, besonders schwerwiegend in die durch die Art. 7 und 8 der Charta garantierten Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten eingreifen. In diesem Zusammenhang hat er festgestellt, dass dieser Eingriff zwar mit einer dem Gemeinwohl dienenden Zielsetzung, wie der Bekämpfung der organisierten Kriminalität, gerechtfertigt werden kann. In diesem Zusammenhang hat der Gerichtshof erstens festgestellt, dass die nach der Richtlinie vorgeschriebene Vorratsspeicherung von Daten nicht geeignet ist, den Wesensgehalt dieser Grundrechte anzutasten, da die Richtlinie die Kenntnisnahme des Inhalts

13 Dieses Urteil wurde im Jahresbericht 2014, S. 60, dargestellt.

elektronischer Kommunikation als solchen nicht gestattet und vorsieht, dass die Anbieter und Betreiber bestimmte Grundsätze des Datenschutzes und der Datensicherheit einhalten müssen. Zweitens entspricht die Vorratsspeicherung von Daten im Hinblick auf deren etwaige Weitergabe an die zuständigen nationalen Behörden tatsächlich einer dem Gemeinwohl dienenden Zielsetzung, nämlich der Bekämpfung schwerer Kriminalität und somit letztlich der öffentlichen Sicherheit (Rn. 38-44).

Der Gerichtshof ist jedoch zu dem Ergebnis gelangt, dass der Unionsgesetzgeber beim Erlass der Richtlinie über die Vorratsdatenspeicherung die Grenzen überschritten hatte, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit einhalten musste. Daher hat er die Richtlinie für ungültig erklärt, da sie einen Eingriff in diese Grundrechte beinhaltet, der 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 (Rn. 65). Die Richtlinie 2006/24/EG erstreckte sich nämlich generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen (Rn. 57-59). Die Richtlinie sah ferner kein objektives Kriterium vor, 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 als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen, und enthielt auch keine materiell- und verfahrensrechtlichen Voraussetzungen für diesen Zugang oder diese Nutzung (Rn. 60-62). Schließlich sah die Richtlinie zur Dauer der Vorratsspeicherung einen Zeitraum von mindestens sechs Monaten vor, ohne zwischen den Datenkategorien anhand der betroffenen Personen oder nach Maßgabe des etwaigen Nutzens der Daten für das verfolgte Ziel zu unterscheiden (Rn. 63, 64).

Der Gerichtshof hat ferner zu den sich aus Art. 8 Abs. 3 der Charta ergebenden Anforderungen festgestellt, dass die Richtlinie 2006/24/EG keine hinreichenden Garantien dafür bot, dass die Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung geschützt sind, und auch keine Speicherung der Daten im Unionsgebiet vorschrieb.

Die Richtlinie gewährleistete damit nicht in vollem Umfang, dass die Einhaltung der Erfordernisse des Datenschutzes und der Datensicherheit durch eine unabhängige Stelle überwacht wird, obwohl die Charta dies ausdrücklich fordert (Rn. 66-68).

2. Wahrung des Rechts auf Schutz personenbezogener Daten bei der Umsetzung des Unionsrechts

Urteil vom 21. Dezember 2016 (Große Kammer), Tele2 Sverige (verbundene Rechtssachen C-203/15 und C-698/15, EU:C:2016:970)[14]

Nachdem die Richtlinie 2006/24/EG mit dem Urteil Digital Rights Ireland und Seitlinger u. a. für ungültig erklärt worden war (siehe oben), wurde der Gerichtshof mit zwei Rechtssachen befasst, in denen es um die in Schweden und im Vereinigten Königreich den Betreibern elektronischer Kommunikationsdienste auferlegte Pflicht zur Vorratsdatenspeicherung ging, die in der ungültig erklärten Richtlinie vorgesehen war.

14 Dieses Urteil wurde im Jahresbericht 2016, S. 62, dargestellt.

Am Tag nach der Verkündung des Urteils Digital Rights Ireland und Seitlinger u. a. teilte das Telekommunikationsunternehmen Tele2 Sverige der schwedischen Überwachungsbehörde Post und Telekommunikation mit, dass es die Vorratsspeicherung von Daten einstellen werde und beabsichtige, die bereits gespeicherten Daten zu löschen (Rechtssache C-203/15). Nach schwedischem Recht sind die Betreiber elektronischer Kommunikationsdienste nämlich verpflichtet, systematisch und kontinuierlich, und dies ohne jede Ausnahme, sämtliche Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel zu speichern. In der Rechtssache C-698/15 hatten drei Personen gegen die britische Regelung über die Vorratsdatenspeicherung geklagt, die den Innenminister ermächtigt, die Betreiber öffentlicher Telekommunikationsdienste zu verpflichten, sämtliche Kommunikationsdaten für bis zu zwölf Monate auf Vorrat zu speichern, wobei die Speicherung des Inhalts der Kommunikationsvorgänge ausgeschlossen ist.

Der Gerichtshof wurde vom Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm, Schweden) und vom Court of Appeal (England and Wales) (Civil Division) (Berufungsgericht [England & Wales] [Abteilung für Zivilsachen], Vereinigtes Königreich) um Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) ersucht, der es den Mitgliedstaaten erlaubt, Ausnahmen von der in der Richtlinie aufgestellten Pflicht vorzusehen, die Vertraulichkeit der elektronischen Kommunikation und der damit verbundenen Verkehrsdaten sicherzustellen.

In seinem Urteil hat der Gerichtshof zunächst entschieden, dass Art. 15 Abs. 1 der Richtlinie 2002/58/EG im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta betrachtet einer nationalen Regelung wie der schwedischen entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht. Eine solche Regelung überschreitet nämlich die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 Abs. 1 der Richtlinie im Licht der genannten Artikel der Charta verlangt (Rn. 99-105, 107, 112, Tenor 1).

Diese Vorschrift im Licht dieser Artikel der Charta betrachtet steht auch einer nationalen Regelung entgegen, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten, zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind (Rn. 118-122, 125, Tenor 2).

Dagegen steht Art. 15 Abs. 1 der Richtlinie 2002/58/EG nicht einer nationalen Regelung entgegen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist. Um diesen Erfordernissen zu genügen, muss die nationale Regelung erstens klare und präzise Regeln aufstellen, um einen wirksamen Schutz der Daten vor Missbrauchsrisiken zu ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird. Zweitens muss die Vorratsspeicherung der Daten, was die materiellen Voraussetzungen angeht, die eine nationale Regelung erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen. Bei dieser Begrenzung muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren

Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern (Rn. 108-111).

II. Verarbeitung personenbezogener Daten im Sinne der Richtlinie 95/46/EG

1. Vom Anwendungsbereich der Richtlinie 95/46/EG ausgenommene Verarbeitungen

Urteil vom 30. Mai 2006 (Große Kammer), Parlament/Rat (C-317/04 und C-318/04, EU:C:2006:346)

Nach den Terroranschlägen vom 11. September 2001 erließen die Vereinigten Staaten Rechtsvorschriften, wonach Fluggesellschaften, die Flüge in die oder aus den Vereinigten Staaten oder über deren Gebiet durchführen, den amerikanischen Behörden einen elektronischen Zugriff auf die Daten ihrer automatischen Reservierungs- und Abfertigungssysteme, die sogenannten „Passenger Name Records" (PNR), gewähren müssen.

Da die Kommission der Auffassung war, dass diese Bestimmungen mit den europäischen und mitgliedstaatlichen Rechtsvorschriften über den Datenschutz in Konflikt geraten könnten, nahm sie Verhandlungen mit den amerikanischen Behörden auf und erließ nach Abschluss dieser Verhandlungen am 14. Mai 2004 die Entscheidung 2004/535/EG[15], mit der festgestellt wurde, dass die Zoll- und Grenzschutzbehörde der Vereinigten Staaten (United States Bureau of Customs and Border Protection, im Folgenden: CBP) einen angemessenen Schutz für PNR-Daten gewährleistet, die aus der Gemeinschaft übermittelt werden (die Angemessenheitsentscheidung). Daraufhin erließ der Rat am 17. Mai 2004 den Beschluss 2004/496/EG[16], mit dem der Abschluss eines Abkommens zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten über die Verarbeitung von PNR-Daten und deren Übermittlung durch die im Hoheitsgebiet der Mitgliedstaaten der Gemeinschaft ansässigen Fluggesellschaften an das CBP genehmigt wurde.

Das Europäische Parlament beantragte beim Gerichtshof, die Entscheidung und den Beschluss für nichtig zu erklären, und machte insbesondere geltend, die Angemessenheitsentscheidung sei ultra vires ergangen, Art. 95 EG (jetzt Art. 114 AEUV) sei keine geeignete Rechtsgrundlage für den Beschluss über die Genehmigung des Abkommens, und Grundrechte seien verletzt

In Bezug auf die Angemessenheitsentscheidung hat der Gerichtshof zunächst geprüft, ob die Kommission ihre Entscheidung auf der Grundlage der Richtlinie 95/46/EG erlassen durfte. In diesem Zusammenhang hat er festgestellt, dass sich aus der Angemessenheitsentscheidung ergibt, dass die Übermittlung der PNR-Daten an das CBP eine Verarbeitung darstellt, die die öffentliche Sicherheit und die Tätigkeiten des Staates im strafrechtlichen Bereich betrifft. Zwar sind diese Daten ursprünglich von

15 Entscheidung 2004/535/EG der Kommission vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden (ABl. L 235 vom 6.7.2004, S. 11).

16 Beschluss 2004/496/EG des Rates vom 17. Mai 2004 über den Abschluss eines Abkommens zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security (ABl. L 183 vom 20.5.2004, S. 83, berichtigt im ABl. L 255 vom 30.9.2005, S. 168).

den Fluggesellschaften im Rahmen einer unter das Unionsrecht fallenden Tätigkeit erhoben worden, nämlich beim Verkauf eines Flugscheins, der zu einer Dienstleistung berechtigt; die Datenverarbeitung, um die es in der Angemessenheitsentscheidung geht, ist jedoch von ganz anderer Art. Denn diese Entscheidung bezieht sich nicht auf eine Datenverarbeitung, die für die Erbringung einer Dienstleistung erforderlich ist, sondern auf eine Datenverarbeitung, die zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken erforderlich angesehen wird (Rn. 56, 57).

Der Gerichtshof hat darauf hingewiesen, dass aus der Tatsache, dass es private Wirtschaftsteilnehmer sind, die die PNR-Daten zu gewerblichen Zwecken erhoben haben und in einen Drittstaat übermitteln, nicht folgt, dass diese Übermittlung vom Anwendungsbereich der Richtlinie ausgenommen ist. Die Übermittlung findet nämlich in einem von staatlichen Stellen geschaffenen Rahmen statt und dient der öffentlichen Sicherheit. Der Gerichtshof hat daher festgestellt, dass die Angemessenheitsentscheidung nicht in den Anwendungsbereich der Richtlinie fällt, da sie eine davon ausgenommene Verarbeitung personenbezogener Daten betraf. Er hat sie daher für nichtig erklärt (Rn. 58, 59).

Zum Beschluss des Rates hat der Gerichtshof festgestellt, dass Art. 95 EG in Verbindung mit Art. 25 der Richtlinie 95/46/EG die Zuständigkeit der Gemeinschaft für den Abschluss des fraglichen Abkommens mit den Vereinigten Staaten nicht begründen kann. Das Abkommen betrifft nämlich die gleiche Datenübermittlung wie die Angemessenheitsentscheidung und damit vom Anwendungsbereich der Richtlinie ausgenommene Datenverarbeitungen. Der Gerichtshof hat daher auch den Beschluss des Rates zur Genehmigung des Abschlusses des Abkommens für nichtig erklärt (Rn. 67-69).

Urteil vom 11. Dezember 2014, Ryneš (C-212/13, EU:C:2014:2428)

Als Reaktion auf wiederholte Angriffe hatte Herr Ryneš an seinem Haus eine Überwachungskamera angebracht. Nach einem neuen Angriff auf sein Haus konnten anhand der Kameraaufzeichnungen zwei Verdächtige identifiziert werden, gegen die Strafverfahren eingeleitet wurden. Einer der Verdächtigten machte vor dem tschechischen Amt für den Schutz personenbezogener Daten geltend, dass die Verarbeitung der von der Kamera aufgezeichneten Daten nicht rechtmäßig sei. Das Amt stellte fest, dass Herr Ryneš gegen die Vorschriften über den Schutz personenbezogener Daten verstoßen habe, und erlegte ihm eine Geldbuße auf.

Der Nejvyšší správní soud (Oberstes Verwaltungsgericht, Tschechische Republik), bei dem Herr Ryneš ein Rechtsmittel gegen das Urteil des Městský soud v Praze (Stadtgericht Prag), mit dem die Entscheidung des Amtes bestätigt worden war, eingelegt hatte, wollte vom Gerichtshof wissen, ob die Aufzeichnung, die Herr Ryneš vorgenommen hat, um sein Leben, seine Gesundheit und sein Eigentum zu schützen, eine Datenverarbeitung darstellt, die nicht von der Richtlinie 95/46/EG erfasst wird, weil die Aufzeichnung von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten im Sinne von Art. 3 Abs. 2 zweiter Gedankenstrich der Richtlinie vorgenommen wurde.

Der Gerichtshof hat entschieden, dass der Betrieb eines von einer natürlichen Person an ihrem Einfamilienhaus zum Schutz von Eigentum, Gesundheit und Leben der Besitzer des Hauses angebrachten Kamerasystems, das Videos von Personen auf einer kontinuierlichen Speichervorrichtung wie einer Festplatte aufzeichnet und dabei auch den öffentlichen Raum überwacht, keine Datenverarbeitung darstellt, die im Sinne dieser Bestimmung zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird (Rn. 35 und Tenor).

In diesem Zusammenhang hat der Gerichtshof ausgeführt, dass der Schutz des in Art. 7 garantierten Grundrechts auf Privatleben verlangt, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das absolut Notwendige beschränken. Da die Bestimmungen der Richtlinie 95/46/EG, soweit sie Verarbeitungen personenbezogener Daten betreffen, die zu Beeinträchtigungen der Grundfreiheiten und insbesondere des Rechts auf Achtung des Privatlebens

führen können, im Licht der Grundrechte auszulegen sind, die in der Charta verankert sind, ist die in Art. 3 Abs. 2 zweiter Gedankenstrich dieser Richtlinie vorgesehene Ausnahme eng auszulegen (Rn. 27-29). Bereits nach dem Wortlaut dieser Bestimmung ist von der Richtlinie 95/46/EG nur die Datenverarbeitung ausgenommen, die zur Ausübung von Tätigkeiten vorgenommen wird, die „ausschließlich" persönlicher oder familiärer Art sind. Soweit sich eine Videoüberwachung aber auch nur teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten auf diese Weise verarbeitet, kann sie nicht als eine ausschließlich „persönliche oder familiäre" Tätigkeit im Sinne dieser Bestimmung angesehen werden (Rn. 30, 31, 33).

2. Begriff „personenbezogene Daten"

Urteil vom 19. Oktober 2016, Breyer (C-582/14, EU:C:2016:779)[17]

Herr Breyer hatte bei den deutschen Zivilgerichten eine Klage erhoben, mit der er beantragte, der Bundesrepublik Deutschland zu untersagen, elektronische Daten, die am Ende jedes Zugriffs auf Websites von Einrichtungen des Bundes übertragen werden, zu speichern oder durch Dritte speichern zu lassen. Um Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen, zeichnete der Anbieter von Online-Mediendiensten der deutschen Bundesbehörden Daten auf, die in einer „dynamischen" IP-Adresse – eine IP-Adresse, die sich bei jeder neuen Internetverbindung ändert – und dem Zeitpunkt des über sie vorgenommenen Zugriffs auf eine Website bestehen. Anders als statische IP-Adressen erlauben dynamische IP-Adressen es nicht, anhand allgemein zugänglicher Dateien eine Verbindung zwischen einem Computer und dem vom Internetzugangsanbieter verwendeten physischen Netzanschluss herzustellen. Die aufgezeichneten Daten bieten für sich genommen dem Anbieter nicht die Möglichkeit, den Nutzer zu bestimmen. Er verfügt jedoch über Zusatzinformationen, die – in Verbindung mit dieser IP-Adresse – eine Bestimmung des Nutzers ermöglichen würden.

In diesem Zusammenhang wollte der mit einer Revision befasste Bundesgerichtshof (Deutschland) vom Gerichtshof wissen, ob eine IP-Adresse, die ein Anbieter von Online-Mediendiensten im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen ein personenbezogenes Datum darstellt.

Der Gerichtshof hat zunächst ausgeführt, dass für die Einstufung eines Datums als „personenbezogenes Datum" im Sinne von Art. 2 Buchst. a der Richtlinie 95/46/EG nicht erforderlich ist, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden. Dass über die zur Identifizierung des Nutzers einer Website erforderlichen Zusatzinformationen nicht der Anbieter von Online-Mediendiensten verfügt, sondern der Internetzugangsanbieter dieses Nutzers, vermag somit nicht auszuschließen, dass die von einem Anbieter von Online-Mediendiensten gespeicherten dynamischen IP-Adressen für ihn personenbezogene Daten im Sinne von Art. 2 Buchst. a der Richtlinie 95/46/EG darstellen (Rn. 43, 44).

Der Gerichtshof hat daher festgestellt, dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne von Art. 2 Buchst. a der Richtlinie 95/46/EG darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen (Rn. 49, Tenor 1).

17 Dieses Urteil wurde im Jahresbericht 2016, S. 61, dargestellt.

Urteil vom 20. Dezember 2017, Nowak (C-434/16, EU:C:2017:582)

Herr Nowak, ein Wirtschaftsprüfer/Steuerberater in Ausbildung, hatte die Prüfung des irischen Berufsverbands der Wirtschaftsprüfer/Steuerberater nicht bestanden. Er beantragte nach Art. 4 des irischen Datenschutzgesetzes Zugang zu sämtlichen ihn betreffenden und im Besitz des Berufsverbands befindlichen personenbezogenen Daten. Der Berufsverband übermittelte ihm einige Dokumente, weigerte sich aber, ihm seine Prüfungsarbeit herauszugeben, und zwar mit der Begründung, dass diese keine ihn betreffenden personenbezogenen Daten im Sinne des Datenschutzgesetzes enthalte.

Nachdem der Datenschutzbeauftragte seinen Antrag aus denselben Gründen ebenfalls abgelehnt hatte, wandte sich Herr Nowak an die nationalen Gerichte. Der Supreme Court (Oberster Gerichtshof, Irland), der mit einem von Herrn Nowak eingelegten Rechtsmittel befasst war, wollte vom Gerichtshof wissen, ob Art. 2 Buchst. a der Richtlinie 95/46/EG dahin auszulegen ist, dass unter Umständen wie denen des Ausgangsverfahrens die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung und etwaige Anmerkungen des Prüfers dazu „personenbezogene Daten" im Sinne dieser Bestimmung darstellen.

Der Gerichtshof hat erstens darauf hingewiesen, dass es, um Daten als „personenbezogene Daten" im Sinne von Art. 2 Buchst. a der Richtlinie 95/46/EG qualifizieren zu können, nicht erforderlich ist, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden. In dem Fall, dass dem Prüfer die Identität des Prüflings bei der Bewertung der von diesem bei einer Prüfung gegebenen Antworten nicht bekannt ist, ist die die Prüfung organisierende Einrichtung im Besitz der notwendigen Informationen, die es ihr ermöglichen, den Prüfling unschwer und zweifelsfrei anhand seiner auf der Prüfungsarbeit oder deren Deckblatt angebrachten Kennnummer zu identifizieren und ihm seine Antworten zuzuordnen.

Zweitens hat der Gerichtshof ausgeführt, dass die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung Informationen darstellen, die mit seiner Person verknüpft sind. Der Inhalt dieser Antworten spiegelt nämlich den Kenntnisstand und das Kompetenzniveau des Prüflings in einem bestimmten Bereich sowie gegebenenfalls seine Gedankengänge, sein Urteilsvermögen und sein kritisches Denken wider. Des Weiteren zielt die Sammlung dieser Antworten darauf ab, die beruflichen Fähigkeiten des Prüflings und seine Eignung zur Ausübung des betreffenden Berufs zu beurteilen. Schließlich kann sich die Verwendung dieser Informationen, die insbesondere im Erfolg oder Scheitern des Prüflings bei der Prüfung zum Ausdruck kommt, insoweit auf dessen Rechte und Interessen auswirken, als sie beispielsweise seine Chancen, den gewünschten Beruf zu ergreifen oder die gewünschte Anstellung zu erhalten, bestimmen oder beeinflussen kann. Die Feststellung, dass die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung Informationen darstellen, die aufgrund ihres Inhalts, ihres Zwecks und ihrer Auswirkungen Informationen über diesen Prüfling darstellen, gilt im Übrigen auch dann, wenn es sich um eine Prüfung handelt, bei der Dokumente benutzt werden dürfen.

Drittens hat der Gerichtshof hinsichtlich der Anmerkungen des Prüfers zu den Antworten des Prüflings darauf hingewiesen, dass diese – ebenso wie die Antworten des Prüflings in der Prüfung – Informationen über diesen darstellen, da im Inhalt dieser Anmerkungen die Ansicht oder Beurteilung des Prüfers in Bezug auf die individuelle Leistung des Prüflings in der Prüfung und insbesondere in Bezug auf dessen Kenntnisse und Kompetenzen in dem betreffenden Bereich zum Ausdruck kommen. Die Anmerkungen zielen im Übrigen gerade darauf ab, die Beurteilung der Leistung des Prüflings durch den Prüfer zu dokumentieren, und können Auswirkungen auf den Prüfling haben.

Viertens hat der Gerichtshof entschieden, dass die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung und etwaige Anmerkungen des Prüfers dazu somit – insbesondere im Hinblick auf ihre Richtigkeit und die Notwendigkeit ihrer Aufbewahrung – einer Überprüfung im Sinne von Art. 6 Abs. 1 Buchst. d und e der Richtlinie 95/46/EG zugänglich sind und gemäß deren Art. 12 Buchst. b

berichtigt oder gelöscht werden können. Dass einem Prüfling gemäß Art. 12 Buchst. a dieser Richtlinie ein Recht auf Auskunft hinsichtlich dieser Antworten und dieser Anmerkungen eingeräumt wird, dient dem Ziel der Richtlinie, den Schutz des Rechts auf Privatsphäre des Prüflings in Bezug auf die Verarbeitung der ihn betreffenden Daten zu garantieren, und zwar unabhängig davon, ob ihm auch nach den auf das Prüfungsverfahren anwendbaren nationalen Rechtsvorschriften ein solches Auskunftsrecht zusteht. Die Rechte auf Auskunft und Berichtigung nach Art. 12 Buchst. a und b der Richtlinie 95/46/EG erstrecken sich allerdings nicht auf Prüfungsfragen, die als solche keine personenbezogenen Daten des Prüflings darstellen.

Der Gerichtshof ist demnach zu dem Schluss gelangt, dass unter Umständen wie denen des Ausgangsverfahrens die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung und etwaige Anmerkungen des Prüfers zu diesen Antworten „personenbezogene Daten" im Sinne von Art. 2 Buchst. a der Richtlinie 95/46/EG darstellen.

3. Begriff „Verarbeitung personenbezogener Daten"

Urteil vom 6. November 2003 (Plenum), Lindqvist (C-101/01, EU:C:2003:596)

Frau Lindqvist, die in einer Gemeinde der protestantischen Kirche von Schweden ehrenamtlich tätig war, hatte auf ihrem eigenen Computer Internetseiten eingerichtet und darauf personenbezogene Daten mehrerer Personen veröffentlicht, die wie sie ehrenamtlich in der Gemeinde tätig waren. Frau Lindqvist wurde zur Zahlung einer Geldstrafe verurteilt, da sie personenbezogene Daten in einem automatisierten Verfahren verarbeitet habe, ohne dies zuvor der schwedischen Datainspektion (öffentliche Einrichtung zum Schutz von auf elektronischem Wege übermittelten Daten) gemeldet zu haben, diese Daten ohne Genehmigung in Drittländer übermittelt und sensible personenbezogene Daten verarbeitet habe.

Im Rahmen des von Frau Lindqvist gegen diese Entscheidung beim Göta hovrätt (Berufungsgericht, Schweden) eingelegten Rechtsmittels ersuchte dieses Gericht den Gerichtshof, im Wege der Vorabentscheidung die Frage zu klären, ob Frau Lindqvist eine „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten" im Sinne der Richtlinie 95/46/EG vorgenommen hatte.

Der Gerichtshof hat entschieden, dass die Handlung, die darin besteht, auf einer Internetseite auf verschiedene Personen hinzuweisen und diese entweder durch ihren Namen oder auf andere Weise, etwa durch Angabe ihrer Telefonnummer oder durch Informationen über ihr Arbeitsverhältnis oder ihre Freizeitbeschäftigungen, erkennbar zu machen, eine „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten" im Sinne dieser Richtlinie darstellt (Rn. 27, Tenor 1). Denn eine solche Verarbeitung personenbezogener Daten, die zur Ausübung von ehrenamtlichen und religionsgemeinschaftlichen Tätigkeiten erfolgt, ist von keiner der in der Richtlinie vorgesehenen Ausnahmen von ihrem Anwendungsbereich erfasst, da sie sich weder auf Tätigkeiten, die die öffentliche Sicherheit betreffen, noch auf ausschließlich persönliche oder familiäre Tätigkeiten bezieht, die nicht unter die Richtlinie fallen (Rn. 38, 43-48, Tenor 2).

Urteil vom 13. Mai 2014 (Große Kammer), Google Spain und Google (C-131/12, EU:C:2014:317)

2010 hatte ein spanischer Staatsangehöriger bei der Agencia Española de Protección de Datos (spanische Datenschutzagentur, im Folgenden: AEPD) eine Beschwerde gegen die La Vanguardia Ediciones SL, die Herausgeberin einer in Spanien weitverbreiteten Tageszeitung, sowie gegen Google Spain und Google erhoben. Er machte geltend, dass bei Eingabe seines Namens in die Suchmaschine des Google-Konzerns den Internetnutzern in der Ergebnisliste Links zu zwei Seiten der La Vanguardia von 1998 angezeigt würden, auf denen u. a. die Versteigerung eines gepfändeten Grundstücks im Hinblick auf die

Begleichung seiner Schulden angekündigt worden sei. Mit seiner Beschwerde beantragte er zum einen, La Vanguardia aufzugeben, die fraglichen Seiten zu löschen oder zu ändern oder zum Schutz der Daten von bestimmten, von den Suchmaschinen zur Verfügung gestellten technischen Möglichkeiten Gebrauch zu machen. Zum anderen beantragte er, Google Spain oder Google aufzugeben, seine personenbezogenen Daten zu löschen oder zu verbergen, so dass sie weder in den Suchergebnissen noch in Links zu La Vanguardia erschienen.

Die AEPD wies die Beschwerde gegen La Vanguardia ab, da diese die fraglichen Informationen rechtmäßig veröffentlicht habe, gab ihr aber, was Google Spain und Google betraf, statt und forderte die beiden Unternehmen auf, die erforderlichen Maßnahmen zu ergreifen, um die Daten aus ihrem Index zu entfernen und den Zugang zu ihnen in Zukunft zu verhindern. Die Unternehmen klagten bei der Audiencia Nacional (Nationaler Gerichtshof, Spanien) auf Aufhebung der Entscheidung der AEPD, woraufhin das spanische Gericht dem Gerichtshof eine Reihe von Fragen zur Vorabentscheidung vorlegte.

Der Gerichtshof hatte damit den Begriff „Verarbeitung personenbezogener Daten" im Internet im Zusammenhang mit der Richtlinie 95/46/EG zu präzisieren.

Er hat entschieden, dass die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, sofern die Informationen personenbezogene Daten enthalten, als Verarbeitung personenbezogener Daten einzustufen ist. Er hat außerdem darauf hingewiesen, dass die in der Richtlinie genannten Vorgänge auch dann als Verarbeitung personenbezogener Daten einzustufen sind, wenn sie ausschließlich Informationen enthalten, die genauso bereits in den Medien veröffentlicht worden sind. Eine allgemeine Ausnahme von der Anwendung der Richtlinie in solchen Fällen würde die Richtlinie nämlich weitgehend leerlaufen lassen (Rn. 29, 30).

4. Voraussetzungen für die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten nach Art. 7 der Richtlinie 95/46/EG

Urteil vom 16. Dezember 2008 (Große Kammer), Huber (C-524/06, EU:C:2008:724)[18]

Das Bundesamt für Migration und Flüchtlinge (Deutschland) führte ein zentrales Ausländerregister, in dem bestimmte personenbezogene Daten von Ausländern zusammengefasst wurden, die sich für mehr als drei Monate in Deutschland aufhalten. Das Register wurde zu statistischen Zwecken und bei der Erfüllung der den Sicherheits-, Polizei- und Justizbehörden obliegenden Aufgaben im Bereich der Bekämpfung und Aufklärung strafbarer oder die öffentliche Sicherheit gefährdender Handlungen genutzt.

Herr Huber, ein österreichischer Staatsangehöriger, ließ sich 1996 in Deutschland nieder, um dort den Beruf des selbständigen Versicherungsagenten auszuüben. Da er sich durch die Verarbeitung der ihn betreffenden Daten im Ausländerregister diskriminiert fühlte, weil es eine solche Datenbank für deutsche Staatsangehörige nicht gab, beantragte er die Löschung dieser Daten.

18 Dieses Urteil wurde im Jahresbericht 2008, S. 45, dargestellt.

In diesem Zusammenhang befragte das mit dem Rechtsstreit befasste Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Deutschland) den Gerichtshof zur Vereinbarkeit der in diesem Register vorgenommenen Verarbeitung personenbezogener Daten mit dem Unionsrecht.

Der Gerichtshof hat zunächst darauf hingewiesen, dass das Aufenthaltsrecht eines Unionsbürgers im Hoheitsgebiet eines Mitgliedstaats, dessen Staatsangehörigkeit er nicht besitzt, nicht uneingeschränkt besteht, sondern Beschränkungen unterworfen werden darf. Daher ist der Gebrauch eines solchen Registers zur Unterstützung der mit der Anwendung aufenthaltsrechtlicher Vorschriften betrauten Behörden grundsätzlich legitim und angesichts seiner Natur mit dem in Art. 12 Abs. 1 EG (jetzt Art. 18 Abs. 1 AEUV) niedergelegten Verbot der Diskriminierung aus Gründen der Staatsangehörigkeit vereinbar. Ein solches Register darf jedoch keine anderen Informationen enthalten als die, die im Sinne der Richtlinie über den Schutz personenbezogener Daten zu diesem Zweck erforderlich sind (Rn. 54, 58, 59).

Zum Begriff der Erforderlichkeit der Verarbeitung im Sinne von Art. 7 Buchst. e der Richtlinie 95/46/EG hat der Gerichtshof zunächst ausgeführt, dass es sich dabei um einen autonomen Begriff des Unionsrechts handelt, der so auszulegen ist, dass er in vollem Umfang dem Ziel dieser Richtlinie, wie es in ihrem Art. 1 Abs. 1 definiert wird, entspricht. Er hat sodann festgestellt, dass ein System zur Verarbeitung personenbezogener Daten nur dann dem Unionsrecht entspricht, wenn es nur die Daten enthält, die für die Anwendung der entsprechenden Vorschriften durch die Behörden erforderlich sind, und sein zentralisierter Charakter eine effizientere Anwendung dieser Vorschriften in Bezug auf das Aufenthaltsrecht von Unionsbürgern erlaubt, die keine Staatsangehörigen dieses Mitgliedstaats sind.

Jedenfalls lassen sich die Speicherung und Verarbeitung personenbezogener Daten, die namentlich genannte Personen betreffen, im Rahmen eines solchen Registers zu statistischen Zwecken nicht als im Sinne von Art. 7 Buchst. e der Richtlinie 95/46/EG erforderlich ansehen (Rn. 52, 66, 68).

Zur Frage der Nutzung der in dem Register enthaltenen Daten zur Bekämpfung der Kriminalität hat der Gerichtshof insbesondere ausgeführt, dass mit diesem Ziel auf die Verfolgung von Verbrechen und Vergehen unabhängig von der Staatsangehörigkeit der Täter abgestellt wird. Für einen Mitgliedstaat kann die Situation seiner Staatsangehörigen im Hinblick auf das Ziel der Bekämpfung der Kriminalität somit nicht anders sein als die der Unionsbürger, die keine Staatsangehörigen dieses Mitgliedstaats sind und sich in seinem Hoheitsgebiet aufhalten. Daher ist die unterschiedliche Behandlung dieser Staatsangehörigen und dieser Unionsbürger durch die zur Bekämpfung der Kriminalität vorgenommene systematische Verarbeitung der personenbezogenen Daten allein der Unionsbürger, die keine Staatsangehörigen des betreffenden Mitgliedstaats sind, eine durch Art. 12 Abs. 1 EG untersagte Diskriminierung (Rn. 78-80).

Urteil vom 24. November 2011, ASNEF und FECEMD (C-468/10 und C-469/10, EU:C:2011:777)

Die Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und die Federación de Comercio Electrónico y Marketing Directo (FECEMD) hatten beim Tribunal Supremo (Oberster Gerichtshof, Spanien) eine verwaltungsgerichtliche Klage gegen mehrere Artikel des Real Decreto 1720/2007 erhoben, mit dem das Gesetz 15/1999 zur Umsetzung der Richtlinie 95/46/EG durchgeführt worden war.

Die ASNEF und die FECEMD waren der Ansicht, dass das spanische Recht für die Verarbeitung personenbezogener Daten ohne Einwilligung der betroffenen Person eine Voraussetzung aufstelle, die in der Richtlinie 95/46/EG nicht vorhanden sei, indem es verlange, dass die Daten „in öffentlich zugänglichen Quellen", wie sie in Art. 3 Buchst. j des Gesetzes 15/1999 aufgeführt seien, enthalten seien. Dieses Gesetz und das Real Decreto 1720/2007 schränkten den Anwendungsbereich von Art. 7 Buchst. f der Richtlinie 95/46/EG ein, der für die Verarbeitung personenbezogener Daten ohne Einwilligung der

betroffenen Person allein ein berechtigtes Interesse voraussetze, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen werde, denen die Daten übermittelt würden.

Hierzu hat der Gerichtshof zunächst ausgeführt, dass Art. 7 der Richtlinie 95/46/EG eine erschöpfende und abschließende Liste der Fälle vorsieht, in denen eine Verarbeitung personenbezogener Daten ohne Einwilligung der betroffenen Person als rechtmäßig angesehen werden kann. Die Mitgliedstaaten dürfen daher weder gemäß Art. 5 der Richtlinie andere als die in Art. 7 genannten Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten einführen noch durch zusätzliche Bedingungen die Tragweite der in Art. 7 aufgestellten Grundsätze ändern. Denn Art. 5 erlaubt den Mitgliedstaaten lediglich, nach Maßgabe des Kapitels II und damit des Art. 7 dieser Richtlinie die Voraussetzungen näher zu bestimmen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist (Rn. 30, 32, 33).

Im Einzelnen können die Mitgliedstaaten für die in Art. 7 Buchst. f der Richtlinie vorgesehene notwendige Abwägung der jeweiligen einander gegenüberstehenden Rechte und Interessen Leitlinien aufstellen. Sie können auch berücksichtigen, dass die Grundrechte der betroffenen Person durch die Datenverarbeitung unterschiedlich stark beeinträchtigt sein können, je nachdem, ob die fraglichen Daten bereits in öffentlich zugänglichen Quellen enthalten sind oder nicht (Rn. 44 und 46).

Der Gerichtshof hat jedoch festgestellt, dass es sich, wenn eine nationale Regelung die Verarbeitung bestimmter Kategorien personenbezogener Daten ausschließt, indem sie für diese Kategorien das Ergebnis der Abwägung der einander gegenüberstehenden Rechte und Interessen abschließend vorschreibt, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt, nicht mehr um eine nähere Bestimmung im Sinne von Art. 5 der Richtlinie 95/46/EG handelt. Der Gerichtshof hat daher entschieden, dass Art. 7 Buchst. f der Richtlinie 95/46/EG es verbietet, dass ein Mitgliedstaat kategorisch und verallgemeinernd die Verarbeitung bestimmter Kategorien personenbezogener Daten ausschließt, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen (Rn. 47, 48).

Urteil vom 19. Oktober 2016, Breyer (C-582/14, EU:C:2016:779)

In diesem Urteil (vgl. auch Abschnitt II.2. „Begriff ‚personenbezogene Daten'") hat sich der Gerichtshof auch zu der Frage geäußert, ob Art. 7 Buchst. f der Richtlinie 95/46/EG einer Bestimmung des nationalen Rechts entgegensteht, wonach ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden darf, soweit dies erforderlich ist, um die konkrete Inanspruchnahme des Telemediums durch den jeweiligen Nutzer zu ermöglichen und abzurechnen, und wonach der Zweck, die generelle Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung nicht über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann.

Der Gerichtshof hat entschieden, dass Art. 7 Buchst. f der Richtlinie 95/46/EG der fraglichen Regelung entgegensteht. Denn nach dieser Bestimmung ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie erforderlich ist zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Die deutsche Regelung schloss jedoch kategorisch und ganz allgemein die Verarbeitung bestimmter Kategorien personenbezogener Daten aus, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen. Damit schränkte sie unzulässigerweise die Tragweite dieses in Art. 7 Buchst. f der Richtlinie 95/46/EG aufgestellten Grundsatzes ein, indem sie es ausschließt, dass der Zweck, die generelle Funktionsfähigkeit von Online-Mediendiensten zu gewährleisten, Gegenstand einer Abwägung mit dem Interesse oder den Grundrechten und Grundfreiheiten der Nutzer sein kann (Rn. 62-64, Tenor 2).

Urteil vom 4. Mai 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

Dieser Rechtssache lag ein Rechtsstreit zwischen der lettischen Nationalpolizei und Rīgas satiksme, der Betreiberin der Oberleitungsbusse der Stadt Riga, über einen Antrag auf Übermittlung von Daten zur Identifizierung des Verursachers eines Verkehrsunfalls zugrunde. Ein Taxifahrer hatte sein Fahrzeug am Straßenrand angehalten. In dem Moment, als ein Oberleitungsbus der Rīgas satiksme an dem Taxi vorbeifuhr, öffnete der Fahrgast im Fond des Taxis die Tür, die an den Oberleitungsbus stieß und diesen beschädigte. Um eine zivilrechtliche Klage erheben zu können, verlangte Rīgas satiksme von der Nationalpolizei u. a. die Übermittlung von Daten zur Identifizierung des Unfallverursachers. Die Polizei verweigerte die Übermittlung der Identifikationsnummer und der Adresse des Fahrgasts sowie der Aussagen der Unfallbeteiligten, da die Unterlagen des Verwaltungsverfahrens, das zu Sanktionen geführt habe, nur an die Verfahrensbeteiligten herausgegeben werden dürften und, was die Identifikationsnummer und die Adresse angehe, die Herausgabe solcher Informationen nach dem Gesetz zum Schutz personenbezogener Daten verboten sei.

Unter diesen Umständen wollte die Augstākās tiesas Administratīvo lietu departaments (Oberster Gerichtshof, Abteilung für Verwaltungsstreitsachen, Lettland) vom Gerichtshof wissen, ob Art. 7 Abs. f der Richtlinie 95/46/EG dazu verpflichtet, einem Dritten personenbezogene Daten zu übermitteln, damit er vor einem Zivilgericht Klage auf Ersatz eines durch die Person, um deren Daten es geht, verursachten Schadens erheben kann, und ob deren Minderjährigkeit für die Auslegung der Vorschrift von Bedeutung ist.

Der Gerichtshof hat entschieden, dass Art. 7 Abs. f der Richtlinie 95/46/EG nicht dazu verpflichtet, einem Dritten personenbezogene Daten zu übermitteln, damit er vor einem Zivilgericht Klage auf Ersatz eines durch die betreffende Person verursachten Schadens erheben kann. Er würde der Übermittlung solcher Daten jedoch nicht entgegenstehen, wenn sie auf der Grundlage des nationalen Rechts unter Einhaltung der in ihm genannten Voraussetzungen erfolgen würde (Rn. 27, 34 und Tenor).

In diesem Zusammenhang hat der Gerichtshof ausgeführt, dass es – unter dem Vorbehalt der insoweit von dem nationalen Gericht durchzuführenden Überprüfungen – unter Umständen wie denen des Ausgangsverfahrens nicht gerechtfertigt erscheint, es nur deshalb abzulehnen, dem Geschädigten personenbezogene Daten, die für die Erhebung einer Schadensersatzklage gegen den Verursacher des Schadens oder gegebenenfalls Personen, die die elterliche Sorge ausüben, erforderlich sind, zu übermitteln, weil der Verursacher des Schadens minderjährig ist (Rn. 33).

Urteil vom 27. September 2017, Puškár (C-73/16, EU:C:2017:725)

Im Ausgangsrechtsstreit hatte Herr Puškár eine Klage beim Najvyšší súd Slovenskej republiky (Oberstes Gericht der Slowakischen Republik) erhoben, um der Finančné riaditel'stvo (Finanzdirektion) und allen nachgeordneten Finanzbehörden sowie dem Kriminálny úrad finančnej správy (Amt der Finanzverwaltung für Verbrechensbekämpfung) aufzugeben, seinen Namen nicht in die Liste aufzunehmen, auf der Personen aufgeführt sind, von der die Finanzdirektion annimmt, dass sie für andere als Strohmänner fungieren, die von der Finanzdirektion im Rahmen der Steuererhebung erstellt wurde und deren Aktualisierung von der Finanzdirektion, den ihr nachgeordneten Finanzämtern und dem Amt der Finanzverwaltung für Verbrechensbekämpfung sichergestellt wird (im Folgenden: streitige Liste). Außerdem hatte er beantragt, jede ihn betreffende Angabe aus diesen Listen und aus dem EDV-System der Finanzverwaltung zu entfernen.

Der Najvyšší súd wollte in diesem Zusammenhang vom Gerichtshof wissen, ob das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation in Art. 7 der Charta und das Recht auf Schutz personenbezogener Daten in Art. 8 der Charta dahin auszulegen sind, dass ein Mitgliedstaat ohne Einwilligung des Betroffenen keine Listen personenbezogener Daten für Zwecke der Steuerverwaltung erstellen darf, so dass die Erlangung der Verfügungsmacht über personenbezogene Daten durch eine Behörde zwecks Bekämpfung von Steuerbetrug als solche eine Gefahr darstellt.

Der Gerichtshof hat entschieden, dass Art. 7 Buchst. e der Richtlinie 95/46/EG einer Verarbeitung personenbezogener Daten durch die Behörden eines Mitgliedstaats für Steuererhebungszwecke und zur Bekämpfung von Steuerbetrug, wie sie im Ausgangsverfahren mit der Erstellung der streitigen Liste ohne die Einwilligung der betroffenen Personen vorgenommen wird, nicht entgegensteht, sofern zum einen den betreffenden Behörden durch das nationale Recht im öffentlichen Interesse liegende Aufgaben im Sinne dieser Vorschrift übertragen wurden, die Erstellung dieser Liste und die Aufnahme der Namen der betroffenen Personen in diese zur Verwirklichung der verfolgten Ziele tatsächlich geeignet und erforderlich sind und hinreichende Anhaltspunkte dafür bestehen, dass die betroffenen Personen zu Recht auf dieser Liste geführt werden, und zum anderen sämtliche in der Richtlinie 95/46/EG aufgestellten Bedingungen für die Rechtmäßigkeit der betreffenden Verarbeitung personenbezogener Daten erfüllt sind (Rn. 117, Tenor 3).

Insoweit hat der Gerichtshof ausgeführt, dass es dem nationalen Gericht obliegt, zu prüfen, ob die Erstellung der streitigen Liste für die Durchführung der im öffentlichen Interesse liegenden Aufgaben, die im Ausgangsverfahren in Rede stehen, erforderlich ist, wobei u. a. der genaue Zweck, zu dem die streitige Liste erstellt wurde, die Rechtsfolgen für die in ihr aufgeführten Personen und der Umstand, ob diese Liste öffentlich ist, zu berücksichtigen sind. Ferner hat das nationale Gericht im Hinblick auf den Grundsatz der Verhältnismäßigkeit zu prüfen, ob die Erstellung der streitigen Liste und die Aufnahme des Namens der betroffenen Personen in diese geeignet sind, die damit verfolgten Ziele zu verwirklichen, und ob es nicht andere, mildere Mittel zur Erreichung dieser Ziele gibt (Rn. 111, 112, 113).

Der Gerichtshof hat darüber hinaus festgestellt, dass durch die Führung einer Person in der streitigen Liste bestimmte ihrer Rechte beeinträchtigt werden können. Die Aufnahme in diese Liste könnte nämlich dem Ruf der betroffenen Person schaden und ihre Beziehungen zu den Finanzbehörden beeinträchtigen. Sie könnte zudem die in Art. 48 Abs. 1 der Charta verankerte Unschuldsvermutung zugunsten der betroffenen Person sowie die in Art. 16 der Charta festgeschriebene unternehmerische Freiheit derjenigen juristischen Personen beeinträchtigen, die mit den in der streitigen Liste aufgeführten natürlichen Personen in Verbindung gebracht werden. Ein solcher Eingriff kann nur dann angemessen sein, wenn hinreichende Anhaltspunkte für den Verdacht bestehen, dass der Betroffene Führungspositionen bei den mit ihm in Verbindung gebrachten juristischen Personen nur zum Schein wahrnimmt und dadurch die Erhebung von Steuern und die Bekämpfung von Steuerbetrug beeinträchtigt (Rn. 114).

Sollte es Gründe dafür geben, bestimmte in den Art. 6 und 10 bis 12 der Richtlinie 95/46/EG vorgesehene Rechte, etwa das Auskunftsrecht der betroffenen Person, nach Art. 13 der Richtlinie zu beschränken, müsste eine solche Beschränkung zur Wahrung eines in Art. 13 Abs. 1 der Richtlinie genannten Interesses, etwa eines wichtigen wirtschaftlichen oder finanziellen Interesses in Steuerangelegenheiten, notwendig sein und auf Rechtsvorschriften beruhen (Rn. 116).

III. Übermittlung personenbezogener Daten in Drittländer

Urteil vom 6. November 2003 (Plenum), Lindqvist (C-101/01, EU:C:2003:596)[19]

In dieser Rechtssache (vgl. auch Abschnitt II.3. „Begriff ‚Verarbeitung personenbezogener Daten'") wollte das vorlegende Gericht insbesondere wissen, ob Frau Lindqvist eine Übermittlung personenbezogener Daten in ein Drittland im Sinne der Richtlinie vorgenommen hat.

Der Gerichtshof hat entschieden, dass keine „Übermittlung von Daten in ein Drittland" im Sinne von Art. 25 der Richtlinie 95/46/EG vorliegt, wenn eine sich in einem Mitgliedstaat aufhaltende Person in eine Internetseite, die bei ihrem in demselben oder einem anderen Mitgliedstaat ansässigen Host-Service-Provider gespeichert ist, personenbezogene Daten aufnimmt und diese damit jeder Person, die eine Verbindung zum Internet herstellt, einschließlich Personen in Drittländern, zugänglich macht (Rn. 71, Tenor 4).

Denn angesichts des Entwicklungsstands des Internets zur Zeit der Ausarbeitung der Richtlinie 95/46/EG und des Fehlens von Kriterien für die Internetbenutzung in Kapitel IV dieser Richtlinie, zu dem Art. 25 gehört, wonach die Mitgliedstaaten die Übermittlung personenbezogener Daten in Drittländer kontrollieren müssen und diese Übermittlung unzulässig ist, wenn die Drittländer kein angemessenes Schutzniveau gewährleisten, kann nicht angenommen werden, dass der Gemeinschaftsgesetzgeber unter den Begriff „Übermittlung von Daten in ein Drittland" im Vorgriff auch den Vorgang fassen wollte, dass Daten in eine Internetseite aufgenommen werden, auch wenn diese Daten dadurch Personen aus Drittländern zugänglich gemacht werden, die über die technischen Mittel für diesen Zugang verfügen (Rn. 63, 64, 68).

Urteil vom 6. Oktober 2015 (Große Kammer), Schrems (C-362/14, EU:C:2015:650)[20]

Herr Schrems, ein österreichischer Staatsangehöriger und Nutzer des sozialen Netzwerks Facebook, hatte beim Data Protection Commissioner (Datenschutzbeauftragter, Irland) eine Beschwerde eingelegt, weil Facebook Ireland personenbezogene Daten seiner Nutzer in die Vereinigten Staaten übermittle und sie dort auf Servern speichere und verarbeite. Das Recht und die Praxis der Vereinigten Staaten böten keinen hinreichenden Schutz der in dieses Land übermittelten personenbezogenen Daten vor Überwachungstätigkeiten der dortigen Behörden. Der Data Protection Commissioner lehnte es ab, die Beschwerde zu prüfen, weil die Kommission insbesondere in ihrer Entscheidung 2000/520/EG[21] festgestellt habe, dass die Vereinigten Staaten im Rahmen der Safe-Harbor-Regelung[22] hinsichtlich der übermittelten personenbezogenen Daten ein angemessenes Schutzniveau gewährleisteten.

Vor diesem Hintergrund wurde der Gerichtshof vom High Court (Hoher Gerichtshof, Irland) mit einem Vorabentscheidungsersuchen zur Auslegung von Art. 25 Abs. 6 der Richtlinie 95/46/EG, wonach die Kommission feststellen kann, dass ein Drittland hinsichtlich des Schutzes der übermittelten Daten ein angemessenes Schutzniveau gewährleistet, und zur Gültigkeit der von der Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46/EG erlassenen Entscheidung 2000/520/EG befasst.

19 Dieses Urteil wurde im Jahresbericht 2003, S. 67, dargestellt.
20 Dieses Urteil wurde im Jahresbericht 2015, S. 53, dargestellt.
21 Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46 über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (ABl. L 215 vom 25.8.2000, S. 7).
22 Die Safe-Harbour-Regelung enthält eine Reihe von Grundsätzen über den Schutz personenbezogener Daten, denen sich amerikanische Unternehmen freiwillig unterwerfen können.

Der Gerichtshof hat die Entscheidung der Kommission in vollem Umfang für ungültig erklärt und zunächst ausgeführt, dass ihr Erlass die gebührend begründete Feststellung der Kommission erfordert, dass das betreffende Drittland tatsächlich ein Schutzniveau der Grundrechte gewährleistet, das dem in der Rechtsordnung der Union garantierten Niveau der Sache nach gleichwertig ist. Da die Kommission dies in der Entscheidung 2000/520/EG jedoch nicht getan hat, verstößt deren Art. 1 gegen die in Art. 25 Abs. 6 der Richtlinie 95/46/EG im Licht der Charta festgelegten Anforderungen und ist aus diesem Grund ungültig. Denn die Safe-Harbour-Grundsätze gelten nur für selbstzertifizierte amerikanische Organisationen, die aus der Union personenbezogene Daten erhalten, ohne dass von den amerikanischen Behörden die Einhaltung dieser Grundsätze verlangt wird. Die Entscheidung 2000/520/EG ermöglicht es ferner, in die Grundrechte der Personen einzugreifen, deren personenbezogene Daten aus der Union in die Vereinigten Staaten übermittelt werden oder werden könnten, ohne eine Feststellung dazu zu enthalten, ob es in den Vereinigten Staaten staatliche Regeln zur Begrenzung etwaiger Eingriffe in diese Rechte und einen wirksamen gerichtlichen Rechtsschutz gegen solche Eingriffe gibt (Rn. 82, 87-89, 96-98, Tenor 2).

Der Gerichtshof hat auch Art. 3 der Entscheidung 2000/520/EG für ungültig erklärt, da sie den nationalen Datenschutzbehörden die Befugnisse entzieht, die ihnen nach Art. 28 der Richtlinie 95/46/EG für den Fall zustehen, dass eine Person die Vereinbarkeit einer Entscheidung der Kommission, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte von Personen in Frage stellt (Rn. 102-104). Der Gerichtshof hat festgestellt, dass die Ungültigkeit der Art. 1 und 3 der Entscheidung 2000/520/EG die Gültigkeit der gesamten Entscheidung berührt (Rn. 105, 106).

Zur Frage, ob ein solcher Eingriff gerechtfertigt werden kann, hat der Gerichtshof zunächst ausgeführt, dass eine Unionsregelung, die einen Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte enthält, klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen muss, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht (Rn. 91).

Darüber hinaus verlangt der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene vor allem, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken (Rn. 92). Nicht auf das absolut Notwendige beschränkt ist eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen (Rn. 93). Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Grundrechts auf Achtung des Privatlebens. Desgleichen verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz (Rn. 94, 95).

Gutachten 1/15 (PNR-Abkommen EU–Kanada) vom 26. Juli 2017 (Große Kammer) (EU:C:2017:592)

Am 26. Juli 2017 hat sich der Gerichtshof erstmals zur Vereinbarkeit des Entwurfs einer internationalen Übereinkunft mit der Charta der Grundrechte der Europäischen Union, insbesondere ihrer Bestimmungen über die Achtung des Privatlebens und den Schutz personenbezogener Daten, geäußert.

Die Europäische Union und Kanada hatten ein Abkommen über die Übermittlung und die Verarbeitung von Fluggastdatensätzen (im Folgenden: PNR-Daten) ausgehandelt, das 2014 unterzeichnet wurde. Da der Rat der Europäischen Union das Europäische Parlament ersuchte, dem Abkommen zuzustimmen, beschloss das Parlament, den Gerichtshof mit der Frage zu befassen, ob das geplante Abkommen mit dem Unionsrecht vereinbar ist.

Dieses Abkommen ermöglicht die systematische und kontinuierliche Übermittlung der PNR-Daten sämtlicher Fluggäste, die aus der Union nach Kanada reisen, an die kanadischen Behörden zur Verwendung, Speicherung und etwaigen Weitergabe an andere Behörden oder Drittländer mit dem Ziel, Terrorismus und grenzübergreifende schwere Kriminalität zu bekämpfen. Zu diesem Zweck sieht das geplante Abkommen u. a. eine Speicherung der PNR-Daten für die Dauer von fünf Jahren vor und stellt besondere Anforderungen an die Sicherheit und Integrität der PNR-Daten wie eine sofortige Unkenntlichmachung sensibler Daten sowie Rechte auf Zugang zu den Daten, auf ihre Berichtigung und Löschung. Außerdem besteht die Möglichkeit, verwaltungsrechtliche und gerichtliche Rechtsbehelfe einzulegen.

Zu den PNR-Daten, auf die sich das Abkommen bezieht, gehören außer dem Namen des Fluggasts bzw. der Fluggäste u. a. Informationen, die für die Reservierung erforderlich sind, wie die Daten des geplanten Flugs und die Reiseroute, Flugscheininformationen, Gruppen von Personen, die unter derselben Reservierungsnummer registriert sind, die Kontaktangaben des Fluggasts bzw. der Fluggäste, Zahlungs- oder Abrechnungsinformationen, Informationen zum Gepäck und allgemeine Eintragungen über die Fluggäste.

In seinem Gutachten hat der Gerichtshof entschieden, dass das PNR-Abkommen in seiner aktuellen Fassung nicht geschlossen werden kann, weil einige seiner Bestimmungen gegen die von der Union anerkannten Grundrechte verstoßen.

Der Gerichtshof hat erstens festgestellt, dass sowohl die Übermittlung der PNR-Daten von der Union an die zuständige kanadische Behörde als auch die von der Union mit Kanada ausgehandelte Regelung der Bedingungen, unter denen die Daten gespeichert, verwendet und eventuell an andere kanadische Behörden, Europol, Eurojust, gerichtliche oder Polizeibehörden der Mitgliedstaaten oder Behörden weiterer Drittländer weitergegeben werden können, Eingriffe in das durch Art. 7 der Charta garantierte Grundrecht darstellen. Diese Vorgänge stellen, weil es sich bei ihnen um Verarbeitungen personenbezogener Daten handelt, auch einen Eingriff in das durch Art. 8 der Charta garantierte Grundrecht auf Schutz personenbezogener Daten dar (Rn. 125, 126).

Ferner können die PNR-Daten, auch wenn einige von ihnen für sich genommen nicht geeignet sein dürften, bedeutsame Informationen über das Privatleben der betreffenden Personen zu liefern, zusammen betrachtet u. a. einen gesamten Reiseverlauf, Reisegewohnheiten, Beziehungen zwischen zwei oder mehreren Personen sowie Informationen über die finanzielle Situation der Fluggäste, ihre Ernährungsgewohnheiten oder ihren Gesundheitszustand offenbaren und sogar sensible Daten über die Fluggäste im Sinne von Art. 2 Buchst. e des geplanten Abkommens liefern (Informationen, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse Überzeugungen usw. hervorgehen) (Rn. 128).

Obwohl die fraglichen Eingriffe durch die Verfolgung eines dem Gemeinwohl dienenden Ziels (Gewährleistung der öffentlichen Sicherheit im Rahmen der Bekämpfung terroristischer Straftaten und grenzübergreifender schwerer Kriminalität) gerechtfertigt sein können, beschränken sich mehrere Bestimmungen des Abkommens nicht auf das absolut Notwendige und enthalten keine klaren und präzisen Regeln.

Der Gerichtshof hat insbesondere ausgeführt, dass in Anbetracht des Risikos einer gegen das Diskriminierungsverbot verstoßenden Verarbeitung von Daten die Übermittlung sensibler Daten an Kanada einer präzisen und besonders fundierten, auf andere Gründe als den Schutz der öffentlichen Sicherheit vor Terrorismus und grenzübergreifender schwerer Kriminalität gestützten Rechtfertigung bedürfte. An einer solchen Rechtfertigung fehlt es hier jedoch. Der Gerichtshof hat daraus geschlossen, dass die Bestimmungen des Abkommens über die Übermittlung sensibler Daten nach Kanada sowie die Verarbeitung und die Speicherung dieser Daten nicht mit den Grundrechten vereinbar sind (Rn. 165, 232).

Zweitens hat der Gerichtshof die Auffassung vertreten, dass eine dauerhafte Speicherung der PNR-Daten sämtlicher Fluggäste nach ihrer Ausreise aus Kanada, die das geplante Abkommen zulässt, nicht auf das absolut Notwendige beschränkt ist. Denn bei Fluggästen, bei denen eine Gefahr im Bereich des Terrorismus oder grenzübergreifender schwerer Kriminalität weder bei ihrer Ankunft in Kanada noch bis zu ihrer Ausreise aus diesem Land festgestellt wurde, dürfte kein Zusammenhang, sei er auch mittelbarer Art, zwischen ihren PNR-Daten und dem mit dem geplanten Abkommen verfolgten Ziel bestehen, der die Speicherung der Daten rechtfertigen würde. Dagegen ist eine Speicherung der PNR-Daten von Fluggästen, bei denen objektive Anhaltspunkte dafür bestehen, dass von ihnen auch nach ihrer Ausreise aus Kanada eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität ausgehen könnte, über ihren Aufenthalt in Kanada hinaus, auch für eine Dauer von fünf Jahren, zulässig (Rn. 205-207, 209).

Drittens hat der Gerichtshof festgestellt, dass das in Art. 7 der Charta verbürgte Grundrecht auf Achtung des Privatlebens voraussetzt, dass sich die betroffene Person vergewissern kann, dass ihre personenbezogenen Daten fehlerfrei verarbeitet werden und die Verarbeitung zulässig ist. Um die nötigen Nachprüfungen durchführen zu können, muss sie ein Auskunftsrecht hinsichtlich der sie betreffenden Daten haben, die Gegenstand einer Verarbeitung sind.

Im Abkommen muss somit vorgesehen sein, dass die Fluggäste von der Weitergabe ihrer PNR-Daten an Kanada und der Verwendung dieser Daten in Kenntnis gesetzt werden, sobald dies die Ermittlungen der in diesem Abkommen genannten Behörden nicht mehr beeinträchtigen kann. Diese Mitteilung ist nämlich der Sache nach erforderlich, damit die Fluggäste ihr Recht auf Auskunft über die sie betreffenden PNR-Daten und gegebenenfalls auf Berichtigung der Daten sowie ihr Recht, gemäß Art. 47 Abs. 1 der Charta bei einem Gericht einen wirksamen Rechtsbehelf einzulegen, ausüben können.

In Fällen, in denen objektive Anhaltspunkte vorliegen, die eine solche Verwendung rechtfertigen und eine vorherige Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsstelle erforderlich machen, ist daher eine individuelle Information der Fluggäste erforderlich. Dasselbe gilt für Fälle, in denen die PNR-Daten an andere Behörden oder an Einzelpersonen weitergegeben werden. Eine solche Mitteilung darf aber erst erfolgen, wenn sie die Ermittlungen der im geplanten Abkommen genannten Behörden nicht mehr beeinträchtigen kann (Rn. 219, 220, 223, 224).

IV. Der Schutz personenbezogener Daten im Internet

1. Recht, der Verarbeitung personenbezogener Daten zu widersprechen („Recht auf Vergessenwerden“)

Urteil vom 13. Mai 2014 (Große Kammer), Google Spain und Google (C-131/12, EU:C:2014:317)

In diesem Urteil (vgl. auch Abschnitt II.3. „Begriff ‚Verarbeitung personenbezogener Daten‘“) hat der Gerichtshof die Tragweite der in der Richtlinie 95/46/EG vorgesehenen Rechte auf Zugang zu personenbezogenen Daten im Internet und Widerspruch gegen deren Verarbeitung erläutert.

So hat der Gerichtshof zur Frage, wie weit die Verantwortlichkeit des Betreibers einer Internetsuchmaschine reicht, im Wesentlichen festgestellt, dass der Suchmaschinenbetreiber zur Wahrung der in Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46/EG vorgesehenen Rechte, sofern deren Voraussetzungen erfüllt sind, unter bestimmten Bedingungen dazu verpflichtet ist, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links zu von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person zu entfernen. Diese Pflicht kann auch bestehen, wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden, und gegebenenfalls auch dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist (Rn. 88, Tenor 3).

Der Gerichtshof hat ferner zur Frage, ob die betroffene Person nach der Richtlinie verlangen kann, dass Links zu Internetseiten von einer solchen Ergebnisliste entfernt werden, weil sie möchte, dass die dort zu findenden Informationen über sie nach einer bestimmten Zeit „vergessen“ werden, zunächst ausgeführt, dass auch eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten im Laufe der Zeit nicht mehr den Bestimmungen der Richtlinie entsprechen kann, wenn die Daten für die Zwecke, für die sie erhoben oder verarbeitet worden sind, nicht mehr erforderlich sind. Das ist insbesondere der Fall, wenn sie diesen Zwecken in Anbetracht der verstrichenen Zeit nicht entsprechen, dafür nicht oder nicht mehr erheblich sind oder darüber hinausgehen (Rn. 93). Wird somit auf einen Antrag der betroffenen Person festgestellt, dass die Einbeziehung dieser Links in die Ergebnisliste zum gegenwärtigen Zeitpunkt nicht mit der Richtlinie vereinbar ist, müssen die betreffenden Informationen und Links der Ergebnisliste gelöscht werden (Rn. 94). Die Feststellung eines Rechts der betroffenen Person, dass die Information über sie nicht mehr durch eine Ergebnisliste mit ihrem Namen in Verbindung gebracht wird, setzt nicht voraus, dass der betroffenen Person durch die Einbeziehung der betreffenden Information in die Ergebnisliste ein Schaden entsteht (Rn. 96, Tenor 4).

Schließlich hat der Gerichtshof erläutert, dass, da die betroffene Person in Anbetracht ihrer Grundrechte aus den Art. 7 und 8 der Charta verlangen kann, dass die betreffende Information der breiten Öffentlichkeit nicht mehr durch Einbeziehung in eine derartige Ergebnisliste zur Verfügung gestellt wird, diese Rechte grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit daran, die Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche zu finden, überwiegen. Dies wäre jedoch nicht der Fall, wenn sich aus besonderen Gründen – wie der Rolle der Person im öffentlichen Leben – ergeben sollte, dass der Eingriff in ihre Grundrechte durch das überwiegende Interesse der breiten Öffentlichkeit daran, über die Einbeziehung in eine derartige Ergebnisliste Zugang zu der betreffenden Information zu haben, gerechtfertigt ist (Rn. 97, Tenor 4).

2. Verarbeitung personenbezogener Daten und Rechte des geistigen Eigentums

Urteil vom 29. Januar 2008 (Große Kammer), Promusicae (C-275/06, EU:C:2008:54)[23]

Promusicae, eine spanische Vereinigung ohne Gewinnerzielungsabsicht, der Produzenten und Herausgeber von Musikaufnahmen und audiovisuellen Aufnahmen angehören, hatte sich an die spanischen Gerichte gewandt, um der Telefónica de España SAU (Handelsgesellschaft, die u. a. Internetzugänge bereitstellt) aufzugeben, Name und Anschrift bestimmter Personen offenzulegen, denen Telefónica einen Internetzugang gewährt hatte und deren IP-Adresse sowie Tag und Zeit der Verbindung bekannt waren. Nach Ansicht von Promusicae verwendeten diese Personen ein „peer-to-peer" oder „P2P"-Programm zum Austausch von Dateien (ein offenes, unabhängiges, dezentralisiertes und mit hochentwickelten Such- und Downloadfunktionen ausgestattetes Hilfsmittel zum Austausch von Inhalten) und ließen den Zugriff auf Musikdateien zu, die sich im gemeinsam genutzten Ordner ihres Computers befänden und für die die Urheber- und Lizenzrechte bei Promusicae lägen. Sie verlangte daher die Weitergabe dieser Informationen, um zivilrechtliche Klagen gegen die Betroffenen erheben zu können.

Unter diesen Umständen wollte der Juzgado de lo Mercantil no 5 de Madrid (Handelsgericht Nr. 5 Madrid, Spanien) vom Gerichtshof wissen, ob das europäische Recht den Mitgliedstaaten gebietet, im Hinblick auf den wirksamen Schutz des Urheberrechts die Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorsehen zu müssen.

Der Gerichtshof hat darauf hingewiesen, dass das Vorabentscheidungsersuchen die Frage aufwirft, wie die Erfordernisse des Schutzes verschiedener Grundrechte, nämlich zum einen des Rechts auf Achtung des Privatlebens und zum anderen des Eigentumsrechts und des Rechts auf einen wirksamen Rechtsbehelf, miteinander in Einklang gebracht werden können.

Der Gerichtshof hat hierzu ausgeführt, dass die Richtlinien 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr")[24], 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft[25], 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums[26] und 2002/58/EG es den Mitgliedstaaten nicht gebieten, in einer Situation wie der des Ausgangsverfahrens im Hinblick auf einen effektiven Schutz des Urheberrechts die Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen. Die Mitgliedstaaten sind gemäß dem Unionsrecht jedoch dazu verpflichtet, sich bei der Umsetzung dieser Richtlinien auf eine Auslegung derselben zu stützen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Unionsrechtsordnung geschützten Grundrechten sicherzustellen. Bei der Durchführung der Maßnahmen zur Umsetzung dieser Richtlinien haben die Behörden und Gerichte der Mitgliedstaaten nicht nur ihr nationales Recht im Einklang mit diesen Richtlinien auszulegen, sondern auch darauf zu achten, dass sie sich nicht auf eine Auslegung dieser Richtlinien stützen, die mit diesen Grundrechten oder den anderen allgemeinen Grundsätzen des Unionsrechts, wie etwa dem Grundsatz der Verhältnismäßigkeit, kollidiert (Rn. 70 und Tenor).

---

23 Dieses Urteil wurde im Jahresbericht 2008, S. 46, dargestellt.

24 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr") (ABl. L 178 vom 17.7.2000, S. 1).

25 Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (ABl. L 167 vom 22.6.2001, S. 10).

26 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums (ABl. L 157 vom 30.4.2004, S. 45, und – Berichtigung – ABl. L 195 vom 2.6.2004, S. 16).

Urteil vom 24. November 2011, Scarlet Extended (C-70/10, EU:C:2011:771)[27]

Die Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (Belgische Gesellschaft der Autoren, Komponisten und Verleger) hatte festgestellt, dass Internetnutzer die Dienste der Scarlet Extended SA, eines Anbieters von Internetzugangsdiensten (im Folgenden: Scarlet), in Anspruch nehmen, um über das Internet – ohne Genehmigung und ohne Gebühren zu entrichten – über „Peer-to-Peer"-Netze Werke aus ihrem Repertoire herunterzuladen. SABAM wandte sich an ein nationales Gericht und erwirkte im ersten Rechtszug eine Anordnung gegen Scarlet, diese Verletzungen des Urheberrechts abzustellen, indem sie es ihren Kunden unmöglich mache, Dateien, die ein Werk der Musik aus dem Repertoire von SABAM enthielten, in irgendeiner Form ein Werk mit Hilfe eines „Peer-to-Peer"-Programms zu senden oder zu empfangen.

Von Scarlet befasst, wandte sich die Cour d'appel de Bruxelles (Berufungsgericht Brüssel, Belgien) mit einem Vorabentscheidungsersuchen an den Gerichtshof, um zu klären, ob eine solche Anordnung mit dem europäischen Recht vereinbar ist.

Der Gerichtshof hat entschieden, dass die Richtlinien 95/46/EG, 2000/31/EG, 2001/29/EG, 2002/58/EG und 2004/48/EG in Verbindung miteinander und ausgelegt anhand der sich aus dem Schutz der anwendbaren Grundrechte ergebenden Anforderungen dahin auszulegen sind, dass sie der Anordnung an Scarlet entgegenstehen, ein System der Filterung aller ihrer Dienste durchlaufenden elektronischen Kommunikationen insbesondere durch die Verwendung von „Peer-to-Peer"-Programmen, das unterschiedslos auf alle seine Kunden anwendbar ist, präventiv, allein auf eigene Kosten und zeitlich unbegrenzt einzurichten, mit dem sich im Netz dieses Anbieters der Austausch von Dateien ermitteln lässt, die ein musikalisches, filmisches oder audiovisuelles Werk enthalten, an dem der Antragsteller Rechte des geistigen Eigentums zu haben behauptet, um die Übertragung von Dateien, deren Austausch gegen das Urheberrecht verstößt, zu blockieren (Rn. 54 und Tenor).

Eine solche Anordnung entspricht nämlich weder dem in Art. 15 Abs. 1 der Richtlinie 2000/31/EG festgelegten Verbot, einem solchen Provider allgemeine Überwachungspflichten aufzuerlegen, noch dem Erfordernis, ein angemessenes Gleichgewicht zwischen dem Schutz des Rechts des geistigen Eigentums einerseits und der unternehmerischen Freiheit, dem Recht auf den Schutz personenbezogener Daten und dem Recht auf freien Empfang oder freie Sendung von Informationen andererseits zu gewährleisten (Rn. 40, 49).

In diesem Zusammenhang hat der Gerichtshof zum einen ausgeführt, dass die Anordnung, das streitige Filtersystem einzurichten, eine systematische Prüfung aller Inhalte sowie die Sammlung und Identifizierung der IP-Adressen der Nutzer bedeuten würde, die die Sendung unzulässiger Inhalte in diesem Netz veranlasst haben, wobei es sich bei diesen Adressen um geschützte personenbezogene Daten handelt, da sie die genaue Identifizierung der Nutzer ermöglichen (Rn. 51). Zum anderen könnte die Anordnung die Informationsfreiheit beeinträchtigen, weil die Gefahr bestünde, dass das System nicht hinreichend zwischen einem unzulässigen und einem zulässigen Inhalt unterscheiden kann, so dass sein Einsatz zur Sperrung von Kommunikationen mit zulässigem Inhalt führen könnte. Denn es ist unbestritten, dass die Antwort auf die Frage der Zulässigkeit einer Übertragung auch von der Anwendung gesetzlicher Ausnahmen vom Urheberrecht abhängt, die von Mitgliedstaat zu Mitgliedstaat variieren. Ferner können bestimmte Werke in bestimmten Mitgliedstaaten gemeinfrei sein, oder sie können von den fraglichen Urhebern kostenlos ins Internet gestellt worden sein (Rn. 52).

27 Dieses Urteil wurde im Jahresbericht 2011, S. 37, dargestellt.

Der Gerichtshof hat daher festgestellt, dass das fragliche nationale Gericht, erließe es die Anordnung, mit der der Provider zur Einrichtung des streitigen Filtersystems verpflichtet würde, nicht das Erfordernis beachten würde, ein angemessenes Gleichgewicht zwischen dem Recht des geistigen Eigentums einerseits und der unternehmerischen Freiheit, dem Recht auf den Schutz personenbezogener Daten und dem Recht auf freien Empfang oder freie Sendung von Informationen andererseits zu gewährleisten (Rn. 53).

Urteil vom 19. April 2012, Bonnier Audio u. a. (C-461/10, EU:C:2012:219)

Der Högsta domstol (Oberster Gerichtshof, Schweden) ersuchte den Gerichtshof im Rahmen eines Rechtsstreits zwischen der Bonnier Audio AB, der Earbooks AB, der Norstedts Förlagsgrupp AB, der Piratförlaget AB und der Storyside AB (im Folgenden: Bonnier Audio u. a.) einerseits und der Perfect Communication Sweden AB (im Folgenden: ePhone) andererseits, in dem sich ePhone gegen einen Antrag von Bonnier Audio u. a. auf Anordnung der Weitergabe von Daten wandte, im Wege der Vorabentscheidung um Auslegung der Richtlinien 2002/58/EG und 2004/48/EG.

Bonnier Audio u. a. sind Verlage, die insbesondere das ausschließliche Recht besitzen, 27 Bücher in Hörbuchform herauszugeben, die Werke zu vervielfältigen und sie der Allgemeinheit zugänglich zu machen. Sie waren der Ansicht, dass dadurch in ihre Ausschließlichkeitsrechte eingegriffen worden sei, dass diese 27 Werke ohne ihre Zustimmung über einen FTP(„File transfer protocol")-Server – ein Datei-Sharing-Programm, das die Übertragung von Dateien zwischen Computern über das Internet ermöglicht – der Allgemeinheit zugänglich gemacht worden seien. Sie wandten sich daher an die schwedischen Gerichte und beantragten eine Auskunftsverfügung in Bezug auf Name und Adresse derjenigen Person, die die IP-Adresse nutzte, von der vermutet wurde, dass von ihr aus die in Rede stehenden Daten übertragen wurden.

Der mit einem Rechtsmittel befasste Högsta domstol wollte vom Gerichtshof wissen, ob das Unionsrecht der Anwendung einer Vorschrift des nationalen Rechts entgegensteht, die auf der Grundlage von Art. 8 der Richtlinie 2004/48/EG erlassen wurde und nach der in einem zivilrechtlichen Verfahren einem Internetdienstleister zu dem Zweck, einen bestimmten Teilnehmer identifizieren zu können, aufgegeben werden kann, einem Urheberrechtsinhaber oder dessen Vertreter Auskunft über den Teilnehmer zu geben, dem der Internetdienstleister eine bestimmte IP-Adresse zugeteilt hat, von der aus dieses Recht verletzt worden sein soll. Dabei war davon auszugehen, dass der Antragsteller deutliche Anhaltspunkte für eine Urheberrechtsverletzung geliefert hatte und dass die Maßnahme verhältnismäßig war.

Der Gerichtshof hat zunächst darauf hingewiesen, dass Art. 8 Abs. 3 der Richtlinie 2004/48/EG in Verbindung mit Art. 15 Abs. 1 der Richtlinie 2002/58/EG die Mitgliedstaaten nicht daran hindert, eine Verpflichtung zur Weitergabe personenbezogener Daten an Privatpersonen zu schaffen, um die Verfolgung von Urheberrechtsverstößen vor den Zivilgerichten zu ermöglichen, sie aber auch nicht daran hindert, eine derartige Verpflichtung vorzusehen. Die Behörden und Gerichte der Mitgliedstaaten haben jedoch bei der Durchführung der Maßnahmen zur Umsetzung dieser Richtlinien nicht nur ihr nationales Recht im Einklang mit ihnen auszulegen, sondern auch darauf zu achten, dass sie sich nicht auf eine Auslegung der Richtlinien stützen, die mit den durch die Unionsrechtsordnung geschützten Grundrechten oder anderen allgemeinen Grundsätzen des Unionsrechts, wie etwa dem Grundsatz der Verhältnismäßigkeit, kollidiert (Rn. 55, 56).

Nach den fraglichen nationalen Rechtsvorschriften mussten, damit eine Weitergabe der betreffenden Daten angeordnet werden konnte, insbesondere deutliche Anhaltspunkte für die Verletzung des Urheberrechts an einem Werk vorliegen, die begehrten Auskünfte mussten geeignet sein, die Untersuchung der Urheberrechtsverletzung oder -beeinträchtigung zu erleichtern, und die Gründe für die Anordnung mussten die Unannehmlichkeiten oder anderen Nachteile aufwiegen, die die Maßnahme für

denjenigen, gegen den sie sich richtet, oder für andere entgegenstehende Interessen mit sich bringt (Rn. 58).

Der Gerichtshof hat daher festgestellt, dass die Richtlinien 2002/58/EG und 2004/48/EG nationalen Rechtsvorschriften wie den im Ausgangsverfahren fraglichen nicht entgegenstehen, soweit diese es dem nationalen Gericht, bei dem eine klagebefugte Person beantragt hat, die Weitergabe personenbezogener Daten anzuordnen, ermöglichen, anhand der Umstände des Einzelfalls und unter gebührender Berücksichtigung der sich aus dem Grundsatz der Verhältnismäßigkeit ergebenden Erfordernisse eine Abwägung der einander gegenüberstehenden Interessen vorzunehmen (Rn. 61 und Tenor).

V. Nationale Kontrollstellen

1. Tragweite des Unabhängigkeitserfordernisses

Urteil vom 9. März 2010 (Große Kammer), Kommission/Deutschland (C-518/07, EU:C:2010:125)[28]

Mit ihrer Klage hatte die Kommission beantragt, festzustellen, dass die Bundesrepublik Deutschland gegen ihre Verpflichtungen aus Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG verstoßen hat, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten im nicht öffentlichen Bereich zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterworfen und damit das Erfordernis der „völligen Unabhängigkeit" der mit dem Schutz dieser Daten beauftragten Stellen falsch umgesetzt hat.

Die Bundesrepublik Deutschland war dagegen der Auffassung, dass Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG eine funktionale Unabhängigkeit der Kontrollstellen in dem Sinne verlange, dass sie von dem ihrer Kontrolle unterstellten nicht öffentlichen Bereich unabhängig sein müssten und keinen sachfremden Einflüssen unterliegen dürften. Die staatliche Aufsicht in den Bundesländern stelle keinen sachfremden Einfluss dar, sondern einen verwaltungsinternen Mechanismus der Kontrolle durch Stellen innerhalb desselben Verwaltungsapparats, die in derselben Weise wie die Kontrollstellen den Zielvorgaben der Richtlinie 95/46/EG verpflichtet seien.

Der Gerichtshof hat entschieden, dass die mit dieser Richtlinie gewährleistete Unabhängigkeit der nationalen Kontrollstellen die wirksame und zuverlässige Kontrolle der Einhaltung der Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sicherstellen soll und im Licht dieses Zwecks auszulegen ist. Sie wurde eingeführt, um die von ihren Entscheidungen betroffenen Personen und Einrichtungen stärker zu schützen, und nicht, um diesen Kontrollstellen selbst oder ihren Bevollmächtigten eine besondere Stellung zu verleihen. Folglich müssen die Kontrollstellen bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorgehen (Rn. 25).

Der Gerichtshof hat festgestellt, dass die für die Überwachung der Verarbeitung personenbezogener Daten im nicht öffentlichen Bereich zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch

28 Dieses Urteil wurde im Jahresbericht 2010, S. 34, dargestellt.

die in Frage gestellt werden könnte, dass die Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen. Die bloße Gefahr einer politischen Einflussnahme der Aufsichtsbehörden auf die Entscheidungen der Kontrollstellen reicht aus, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen. Zum einen könnte es einen „vorauseilenden Gehorsam" der Kontrollstellen im Hinblick auf die Entscheidungspraxis der Aufsichtsstellen geben. Zum anderen erfordert die Rolle der Kontrollstellen als Hüter des Rechts auf Privatsphäre, dass ihre Entscheidungen, und damit sie selbst, über jeden Verdacht der Parteilichkeit erhaben sind. Die staatliche Aufsicht, der die nationalen Kontrollstellen unterworfen sind, ist daher nicht mit dem Unabhängigkeitserfordernis vereinbar (Rn. 30, 36, 37 und Tenor).

Urteil vom 16. Oktober 2012 (Große Kammer), Kommission/Österreich (C-614/10, EU:C:2012:631)

Mit ihrer Klage hatte die Kommission beantragt, festzustellen, dass die Republik Österreich dadurch gegen ihre Verpflichtungen aus Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG verstoßen hat, dass sie nicht alle Vorschriften erlassen hat, die erforderlich sind, damit die in Österreich bestehende Rechtslage in Bezug auf die als Kontrollstelle für den Schutz personenbezogener Daten eingerichtete Datenschutzkommission dem Kriterium der Unabhängigkeit genügt.

Der Gerichtshof hat eine Vertragsverletzung Österreichs festgestellt, weil ein Mitgliedstaat, der eine Regelung einführt, nach der das geschäftsführende Mitglied der nationalen Kontrollstelle ein der Dienstaufsicht unterliegender Bediensteter des Staates ist, die Geschäftsstelle der Behörde in die nationale Regierung eingegliedert ist und Regierungschef über ein unbedingtes Recht verfügt, sich über alle Gegenstände der Geschäftsführung der Behörde zu unterrichten, nicht das Erfordernis der Unabhängigkeit der Kontrollstelle erfüllt (Rn. 66 und Tenor).

Der Gerichtshof hat zunächst darauf hingewiesen, dass der Ausdruck „in völliger Unabhängigkeit" in Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG bedeutet, dass die für den Schutz personenbezogener Daten zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Dass die Stelle insoweit über funktionelle Unabhängigkeit verfügt, als ihre Mitglieder in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden sind, reicht für sich allein nicht aus, um sie vor jeder äußeren Einflussnahme zu bewahren. Die in diesem Rahmen erforderliche Unabhängigkeit soll jedoch nicht nur die unmittelbare Einflussnahme in Form von Weisungen ausschließen, sondern auch jede Form der mittelbaren Einflussnahme, die zur Steuerung der Entscheidungen der Kontrollstelle geeignet wäre. In Anbetracht der Rolle der Kontrollstellen als Hüter des Rechts auf Privatsphäre müssen ihre Entscheidungen, und damit sie selbst, über jeden Verdacht der Parteilichkeit erhaben sein (Rn. 41-43, 52).

Der Gerichtshof hat erläutert, dass eine nationale Kontrollstelle nicht über eine eigene Haushaltslinie, wie sie Art. 43 Abs. 3 der Verordnung (EG) Nr. 45/2001 vorsieht, verfügen muss, um das Unabhängigkeitskriterium des Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG erfüllen zu können. Die Mitgliedstaaten sind nämlich nicht verpflichtet, in ihr innerstaatliches Recht ähnliche Vorschriften wie die des Kapitels V der Verordnung (EG) Nr. 45/2001 aufzunehmen, um für ihre Kontrollstelle(n) völlige Unabhängigkeit zu gewährleisten, und können somit die Kontrollstelle haushaltsrechtlich einem bestimmten Ressort zuordnen. Allerdings darf die Zuweisung der von einer solchen Stelle benötigten personellen und sachlichen Mittel diese Stelle nicht daran hindern, ihre Aufgaben „in völliger Unabhängigkeit" im Sinne von Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG wahrzunehmen (Rn. 58).

Urteil vom 8. April 2014 (Große Kammer), Kommission/Ungarn (C-288/12, EU:C:2014:237)[29]

In dieser Rechtssache hatte die Kommission beantragt, festzustellen, dass Ungarn dadurch gegen seine Verpflichtungen aus der Richtlinie 95/46/EG verstoßen hat, dass es das Mandat der Kontrollstelle für den Schutz personenbezogener Daten vorzeitig beendet hat.

Der Gerichtshof hat entschieden, dass ein Mitgliedstaat, der das Mandat der Kontrollstelle für den Schutz personenbezogener Daten vorzeitig beendet, gegen seine Verpflichtungen aus der Richtlinie 95/46/EG verstößt (Rn. 62, Tenor 1).

Nach Auffassung des Gerichtshofs schließt die Unabhängigkeit, über die die für die Überwachung der Verarbeitung dieser Daten zuständigen Kontrollstellen ausgestattet sein müssen, nämlich u. a. jede Anordnung und jede sonstige wie auch immer geartete äußere Einflussnahme aus, sei sie unmittelbar oder mittelbar, an denen ihre Entscheidungen ausgerichtet werden könnten und durch die in Frage gestellt werden könnte, dass die Kontrollstellen ihre Aufgabe erfüllen, zwischen dem Schutz des Rechts auf Privatsphäre und dem freien Verkehr personenbezogener Daten ein ausgewogenes Verhältnis herzustellen (Rn. 51).

Der Gerichtshof hat ferner darauf hingewiesen, dass eine solche funktionelle Unabhängigkeit für sich allein nicht ausreicht, um die Kontrollstellen vor jeder äußeren Einflussnahme zu bewahren, und dass daher schon die bloße Gefahr einer politischen Einflussnahme auf die Entscheidungen der Kontrollstellen ausreicht, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen. Dürfte aber ein Mitgliedstaat das Mandat einer Kontrollstelle vor seinem ursprünglich vorgesehenen Ablauf beenden, ohne die von den anwendbaren Rechtsvorschriften zu diesem Zweck im Voraus festgelegten Grundsätze und Garantien zu beachten, könnte die Drohung einer solchen vorzeitigen Beendigung, die dann während der gesamten Ausübung des Mandats über dieser Stelle schwebte, zu einer Form des Gehorsams dieser Stelle gegenüber den politisch Verantwortlichen führen, die mit dem Unabhängigkeitsgebot nicht vereinbar wäre. Zudem könnte in einer solchen Situation nicht davon ausgegangen werden, dass die Kontrollstelle bei ihrer Tätigkeit in jedem Fall über jeden Verdacht der Parteilichkeit erhaben ist (Rn. 52-55).

2. Bestimmung des anwendbaren Rechts und der zuständigen Kontrollstelle

Urteil vom 1. Oktober 2015, Weltimmo (C-230/14, EU:C:2015:639)[30]

Die Nemzeti Adatvédelmi és Információszabadság Hatóság (Nationale Behörde für Datenschutz und Informationsfreiheit, Ungarn) hatte gegen die in der Slowakei eingetragene Gesellschaft Weltimmo, die eine Website zur Vermittlung von in Ungarn gelegenen Immobilien betreibt, ein Bußgeld verhängt, weil sie trotz entsprechender Anträge von Inserenten personenbezogene Daten nicht gelöscht, sondern an Inkassounternehmen übermittelt hatte, um Außenstände einzutreiben. Nach Auffassung der ungarischen Kontrollstelle hatte Weltimmo damit gegen das ungarische Gesetz zur Umsetzung der Richtlinie 95/46/EG verstoßen.

Die mit einem Rechtsmittel befasste Kúria (Oberster Gerichtshof, Ungarn) hatte Zweifel hinsichtlich der Bestimmung des anwendbaren Rechts und der Befugnisse der ungarischen Kontrollstelle nach Art. 4 Abs. 1 und Art. 28 der Richtlinie 95/46/EG. Sie richtete daher mehrere Vorabentscheidungsfragen an den Gerichtshof.

29 Dieses Urteil wurde im Jahresbericht 2014, S. 62, dargestellt.
30 Dieses Urteil wurde im Jahresbericht 2015, S. 55, dargestellt.

Zum anwendbaren nationalen Recht hat der Gerichtshof festgestellt, dass Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46/EG die Anwendung des Datenschutzrechts eines anderen Mitgliedstaats als dem, in dem der für die Datenverarbeitung Verantwortliche eingetragen ist, erlaubt, soweit dieser mittels einer festen Einrichtung im Hoheitsgebiet dieses Mitgliedstaats eine effektive und tatsächliche Tätigkeit ausübt, in deren Rahmen diese Verarbeitung ausgeführt wird, selbst wenn die Tätigkeit nur geringfügig ist. Um zu bestimmen, ob dies der Fall ist, kann das vorlegende Gericht insbesondere zum einen berücksichtigen, dass die Tätigkeit des für diese Verarbeitung Verantwortlichen, in deren Rahmen diese stattfindet, im Betreiben von Websites besteht, die der Vermittlung von Immobilien dienen, die sich im Hoheitsgebiet dieses Mitgliedstaats befinden, und die in dessen Sprache verfasst sind, und dass sie daher hauptsächlich oder sogar vollständig auf diesen Mitgliedstaat ausgerichtet ist. Zum anderen kann es berücksichtigen, dass dieser Verantwortliche über einen Vertreter in diesem Mitgliedstaat verfügt, der dafür zuständig ist, die Forderungen aus dieser Tätigkeit einzuziehen sowie den Verantwortlichen im Verwaltungsverfahren und im gerichtlichen Verfahren über die Verarbeitung der betreffenden Daten zu vertreten. Die Frage der Staatsangehörigkeit der von dieser Datenverarbeitung betroffenen Personen ist dagegen irrelevant (Rn. 41, Tenor 1).

Zur Zuständigkeit und zu den Befugnissen der mit Beschwerden befassten Kontrollstelle nach Art. 28 Abs. 4 der Richtlinie 95/46/EG hat der Gerichtshof ausgeführt, dass diese Behörde die Beschwerden unabhängig vom anwendbaren Recht und noch bevor sie weiß, welches nationale Recht auf die fragliche Verarbeitung anzuwenden ist, prüfen kann (Rn. 54). Wenn sie jedoch zu dem Schluss gelangen sollte, dass das Recht eines anderen Mitgliedstaats anwendbar ist, darf sie keine Sanktionen außerhalb des Hoheitsgebiets ihres Mitgliedstaats verhängen. In einer solchen Situation obliegt es ihr in Wahrnehmung der Verpflichtung zur Zusammenarbeit, die Art. 28 Abs. 6 dieser Richtlinie vorsieht, die Kontrollstelle dieses anderen Mitgliedstaats zu ersuchen, einen möglichen Verstoß gegen dieses Recht festzustellen und Sanktionen zu verhängen, wenn das nach diesem Recht zulässig ist, und sich dabei gegebenenfalls auf die ihr übermittelten Informationen zu stützen (Rn. 57, 60, Tenor 2).

3. Befugnisse der nationalen Kontrollstellen

Urteil vom 6. Oktober 2015 (Große Kammer), Schrems (C-362/14, EU:C:2015:650)

In dieser Rechtssache (vgl. auch Abschnitt III „Übermittlung personenbezogener Daten in Drittländer“) hat der Gerichtshof u. a. entschieden, dass die nationalen Kontrollstellen für die Kontrolle der Übermittlungen personenbezogener Daten in Drittländer zuständig sind.

Insoweit hat der Gerichtshof zunächst festgestellt, dass die nationalen Kontrollstellen über eine große Bandbreite von Befugnissen verfügen, die in Art. 28 Abs. 3 der Richtlinie 95/46/EG in nicht abschließender Weise aufgezählt sind und notwendige Mittel für die Erfüllung ihrer Aufgaben darstellen. So verfügen sie u. a. über Untersuchungsbefugnisse wie etwa das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen, über wirksame Einwirkungsbefugnisse wie etwa die Befugnis, das vorläufige oder endgültige Verbot einer Verarbeitung von Daten anzuordnen, oder über das Klagerecht (Rn. 43).

Zur Befugnis, die Übermittlung personenbezogener Daten in Drittländer zu kontrollieren, hat der Gerichtshof ausgeführt, dass aus Art. 28 Abs. 1 und 6 der Richtlinie 95/46/EG hervorgeht, dass die Befugnisse der nationalen Kontrollstellen die Verarbeitung personenbezogener Daten im Hoheitsgebiet ihres Mitgliedstaats betreffen, so dass Art. 28 ihnen keine Befugnisse in Bezug auf die Verarbeitung solcher Daten im Hoheitsgebiet eines Drittlands verleiht (Rn. 44).

Die Übermittlung personenbezogener Daten aus einem Mitgliedstaat in ein Drittland stellt jedoch als solche eine Verarbeitung personenbezogener Daten im Hoheitsgebiet eines Mitgliedstaats dar. Da die

nationalen Kontrollstellen gemäß Art. 8 Abs. 3 der Charta und Art. 28 der Richtlinie 95/46/EG die Einhaltung der Unionsvorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu überwachen haben, ist jede von ihnen zu der Prüfung befugt, ob bei einer Übermittlung personenbezogener Daten aus ihrem Mitgliedstaat in ein Drittland die in der Richtlinie aufgestellten Anforderungen eingehalten werden (Rn. 45, 47).

VI. Räumlicher Anwendungsbereich der europäischen Rechtsvorschriften

Urteil vom 13. Mai 2014 (Große Kammer), Google Spain und Google (C-131/12, EU:C:2014:317)

In diesem Urteil (vgl. auch die Abschnitte II.3. „Begriff ‚Verarbeitung personenbezogener Daten'" und IV.1. „Recht, der Verarbeitung personenbezogener Daten zu widersprechen [‚Recht auf Vergessenwerden']") hat sich der Gerichtshof zum räumlichen Anwendungsbereich der Richtlinie 95/46/EG geäußert.

Er hat entschieden, dass im Sinne der Richtlinie 95/46/EG eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt, ausgeführt wird, wenn der Suchmaschinenbetreiber, obwohl er seinen Sitz in einem Drittstaat hat, in einem Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst eine Zweigniederlassung oder Tochtergesellschaft gründet, deren Tätigkeit auf die Einwohner dieses Staates ausgerichtet ist (Rn. 55, 60, Tenor 2).

Unter solchen Umständen sind die Tätigkeiten des Suchmaschinenbetreibers und die seiner Niederlassung in dem betreffenden Mitgliedstaat, auch wenn sie voneinander verschieden sind, untrennbar miteinander verbunden, da die die Werbeflächen betreffenden Tätigkeiten das Mittel darstellen, um die Suchmaschine wirtschaftlich rentabel zu machen, und die Suchmaschine gleichzeitig das Mittel ist, das die Durchführung dieser Tätigkeiten ermöglicht (Rn. 56).

VII. Recht der Öffentlichkeit auf Zugang zu Dokumenten der Organe der Europäischen Union und Schutz personenbezogener Daten

Urteil vom 29. Juni 2010 (Große Kammer), Kommission/Bavarian Lager (C-28/08 P, EU:C:2010:378)

Bavarian Lager, eine zum Zweck der Einfuhr deutschen Biers, das für den Ausschank in Gaststätten im Vereinigten Königreich bestimmt war, gegründete Gesellschaft, hatte Schwierigkeiten, ihr Erzeugnis abzusetzen, weil im Vereinigten Königreich viele Gastwirte durch Alleinbezugsvereinbarungen gebunden waren, die sie zum ausschließlichen Bierbezug von einer bestimmten Brauerei verpflichteten.

Nach der Bierlieferungsregelung des Vereinigten Königreichs mussten britische Brauereien es den Gaststättenbetreibern gestatten, auch von einer anderen Brauerei Bier zu beziehen, sofern es sich hierbei um Fassbier handelte („Guest Beer Provision", im Folgenden: GBP). Die meisten außerhalb des Vereinigten Königreichs erzeugten Biere konnten jedoch nicht als „Fassbier" im Sinne der GBP

angesehen werden und fielen somit nicht unter diese Bestimmung. Da Bavarian Lager diese Regelung als eine Maßnahme mit gleicher Wirkung wie eine mengenmäßige Einfuhrbeschränkung ansah, reichte sie eine Beschwerde bei der Kommission ein.

Im Rahmen des von dieser gegen das Vereinigte Königreich eingeleiteten Vertragsverletzungsverfahrens fand am 11. Oktober 1996 ein Treffen statt, an dem Vertreter der Gemeinschaftsverwaltung, der britischen Verwaltung und des Verbands der Bierbrauer des Gemeinsamen Marktes (CBMC) teilnahmen. Die britischen Behörden kündigten an, dass die fragliche Regelung dahin geändert werde, dass neben Fassbier auch Flaschenbier anderer Brauereien verkauft werden könne. Daraufhin teilte die Kommission Bavarian Lager mit, dass das Verfahren ausgesetzt werde.

Später stellte Bavarian Lager einen Antrag auf Übermittlung des vollständigen Protokolls des Treffens vom Oktober 1996 mit den Namen aller Teilnehmer, der von der Kommission mit Entscheidung vom 18. März 2004 unter Berufung auf den durch die Verordnung über den Schutz personenbezogener Daten garantierten Schutz der Privatsphäre dieser Personen abgelehnt wurde.

Bavarian Lager focht diese Entscheidung vor dem Gericht an. Mit Urteil vom 8. November 2007 erklärte das Gericht die Entscheidung der Kommission insbesondere deshalb für nichtig, weil die bloße Aufnahme der Namen der Betroffenen in die Liste der Personen, die für die von ihnen vertretenen Einrichtungen an einer Sitzung teilnähmen, keine Rechtsverletzung darstelle und nicht in ihre Privatsphäre eingreife. Die Kommission, unterstützt durch das Vereinigte Königreich und den Rat, legte daraufhin beim Gerichtshof ein Rechtsmittel gegen das Urteil des Gerichts ein.

Der Gerichtshof hat zunächst daraufhin hingewiesen, dass bei einem nach der Verordnung (EG) Nr. 1049/2001[31] über den Zugang zu Dokumenten gestellten Antrag auf Gewährung des Zugangs zu Dokumenten, die personenbezogene Daten enthalten, die Bestimmungen der Verordnung (EG) Nr. 45/2001 in vollem Umfang anwendbar werden, einschließlich der Bestimmung, wonach der Empfänger der Übermittlung personenbezogener Daten die Notwendigkeit der Preisgabe dieser Daten nachzuweisen hat, und derjenigen, wonach der Betroffene jederzeit aus zwingenden, schutzwürdigen, sich aus seiner besonderen Situation ergebenden Gründen gegen die Verarbeitung von ihn betreffenden Daten Widerspruch einlegen kann (Rn. 63).

Er hat weiter ausgeführt, dass die Liste der Teilnehmer eines im Rahmen eines Vertragsverletzungsverfahrens abgehaltenen Treffens im Protokoll dieses Treffens personenbezogene Daten im Sinne von Art. 2 Buchst. a der Verordnung Nr. 45/2001 enthält, da die Personen, die an diesem Treffen teilnahmen, identifiziert werden können (Rn. 70).

Demnach befand sich die Kommission mit ihrer Forderung, hinsichtlich der Personen, deren ausdrückliches Einverständnis mit der Übermittlung der sie betreffenden und im Protokoll enthaltenen personenbezogenen Daten fehlte, die Notwendigkeit der Übermittlung dieser Daten nachzuweisen, im Einklang mit Art. 8 Buchst. b dieser Verordnung (Rn. 77).

Wird nämlich in einem nach der Verordnung (EG) Nr. 1049/2001 gestellten Antrag keine ausdrückliche rechtliche Begründung gegeben und kein überzeugendes Argument vorgetragen, um die Notwendigkeit der Übermittlung dieser personenbezogenen Daten darzutun, ist es der Kommission nicht möglich, die verschiedenen Interessen der Beteiligten gegeneinander abzuwägen. Sie kann auch nicht gemäß Art. 8 Buchst. b der Verordnung (EG) Nr. 45/2001 prüfen, ob Gründe für die Annahme bestehen, dass durch

31 Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

diese Übermittlung möglicherweise die berechtigten Interessen der Betroffenen beeinträchtigt werden (Rn. 78)[32].

Urteil vom 16. Juli 2015, ClientEarth und PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

Die Europäische Behörde für Lebensmittelsicherheit (EFSA) hatte eine Arbeitsgruppe gebildet, um einen Leitfaden zur Präzisierung der Art und Weise der Durchführung von Art. 8 Abs. 5 der Verordnung (EG) Nr. 1107/2009[33] auszuarbeiten. Nach dieser Vorschrift fügt der Wirtschaftsteilnehmer, der eine Zulassung zum Inverkehrbringen eines Pflanzenschutzmittels beantragt, entsprechend den Vorgaben der EFSA dem Dossier ein Verzeichnis mit der wissenschaftlichen und von Fachleuten überprüften frei verfügbaren Literatur über den Wirkstoff und seine Metaboliten bei, in der die Nebenwirkungen auf die Gesundheit, die Umwelt und Nichtzielarten behandelt werden.

In der öffentlichen Konsultation zum Entwurf dieses Leitfadens reichten ClientEarth und Pesticide Action Network Europe (PAN Europe) Stellungnahmen ein. In diesem Zusammenhang stellten sie gemeinsam bei der EFSA einen Antrag auf Zugang zu mehreren Dokumenten, die die Vorbereitung dieses Entwurfs betrafen, einschließlich der Stellungnahmen externer Sachverständiger.

Die EFSA gewährte ClientEarth und PAN Europe Zugang u. a. zu den Stellungnahmen der externen Sachverständigen zum Leitfadenentwurf, wies jedoch darauf hin, dass sie die Namen dieser Sachverständigen gemäß Art. 4 Abs. 1 Buchst. b der Verordnung Nr. 1049/2001 und den Rechtsvorschriften der Union über den Schutz personenbezogener Daten, insbesondere der Verordnung (EG) Nr. 45/2001, unkenntlich gemacht habe. Die Verbreitung der Namen der Sachverständigen stelle eine Übermittlung personenbezogener Daten im Sinne von Art. 8 der Verordnung (EG) Nr. 45/2001 dar. Die dort genannten Voraussetzungen für eine Übermittlung dieser Daten seien im vorliegenden Fall aber nicht erfüllt.

ClientEarth und PAN Europe fochten diese Entscheidung vor dem Gericht an, das die Klage abwies. Daraufhin legten ClientEarth und PAN Europe beim Gerichtshof ein Rechtsmittel gegen das Urteil[34] des Gerichts ein.

Der Gerichtshof hat erstens festgestellt, dass es sich bei der angeforderten Information, da eine bestimmte Stellungnahme einem bestimmten Sachverständigen zugeordnet werden könnte, um eine Information über eine bestimmte natürliche Person und somit um eine Gesamtheit personenbezogener Daten im Sinne von Art. 2 Buchst. a der Verordnung (EG) Nr. 45/2001 handelt. Da sich der Begriff der personenbezogenen Daten im Sinne von Art. 2 Buchst. a der Verordnung (EG) Nr. 45/2001 und der Begriff der Daten über das Privatleben nicht überschneiden, hat der Gerichtshof ausgeführt, dass das Vorbringen von ClientEarth und PAN Europe, die streitige Information falle nicht unter das Privatleben der betreffenden Sachverständigen, im vorliegenden Fall ins Leere ging (Rn. 29, 32).

Der Gerichtshof hat zweitens das Vorbringen von ClientEarth und PAN Europe geprüft, wonach ein Klima des Misstrauens gegenüber der EFSA bestehe, der oft Parteilichkeit vorgeworfen werde, weil sie auf Sachverständige zurückgreife, die durch ihre Verbindungen zur Industrie bedingte persönliche Interessen hätten, und die Transparenz des Entscheidungsprozesses der EFSA gewährleistet werden müsse. Dieses Vorbringen war auf eine Studie gestützt, in der festgestellt wurde, dass die meisten Sachverständigen, die Mitglieder einer Arbeitsgruppe der EFSA sind, Verbindungen zu Industrielobbys unterhalten. Der Gerichtshof hat hierzu festgestellt, dass die Erlangung der streitigen Information erforderlich war, um

32 Dieses Urteil wurde im Jahresbericht 2010, S. 14, dargestellt.

33 Verordnung (EG) Nr. 1107/2009 des Europäischen Parlaments und des Rates vom 21. Oktober 2009 über das Inverkehrbringen von Pflanzenschutzmitteln und zur Aufhebung der Richtlinien 79/117/EWG und 91/414/EWG des Rates (ABl. L 309 vom 24.11.2009, S. 1).

34 Urteil des Gerichts vom 13. September 2013, ClientEarth und PAN Europe/EFSA (T-214/11, EU:T:2013:483).

konkret prüfen zu können, ob die einzelnen Sachverständigen bei der Erfüllung ihrer wissenschaftlichen Aufgabe im Dienste der EFSA unparteiisch waren. Der Gerichtshof hat daher das Urteil des Gerichts aufgehoben, da dieses zu Unrecht festgestellt hatte, dass dieses Vorbringen von ClientEarth und PAN Europe für den Nachweis der Notwendigkeit der Übermittlung der streitigen Information nicht genüge (Rn. 57-59).

Drittens hat der Gerichtshof zur Beurteilung der Rechtmäßigkeit der streitigen Entscheidung der EFSA geprüft, ob Grund zu der Annahme besteht, dass durch die Übermittlung möglicherweise die berechtigten Interessen der betroffenen Personen beeinträchtigt worden wären. Insoweit hat der Gerichtshof ausgeführt, dass es sich bei der Behauptung der EFSA, bei Verbreitung der streitigen Information hätte die Gefahr einer Beeinträchtigung des Privatlebens und der Integrität der Sachverständigen bestanden, um eine allgemeine Erwägung handelte, die durch keinen fallspezifischen Umstand weiter begründet wurde. Vielmehr hätte, so der Gerichtshof, durch die Verbreitung der streitigen Information als solche der Verdacht der Parteilichkeit zerstreut oder den eventuell betroffenen Sachverständigen Gelegenheit gegeben werden können, die Begründetheit dieser Behauptungen der Parteilichkeit, gegebenenfalls mittels der verfügbaren Rechtsbehelfe, in Zweifel zu ziehen. In Anbetracht dessen hat der Gerichtshof die Entscheidung der EFSA für nichtig erklärt (Rn. 69, 73).

* * *

Die in dieser Übersicht angeführten Urteile sind im Repertorium der Rechtsprechung unter den Rubriken 1.04.03.07, 1.04.03.08, 1.04.03.11, 2.04, 2.05.00, 4.11.01 und 4.11.07 indexiert.