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 war 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 legte die allgemeinen Bedingungen, unter denen die Verarbeitung dieser Daten rechtmäßig ist, und die Rechte der betroffenen Personen fest und sah u. a. die Errichtung unabhängiger Kontrollbehörden in den Mitgliedstaaten vor.

Die Richtlinie 2002/58/EG[2] wurde sodann durch die Richtlinie 95/46 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]. Der Unionsgesetzgeber beabsichtigt eine Überarbeitung dieser Richtlinie. Hierzu legte die Kommission am 10. Januar 2017 einen Vorschlag zur Ersetzung der Richtlinie 95/46 durch eine Verordnung über das Privatleben und die elektronische Kommunikation[4] vor.

Auf dem Gebiet des Raums der Freiheit, der Sicherheit und des Rechts (früher Art. 30 und 31 EUV) regelte der Rahmenbeschluss 2008/977/JI[5] (bis Mai 2018) den Schutz personenbezogener Daten im Zusammenhang mit der justiziellen Zusammenarbeit in Straf- und Polizeisachen.

2016 reformierte die Europäische Union die einschlägigen allgemeinen Regelungen. Zu diesem Zweck hat sie die Verordnung (EU) 2016/679[6] zum Datenschutz (im Folgenden: DSGVO) erlassen, die die Richtlinie 95/46 aufhebt und seit dem 25. Mai 2018 anwendbar ist, sowie die Richtlinie (EU) 2016/680[7] 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 wurde der Schutz personenbezogener Daten im Zusammenhang mit ihrer Verarbeitung durch die Organe und Einrichtungen der EU zunächst durch die Verordnung (EG)

---

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. 1995, L 281, S. 31), konsolidierte Fassung vom 20. November 2003, aufgehoben zum 25. Mai 2018 (siehe Fn. 5).

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. 2002; L 201, S. 37), konsolidierte Fassung vom 19. Dezember 2009.

3 Die Richtlinie 2002/58 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. 2006, L 105, 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 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 10 final – 2017/3 (COD).

5 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. 2008, L 350, S. 60), aufgehoben mit Wirkung vom 6. Mai 2018 (siehe Fn. 6).

6 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. 2016, L 119, S. 1).

7 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. 2016, L 119, S. 89).

Nr. 45/2001[8] gewährleistet. Aufgrund dieser Verordnung wurde u. a. 2004 der Europäische Datenschutzbeauftragte berufen. 2018 wurde dieser Bereich von der Europäischen Union insbesondere durch den Erlass der seit dem 11. Dezember 2018 geltenden Verordnung (EU) 2018/1725[9], mit der die Verordnung Nr. 45/2001 und der Beschluss Nr. 1247/2002/EG[10] aufgehoben wurden, neu geregelt. Im Interesse einer einheitlichen Herangehensweise hinsichtlich des Schutzes personenbezogener Daten in der gesamten Union sollen mit dieser neuen Verordnung die Datenschutzbestimmungen so weit wie möglich an die Regelung der DSGVO angeglichen werden.

8 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. 2001, L 8, S. 1).

9 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018, 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 (ABl. 2018, L 295, S. 39).

10 Beschluss Nr. 1247/2002/EG des Europäischen Parlaments, des Rates und der Kommission vom 1. Juli 2002 über die Regelungen und allgemeinen Bedingungen für die Ausübung der Aufgaben des Europäischen Datenschutzbeauftragten (ABl. 2002, L 183, S. 1).

INHALTSVERZEICHNIS

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)[11]

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[12] und 259/2008[13] 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 Nr. 1290/2005 und zur Gültigkeit der Verordnung 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

---

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

12 Verordnung (EG) Nr. 1290/2005 des Rates vom 21. Juni 2005 über die Finanzierung der Gemeinsamen Agrarpolitik (ABl. 2005, L 209, 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. 2013, L 347, S. 549).

13 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. 2008, L 76, 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. 2014, L 255, S. 59).

ihres Privatlebens im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen darstellt, da Dritte Zugang zu diesen Daten erhalten (Rn. 56 bis 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 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 und 86).

Der Gerichtshof hat daher bestimmte Vorschriften der Verordnung Nr. 1290/2005 sowie die Verordnung 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 und 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 (Rn. 94 und 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[14], 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.

[14] 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. 2004, L 385, S. 1) in der durch die Verordnung (EG) Nr. 444/2009 des Europäischen Parlaments und des Rates vom 6. Mai 2009 (ABl. 2009, L 142, S. 1) geänderten Fassung.

Der Gerichtshof hat dies bejaht. Er hat entschieden, dass die in Art. 1 Abs. 2 der Verordnung 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 bis 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 bis 45).

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 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 bis 57, 60 und 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)[15]

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 in das österreichische Recht befasst worden.

[15] Dieses Urteil wurde im Jahresbericht 2014, S. 62 und 63, dargestellt.

Mit ihren Vorabentscheidungsersuchen befragten das irische und das österreichische Gericht den Gerichtshof zur Gültigkeit der Richtlinie 2006/24 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 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 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 bis 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 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 bis 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 bis 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 und 64).

Der Gerichtshof hat ferner zu den sich aus Art. 8 Abs. 3 der Charta ergebenden Anforderungen festgestellt, dass die Richtlinie 2006/24 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 bis 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)[16]

Nachdem die Richtlinie 2006/24 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.

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.

[16] Dieses Urteil wurde im Jahresbericht 2016, S. 63 und 64, dargestellt.

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 (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 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 bis 105, 107, 112 und 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 bis 122, 125 und Tenor 2).

Dagegen steht Art. 15 Abs. 1 der Richtlinie 2002/58 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 bis 111).

II. Verarbeitung personenbezogener Daten im Sinne der allgemeinen Datenschutzregelung

1. Vom Anwendungsbereich der Richtlinie 95/46 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[17], 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[18], 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 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 den Fluggesellschaften im Rahmen einer unter das Unionsrecht fallenden Tätigkeit erhoben worden, nämlich beim Verkauf eines Flugscheins, der zu einer

[17] 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. 2004, L 235, S. 11).

[18] 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. 2004, L 183, S. 83, berichtigt in ABl. 2005, L 255, S. 168).

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 als erforderlich angesehen wird (Rn. 56 und 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 und 59).

Zum Beschluss des Rates hat der Gerichtshof festgestellt, dass Art. 95 EG in Verbindung mit Art. 25 der Richtlinie 95/46 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 bis 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), bei dem Herr Ryneš ein Rechtsmittel gegen das Urteil des Městský soud v Praze (Stadtgericht Prag, Tschechische Republik), 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 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, 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 bis 29). Bereits nach dem Wortlaut dieser Bestimmung ist von der Richtlinie 95/46 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 und 33).

2. Begriff „personenbezogene Daten"

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

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.

[19] Dieses Urteil wurde im Jahresbericht 2016, S. 62 und 63, dargestellt.

Der Gerichtshof hat zunächst ausgeführt, dass es für die Einstufung eines Datums als „personenbezogenes Datum“ im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 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 darstellen (Rn. 43 und 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 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 und Tenor 1).

Urteil vom 20. Dezember 2017, Nowak (C-434/16, EU:C:2017:994)

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 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 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 (Rn. 31 und 36 bis 40).

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 (Rn. 42 und 43).

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 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 erstrecken sich allerdings nicht auf Prüfungsfragen, die als solche keine personenbezogenen Daten des Prüflings darstellen (Rn. 56 und 58).

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 darstellen (Rn. 62 und Tenor).

3. Begriff „Verarbeitung personenbezogener Daten“

Urteil vom 6. November 2003 (Große Kammer), 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 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 und 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 bis 48 und 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 weit verbreiteten 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 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 und 30).

Urteil vom 10. Juli 2018 (Große Kammer), Jehovan todistajat (C-25/17, EU:C:2018:551)[20]

Die finnische Datenschutzbehörde hatte eine Entscheidung erlassen, mit der der Gemeinschaft der Zeugen Jehovas verboten wurde, im Rahmen der von ihren Mitgliedern von Tür zu Tür durchgeführten Verkündigungstätigkeit personenbezogene Daten zu erheben oder zu verarbeiten, ohne dass die nach den finnischen Rechtsvorschriften für die Verarbeitung solcher Daten erforderlichen Voraussetzungen eingehalten werden. Die Mitglieder dieser Gemeinschaft machen sich im Rahmen ihrer von Tür zu Tür durchgeführten Verkündigungstätigkeit Notizen über Besuche bei Personen, die weder ihnen noch der Gemeinschaft bekannt sind. Diese Daten werden als Gedächtnisstütze erhoben, um für den Fall eines erneuten Besuchs wiederauffindbar zu sein, ohne dass die betroffenen Personen hierin eingewilligt hätten oder darüber informiert worden wären. Die Gemeinschaft der Zeugen Jehovas hat ihren Mitgliedern insoweit Anleitungen zur Anfertigung solcher Notizen gegeben, die in mindestens einem ihrer der Verkündigungstätigkeit gewidmeten Mitteilungsblätter abgedruckt sind.

Der Gerichtshof hat entschieden, dass die Erhebung personenbezogener Daten, die durch Mitglieder einer Religionsgemeinschaft im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erfolgt, und die anschließenden Verarbeitungen dieser Daten nicht unter die Ausnahmen vom Anwendungsbereich der Richtlinie 95/46 fallen, da es sich dabei weder um Verarbeitungen personenbezogener Daten, die für die Ausübung von in Art. 3 Abs. 2 erster Gedankenstrich dieser Richtlinie genannten Tätigkeiten erfolgen, noch um Verarbeitungen personenbezogener Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder

[20] Dieses Urteil wurde im Jahresbericht 2018, S. 90, dargestellt.

familiärer Tätigkeiten vorgenommen werden, im Sinne von Art. 3 Abs. 2 zweiter Gedankenstrich der Richtlinie handelt (Rn. 51 und Tenor 1).

Urteil vom 14. Februar 2019, Buivids (C-345/17, EU:C:2019:122)

In dieser Rechtssache hatte der Gerichtshof über den Anwendungsbereich der Richtlinie 95/46 und über den Begriff „Verarbeitung personenbezogener Daten, die allein zu journalistischen … Zwecken erfolgt", im Sinne von Art. 9 dieser Richtlinie zu befinden.

Ihm lag ein Vorabentscheidungsersuchen des Obersten Gerichtshof von Lettland vor, das über einen Rechtsstreit zwischen Herrn Buivids (im Folgenden: Kläger) und der nationalen Datenschutzbehörde zu entscheiden hatte. Gegenstand war eine Klage auf Feststellung der Rechtswidrigkeit einer Entscheidung der nationalen Datenschutzbehörde, nach der Herr Buivids gegen nationale Datenschutzvorschriften verstoßen haben soll, indem er auf einer Website ein von ihm selbst gefilmtes Video über die Aufnahme seiner Aussage durch Polizeibeamte in den Räumlichkeiten einer Dienststelle der nationalen Polizei im Rahmen eines Ordnungswidrigkeitenverfahrens veröffentlicht habe. Nachdem seine Klage von den beiden Vorinstanzen abgewiesen worden war, legte der Kläger beim Obersten Gerichtshof eine Kassationsbeschwerde ein. Er berief sich auf sein Recht auf freie Meinungsäußerung und machte geltend, dass das in Rede stehende Video Beamte der nationalen Polizei, die öffentliche Personen seien, an einem für die Öffentlichkeit zugänglichen Ort zeige. Das Datenschutzgesetz finde auf diese Personen daher keine Anwendung.

Als Erstes hat der Gerichtshof zum Anwendungsbereich der Richtlinie 95/46 festgestellt, dass die Bilder der in dem Video aufgezeichneten Polizeibeamten personenbezogene Daten darstellen und dass die im Speicher der vom Kläger verwendeten Kamera gespeicherte Videoaufzeichnung dieser Personen eine Verarbeitung personenbezogener Daten darstellt. Der Gerichtshof hat weiter festgestellt, dass die Veröffentlichung einer Videoaufzeichnung mit personenbezogenen Daten auf einer Website, auf der Videos angeschaut und geteilt werden können, eine ganz oder teilweise automatisierte Verarbeitung dieser Daten darstellt. Er hat klargestellt, dass die Aufzeichnung und die Veröffentlichung eines solchen Videos weder als Verarbeitung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich der Richtlinie 95/46 fallen, noch als Verarbeitung personenbezogener Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird, vom Anwendungsbereich der Richtlinie 95/46 ausgenommen sind. Der Gerichtshof ist daher zu dem Schluss gelangt, dass die Aufzeichnung von Polizeibeamten in einer Polizeidienststelle auf Video während der Aufnahme einer Aussage und die Veröffentlichung des so aufgezeichneten Videos auf einer Video-Website, auf der die Nutzer Videos versenden, anschauen und teilen können, in den Anwendungsbereich der Richtlinie 95/46 fällt (Rn. 31, 32, 35, 39, 42, 43 und Tenor 1).

Als Zweites hat der Gerichtshof zum Begriff „Verarbeitung personenbezogener Daten, die allein zu journalistischen … Zwecken erfolgt" festgestellt, dass der Begriff des Journalismus weit auszulegen ist und die in Art. 9 der Richtlinie 95/46 vorgesehenen Befreiungen und Ausnahmen somit für jeden gelten, der journalistisch tätig ist. Er hat deshalb entschieden, dass der Umstand, dass der Kläger kein Berufsjournalist ist, es nicht ausschließt, dass die Aufzeichnung des in Rede

stehenden Videos und dessen Veröffentlichung als Verarbeitung personenbezogener Daten, die allein zu journalistischen Zwecken erfolgt, eingestuft werden können. Der Gerichtshof hat weiter darauf hingewiesen, dass die in Art. 9 der Richtlinie 95/46 vorgesehenen Befreiungen und Ausnahmen nur in dem Umfang angewandt werden dürfen, in dem sie sich als notwendig erweisen, um zwei Grundrechte, nämlich das Recht auf Schutz der Privatsphäre und das Recht auf freie Meinungsäußerung, miteinander in Einklang zu bringen. Insoweit hat der Gerichtshof festgestellt, dass nicht ausgeschlossen werden kann, dass die Aufzeichnung und die Veröffentlichung des in Rede stehenden Videos, die erfolgt sind, ohne dass die in dem Video zu sehenden Polizisten über diese Aufzeichnung und deren Zwecke informiert wurden, einen Eingriff in das Grundrecht auf Achtung des Privatlebens dieser Personen darstellt. Der Gerichtshof ist daher zu dem Schluss gelangt, dass die Aufzeichnung und die Veröffentlichung des in Rede stehenden Videos auf einer Video-Website, eine Verarbeitung personenbezogener Daten allein zu journalistischen Zwecken darstellen können, sofern aus dem Video hervorgeht, dass seine Aufzeichnung und seine Veröffentlichung ausschließlich zum Ziel hatten, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten, was zu prüfen Sache des vorlegenden Gerichts ist (Rn. 51, 52, 55, 63, 67 und Tenor 2).

Urteil vom 22. Juni 2021 (Große Kammer), Latvijas Republikas Saeima (Strafpunkte) (C-439/19, EU:C:2021:504)

Gegen B, eine natürliche Person, waren wegen eines oder mehrerer Verkehrsverstöße Strafpunkte verhängt worden. Diese Strafpunkte wurden von der Ceļu satiksmes drošības direkcija (Direktion für Straßenverkehrssicherheit, Lettland) (im Folgenden: CSDD) in das nationale Register für Fahrzeuge und Fahrzeugführer eingetragen.

Nach der lettischen Straßenverkehrsregelung[21] sind die Informationen über gegen Fahrzeugführer verhängte und in diesem Register eingetragene Strafpunkte öffentlich zugänglich und werden von der CSDD jeder Person übermittelt, die dies beantragt, ohne dass sie ein besonderes Interesse am Erhalt dieser Informationen nachzuweisen hätte, u. a. an Wirtschaftsteilnehmer zum Zweck der Weiterverwendung. B, der Zweifel an der Rechtmäßigkeit dieser Regelung hatte, legte bei der Latvijas Republikas Satversmes tiesa (Verfassungsgericht, Lettland) Verfassungsbeschwerde ein, damit sie die Vereinbarkeit dieser Regelung mit dem Recht auf Achtung des Privatlebens prüft.

Das Verfassungsgericht meinte, dass es im Rahmen seiner Beurteilung dieses durch die Verfassung garantierten Rechts die DSGVO zu berücksichtigen habe. Daher ersuchte es den Gerichtshof, die Bedeutung mehrerer Bestimmungen der DSGVO zu erläutern, um zu klären, ob die lettische Straßenverkehrsregelung mit dieser Verordnung vereinbar ist.

Mit seinem Urteil hat der Gerichtshof (Große Kammer) entschieden, dass die Verarbeitung personenbezogener Daten über Strafpunkte eine „Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten“[22] darstellt, für die die DSGVO wegen der

[21] Art. 14[1] Abs. 2 des Ceļu satiksmes likums (Straßenverkehrsgesetz) vom 1. Oktober 1997 (Latvijas Vēstnesis, 1997, Nr. 274/276).
[22] Art. 10 DSGVO.

besonderen Sensibilität der betreffenden Daten einen erhöhten Schutz vorsieht (Rn. 10, 46, 74, 94 und Tenor 1).

In diesem Zusammenhang hat der Gerichtshof einleitend ausgeführt, dass die Informationen über Strafpunkte personenbezogene Daten darstellen und dass ihre Übermittlung durch die CSDD an Dritte eine Verarbeitung darstellt, die in den sachlichen Anwendungsbereich der DSGVO fällt. Dieser Anwendungsbereich ist nämlich sehr weit, und die entsprechende Verarbeitung fällt unter keine der Ausnahmen von der Anwendbarkeit dieser Verordnung (Rn. 60, 61 und 72).

Diese Verarbeitung fällt zum einen nicht unter die Ausnahme, wonach die DSGVO keine Anwendung auf eine Verarbeitung im Rahmen einer Tätigkeit findet, die nicht in den Anwendungsbereich des Unionsrechts fällt[23]. Diese Ausnahme ist so zu verstehen, dass damit vom Anwendungsbereich dieser Verordnung allein Verarbeitungen personenbezogener Daten ausgenommen sein sollen, die von staatlichen Stellen im Rahmen einer Tätigkeit, die der Wahrung der nationalen Sicherheit dient, oder einer Tätigkeit, die dieser Kategorie zugeordnet werden kann, vorgenommen werden. Dazu gehören insbesondere Tätigkeiten, die den Schutz der grundlegenden Funktionen des Staates und der grundlegenden Interessen der Gesellschaft bezwecken. Mit den Tätigkeiten, die die Straßenverkehrssicherheit betreffen, wird jedoch kein solches Ziel verfolgt, so dass sie nicht der Kategorie der auf die Wahrung der nationalen Sicherheit abzielenden Tätigkeiten zugeordnet werden können (Rn. 62 und 66 bis 68).

Zum anderen ist die Übermittlung personenbezogener Daten über Strafpunkte auch keine Verarbeitung, die von der Ausnahme erfasst wird, wonach die DSGVO auf Verarbeitungen personenbezogener Daten durch die zuständigen Behörden im Bereich des Strafrechts keine Anwendung findet[24]. Die CSDD kann nämlich bei der entsprechenden Übermittlung nicht als eine solche „zuständige Behörde“[25] angesehen werden (Rn. 69 bis 71).

Um zu bestimmen, ob der Zugang zu personenbezogenen Daten über Verkehrsverstöße, etwa Strafpunkten, eine Verarbeitung personenbezogener Daten über „Straftaten“[26] darstellt, für die ein verstärkter Schutz gilt, hat der Gerichtshof insbesondere unter Heranziehung der Entstehungsgeschichte der DSGVO festgestellt, dass dieser Begriff ausschließlich auf Straftaten im Sinne des Strafrechts verweist. Allerdings ist der Umstand, dass Verkehrsverstöße in der lettischen Rechtsordnung als Ordnungswidrigkeiten eingestuft werden, für die Beurteilung, ob diese Verstöße unter den Begriff „Straftaten“ fallen, nicht entscheidend, da es sich um einen autonomen Begriff des Unionsrechts handelt, der in der gesamten Union autonom und einheitlich auszulegen ist. Nach einem Hinweis auf die drei Kriterien, die für die Beurteilung des strafrechtlichen Charakters einer Zuwiderhandlung maßgeblich sind, nämlich die rechtliche Einordnung der Zuwiderhandlung im innerstaatlichen Recht, die Art der Zuwiderhandlung und der Schweregrad der drohenden Sanktion, hat der Gerichtshof festgestellt, dass die fraglichen Verkehrsverstöße unter den Begriff „Straftaten“ im Sinne der DSGVO fallen. Zu den ersten

[23] Art. 2 Abs. 2 Buchst. a DSGVO.
[24] Art. 2 Abs. 2 Buchst. d DSGVO.
[25] Art. 3 Nr. 7 der 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. 2016, L 119, S. 89).
[26] Art. 10 DSGVO.

beiden Kriterien hat der Gerichtshof ausgeführt, dass die entsprechenden Verstöße zwar im innerstaatlichen Recht nicht als „strafrechtliche“ Verstöße eingestuft werden, dass sich ein solcher Charakter aber aus der Art der Zuwiderhandlung und insbesondere dem repressiven Zweck der Sanktion, die der Verstoß nach sich ziehen kann, ergeben kann. Im vorliegenden Fall wird mit der Verhängung von Strafpunkten für Verkehrsverstöße ebenso wie mit den anderen Sanktionen, die ihre Begehung nach sich ziehen kann, u. a. ein solcher repressiver Zweck verfolgt. In Bezug auf das dritte Kriterium hat der Gerichtshof darauf hingewiesen, dass nur Verkehrsverstöße von gewisser Schwere zur Verhängung von Strafpunkten führen und dass diese Verstöße somit zu Sanktionen mit einem gewissen Schweregrad führen können. Außerdem kommt die Verhängung solcher Punkte im Allgemeinen zu der verhängten Sanktion hinzu, und die Kumulierung solcher Punkte hat rechtliche Folgen, die bis zu einem Fahrverbot reichen können (Rn. 77, 80, 85, 87 bis 90 und 93).

4. Begriff „Datei mit personenbezogenen Daten“

Urteil vom 10. Juli 2018 (Große Kammer), Jehovan todistajat (C-25/17, EU:C:2018:551)

In diesem Urteil (vgl. auch Abschnitt II.3 „Begriff ‚Verarbeitung personenbezogener Daten‘“) hat der Gerichtshof den Begriff der Datei im Sinne von Art. 2 Buchst. c der Richtlinie 95/46 präzisiert.

Nach einem Hinweis darauf, dass die Richtlinie für manuelle Verarbeitungen personenbezogener Daten nur dann gilt, wenn die verarbeiteten Daten in einer Datei gespeichert sind oder gespeichert werden sollen, hat der Gerichtshof festgestellt, dass der Begriff der Datei eine Sammlung personenbezogener Daten, die im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erhoben wurden und zu denen Namen und Adressen sowie weitere Informationen über die aufgesuchten Personen gehören, umfasst, sofern diese Daten in der Praxis zur späteren Verwendung leicht wiederauffindbar sind. Es ist hingegen nicht erforderlich, dass diese Sammlung aus spezifischen Kartotheken oder Verzeichnissen oder anderen der Recherche dienenden Ordnungssystemen besteht. (Rn. 62 und Tenor 2).

5. Begriff „für die Verarbeitung [personenbezogener Daten] Verantwortlicher“

Urteil vom 10. Juli 2018 (Große Kammer), Jehovan todistajat (C-25/17, EU:C:2018:551)

In dieser Rechtssache (vgl. auch Abschnitte II.3 „Begriff ‚Verarbeitung personenbezogener Daten‘“ und II.4 „Begriff ‚Datei mit personenbezogenen Daten‘“) hat der Gerichtshof darüber entschieden, ob eine Religionsgemeinschaft für die Verarbeitungen personenbezogener Daten verantwortlich ist, die im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erfolgen, die von der Gemeinschaft organisiert und koordiniert wird und zu der sie ermuntert.

Der Gerichtshof hat hierzu ausgeführt, dass die für jedermann geltende Pflicht, die Vorschriften des Unionsrechts über den Schutz personenbezogener Daten einzuhalten, nicht als Eingriff in die organisatorische Autonomie der Religionsgemeinschaften angesehen werden kann. Er hat daher entschieden, dass Art. 2 Buchst. d der Richtlinie 95/46 im Licht von Art. 10 Abs. 1 der Charta dahin auszulegen ist, dass eine Religionsgemeinschaft gemeinsam mit ihren als

Verkündiger tätigen Mitgliedern als Verantwortliche für die Verarbeitungen personenbezogener Daten angesehen werden kann, die durch diese Mitglieder im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erfolgen, die von dieser Gemeinschaft organisiert und koordiniert wird und zu der sie ermuntert, ohne dass es hierfür erforderlich wäre, dass die Gemeinschaft Zugriff auf diese Daten hat oder ihren Mitgliedern nachweislich schriftliche Anleitungen oder Anweisungen zu diesen Datenverarbeitungen gegeben hat (Rn. 74, 75 und Tenor 3).

Urteil vom 5. Juni 2018 (Große Kammer), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)[27]

Eine deutsche Datenschutzbehörde hatte in ihrer Eigenschaft als Kontrollstelle im Sinne von Art. 28 der Richtlinie 95/46 einem deutschen Bildungsunternehmen, das Bildungsdienstleistungen über eine auf dem sozialen Netzwerk Facebook unterhaltene Fanpage anbietet, aufgegeben, diese zu deaktivieren. Denn ihrer Ansicht nach hatten weder das Unternehmen noch Facebook die Besucher der Fanpage darüber informiert, dass Facebook über Cookies sie betreffende personenbezogene Daten erhebt und dass das Unternehmen und Facebook diese anschließend verarbeiten.

In diesem Zusammenhang hat der Gerichtshof den Begriff des für die Verarbeitung personenbezogener Daten Verantwortlichen präzisiert. Der Gerichtshof hat insoweit ausgeführt, dass der Betreiber einer auf Facebook unterhaltenen Fanpage wie das im Ausgangsverfahren in Rede stehende Unternehmen durch die von ihm vorgenommene Parametrierung (u. a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten) an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt ist. Daher ist dieser Betreiber gemeinsam mit Facebook Ireland (die Tochtergesellschaft des amerikanischen Unternehmens Facebook) als in der Union für diese Verarbeitung Verantwortlicher im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 einzustufen (Rn. 39).

Urteil vom 29. Juli 2019, Fashion ID (C-40/17, EU:C:2019:629)

In dieser Rechtssache hatte der Gerichtshof Gelegenheit, den Begriff „für die Verarbeitung Verantwortlicher“ im Hinblick auf die Einbindung eines Plugins in eine Website weiterzuentwickeln.

Fashion ID, ein deutscher Online-Händler für Modeartikel, hatte in ihre Website das Social Plugin „Gefällt mir“ des sozialen Netzwerks Facebook eingebunden. Aufgrund der Einbindung dieses Plugins in die Website wurden beim Aufrufen der Website von Fashion ID durch einen Besucher offenbar personenbezogene Daten dieses Besuchers an Facebook Ireland übermittelt. Offenbar erfolgt diese Übermittlung, ohne dass sich der Besucher dessen bewusst ist und unabhängig davon, ob er Mitglied des sozialen Netzwerks Facebook ist oder den „Gefällt mir“-Button von Facebook angeklickt hat.

[27] Dieses Urteil wurde im Jahresbericht 2018, S. 89, dargestellt.

Die Verbraucherzentrale NRW, ein deutscher gemeinnütziger Verband zur Wahrung von Verbraucherinteressen, wirft Fashion ID vor, personenbezogene Daten der Besucher ihrer Website ohne deren Einwilligung und unter Verstoß gegen die Informationspflichten nach den Vorschriften über den Schutz personenbezogener Daten an Facebook Ireland übermittelt zu haben. Das Oberlandesgericht Düsseldorf (Deutschland), das über den Rechtsstreit zu entscheiden hatte, ersuchte den Gerichtshof um die Auslegung mehrerer Bestimmungen der Richtlinie 95/46.

Der Gerichtshof hat festgestellt, dass der Betreiber einer Website wie Fashion ID als für die Verarbeitung Verantwortlicher im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 angesehen werden kann. Diese Verantwortlichkeit ist jedoch auf den Vorgang oder die Vorgänge der Verarbeitung personenbezogener Daten beschränkt, für den bzw. für die er tatsächlich über die Zwecke und Mittel entscheidet, d. h. das Erheben der in Rede stehenden Daten und deren Weitergabe durch Übermittlung. Dagegen ist nach Auffassung des Gerichtshofs auf den ersten Blick ausgeschlossen, dass Fashion ID über die Zwecke und Mittel der Vorgänge der Verarbeitung personenbezogener Daten entscheidet, die Facebook Ireland nach der Übermittlung dieser Daten an sie vorgenommen hat, so dass Fashion ID für diese Vorgänge nicht als verantwortlich im Sinne von Art. 2 Buchst. d angesehen werden kann (Rn. 76, 85 und Tenor 2).

Der Gerichtshof hat weiter festgestellt, dass es erforderlich ist, dass der Betreiber einer Website und der Anbieter eines Social Plugins mit diesen Verarbeitungsvorgängen jeweils ein berechtigtes Interesse im Sinne von Art. 7 Buchst. f der Richtlinie 95/46 wahrnehmen, damit diese Vorgänge für jeden Einzelnen von ihnen gerechtfertigt sind (Rn. 97 und Tenor 3).

Schließlich hat der Gerichtshof erläutert, dass die nach Art. 2 Buchst. h und Art. 7 Buchst. a der Richtlinie 95/46 zu erklärende Einwilligung von dem Betreiber einer Website nur in Bezug auf die Vorgänge der Verarbeitung personenbezogener Daten einzuholen ist, für die der Betreiber der Website tatsächlich über die Zwecke und Mittel entscheidet. In einer solchen Situation trifft die in Art. 10 der Richtlinie vorgesehene Informationspflicht auch den Betreiber der Website. Dieser muss die betroffene Person jedoch nur in Bezug auf den Vorgang oder die Vorgänge der Verarbeitung personenbezogener Daten informieren, für den bzw. für die er tatsächlich über die Zwecke und Mittel entscheidet (Rn. 106 und Tenor 4).

Urteil vom 9. Juli 2020, Land Hessen, C-272/19, EU:C:2020:535

Ein Bürger, der eine Petition beim Petitionsausschuss des Parlaments des Landes Hessen (Deutschland) eingereicht hatte, begehrte von diesem Ausschuss Auskunft über die ihn betreffenden personenbezogenen Daten, die dieser im Rahmen der Behandlung seiner Petition gespeichert hatte. Dabei stützte er sich auf die DSGVO, die das Recht der betroffenen Person vorsieht, von dem für die Verarbeitung Verantwortlichen Auskunft über die sie betreffenden personenbezogenen Daten zu erhalten.

Der Präsident des Hessischen Landtags lehnte diesen Antrag mit der Begründung ab, dass das Petitionsverfahren eine parlamentarische Aufgabe sei und dass das Parlament nicht der DSGVO unterliege.

Das von diesem Bürger angerufene Verwaltungsgericht Wiesbaden (Deutschland) ist der Auffassung, dass das deutsche Recht im Rahmen einer solchen Petition kein Recht auf Auskunft über die personenbezogenen Daten vorsehe. Ein Auskunftsrecht könnte sich jedoch aus der DSGVO ergeben, was vom Gerichtshof zu klären sei. Da das Verwaltungsgericht außerdem Zweifel an seiner eigenen Unabhängigkeit und somit an seiner Eigenschaft als Gericht hatte, das zur Vorlage an den Gerichtshof berechtigt ist, befragte es den Gerichtshof auch zu diesem Aspekt.

Mit seinem Urteil hat der Gerichtshof geantwortet, dass der Petitionsausschuss eines Gliedstaats eines Mitgliedstaats insoweit, als er allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, als „Verantwortlicher" im Sinne der DSGVO[28] einzustufen ist. Die von einem solchen Ausschuss vorgenommene Verarbeitung personenbezogener Daten unterliegt daher dieser Verordnung, u. a. der Bestimmung, die den betroffenen Personen ein Recht auf Auskunft über die sie betreffenden personenbezogenen Daten verleiht[29].

Der Gerichtshof hat insbesondere festgestellt, dass die Tätigkeiten des Petitionsausschusses des Hessischen Landtags nicht unter eine in der DSGVO vorgesehene Ausnahme fallen. Zwar sind diese Tätigkeiten behördlicher Art und für dieses Land spezifisch, da der Ausschuss mittelbar zur parlamentarischen Tätigkeit beiträgt, sie sind jedoch auch politischer und administrativer Natur. Zudem, so der Gerichtshof, ergibt sich aus den ihm vorliegenden Akten nicht, dass diese Tätigkeiten in diesem Fall unter eine der Ausnahmen nach der DSGVO fielen (Rn. 71 bis 74 und Tenor).

6. Voraussetzungen für die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Urteil vom 16. Dezember 2008 (Große Kammer), Huber (C-524/06, EU:C:2008:724)[30]

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.

---

28 Art. 4 Nr. 7 DSGVO.
29 Art. 15 DSGVO.
30 Dieses Urteil wurde im Jahresbericht 2008, S. 47 und 48, 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 und 59).

Zum Begriff der Erforderlichkeit der Verarbeitung im Sinne von Art. 7 Buchst. e der Richtlinie 95/46 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 der Richtlinie 95/46, 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 erforderlich ansehen (Rn. 52, 66 und 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 bis 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 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 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 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 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 und 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 handelt. Der Gerichtshof hat daher entschieden, dass Art. 7 Buchst. f der Richtlinie 95/46 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 und 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 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 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 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 bis 64 und 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 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 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 Slovenskej republiky (Oberstes Gericht der Slowakischen Republik) 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 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 aufgestellten Bedingungen für die Rechtmäßigkeit der betreffenden Verarbeitung personenbezogener Daten erfüllt sind (Rn. 117 und 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 und 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 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).

Urteil vom 11. November 2020, Orange România (C-61/19, EU:C:2020:901)

Die Orange România SA bietet Mobiltelekommunikationsdienste auf dem rumänischen Markt an. Am 28. März 2018 verhängte die Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Nationale Behörde zur Überwachung der Verarbeitung personenbezogener Daten, Rumänien) gegen Orange România eine Geldbuße, weil sie Kopien der Ausweisdokumente ihrer Kunden ohne deren ausdrückliche Einwilligung aufbewahrt hatte.

Nach den Angaben dieser Behörde hatte Orange România im Zeitraum vom 1. März 2018 bis zum 26. März 2018 Verträge über Mobiltelekommunikationsdienste geschlossen, die die Klausel enthielten, dass die Kunden informiert wurden und in die Sammlung und Aufbewahrung einer Kopie ihres Ausweisdokuments mit Identifikationsfunktion einwilligten. Das diese Klausel betreffende Kästchen wurde vom für die Verarbeitung Verantwortlichen vor Unterzeichnung des Vertrags angekreuzt.

Vor diesem Hintergrund ersuchte das Tribunalul București (Landgericht Bukarest, Rumänien) den Gerichtshof, klarzustellen, unter welchen Voraussetzungen die Einwilligung von Kunden in die Verarbeitung personenbezogener Daten als gültig angesehen werden kann.

Der Gerichtshof hat zunächst darauf hingewiesen, dass das Unionsrecht[31] eine abschließende Aufzählung der Fälle vorsieht, in denen die Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann. Konkret muss die Einwilligung der betreffenden Person freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich erfolgen[32]. Die Einwilligung wird bei Stillschweigen, bereits angekreuzten Kästchen oder Untätigkeit nicht gültig erteilt (Rn. 34, 36, 37 und 39).

Zudem muss, wenn die Einwilligung der betroffenen Person durch eine schriftliche Erklärung erfolgt, die noch andere Sachverhalte betrifft, diese Erklärung in verständlicher und leicht zugänglicher Form zur Verfügung gestellt werden und in einer klaren und einfachen Sprache formuliert sein. Zur Sicherstellung einer echten Wahlfreiheit für die betroffene Person dürfen die Vertragsbestimmungen diese nicht über die Möglichkeit irreführen, den Vertrag abschließen zu können, auch wenn sie sich weigert, in die Verarbeitung ihrer Daten einzuwilligen (Rn. 34, 36, 37, 39 und 41).

Der Gerichtshof hat erläutert, dass Orange România, da sie die für die Verarbeitung personenbezogener Daten Verantwortliche ist, in der Lage sein muss, die Rechtmäßigkeit der Verarbeitung dieser Daten nachzuweisen, in diesem Fall also das Vorliegen einer gültigen Einwilligung ihrer Kunden. Da die betroffenen Kunden das Kästchen in Bezug auf die Sammlung und die Aufbewahrung von Kopien ihres Ausweisdokuments anscheinend nicht selbst angekreuzt haben, ist der bloße Umstand, dass dieses Kästchen angekreuzt wurde, nicht geeignet, eine positive Einwilligungserklärung dieser Kunden nachzuweisen. Es ist Sache des nationalen Gerichts, die dafür erforderlichen Feststellungen zu treffen (Rn. 42 und 46).

Es ist ebenfalls Sache des nationalen Gerichts, zu prüfen, ob die in Rede stehenden Vertragsbestimmungen die betroffenen Kunden mangels näherer Angaben zu der Möglichkeit, den Vertrag trotz der Weigerung, in die Verarbeitung ihrer Daten einzuwilligen, abzuschließen, hinsichtlich dieses Punkts irreführen konnten. Der Gerichtshof hat darauf hingewiesen, dass Orange România für den Fall, dass ein Kunde die Einwilligung in die Verarbeitung seiner Daten verweigert hat, verlangt hat, dass dieser schriftlich erklärt, weder in die Sammlung noch in die Aufbewahrung der Kopie seines Ausweisdokuments einzuwilligen. Nach Ansicht des Gerichtshofs ist eine solche zusätzliche Anforderung geeignet, die freie Entscheidung, sich dieser Sammlung und Aufbewahrung zu widersetzen, ungebührlich zu beeinträchtigen. Da es jedenfalls Orange România obliegt, nachzuweisen, dass ihre Kunden ihre Einwilligung in die Verarbeitung ihrer personenbezogenen Daten durch aktives Verhalten bekundet haben, kann sie nicht von ihnen verlangen, dass sie ihre Weigerung aktiv bekunden (Rn. 49 bis 51).

Der Gerichtshof ist daher zu dem Ergebnis gelangt, dass ein Vertrag über die Erbringung von Telekommunikationsdiensten, der die Klausel enthält, dass die betroffene Person über die Sammlung und die Aufbewahrung einer Kopie ihres Ausweisdokuments mit Identifikationsfunktion informiert worden ist und darin eingewilligt hat, nicht als Nachweis dafür geeignet ist, dass diese Person ihre Einwilligung in die Sammlung und Aufbewahrung dieser Dokumente gültig erteilt hat, wenn das Kästchen, das sich auf diese Klausel bezieht, von dem für die Verarbeitung der Daten Verantwortlichen vor Unterzeichnung dieses Vertrags angekreuzt

---

31 Art. 7 der Richtlinie 95/46 und Art. 6 DSGVO.
32 Art. 2 Buchst. h der Richtlinie 95/46 und Art. 4 Nr. 11 DSGVO.

worden ist, wenn die Vertragsbestimmungen dieses Vertrags die betroffene Person über die Möglichkeit, den Vertrag abzuschließen, auch wenn sie sich weigert, in die Verarbeitung ihrer Daten einzuwilligen, irreführen können oder wenn die freie Entscheidung, sich dieser Sammlung und Aufbewahrung zu widersetzen, von diesem Verantwortlichen ungebührlich beeinträchtigt wird, indem verlangt wird, dass die betroffene Person zur Verweigerung ihrer Einwilligung ein zusätzliches Formular unterzeichnet, in dem diese Weigerung zum Ausdruck kommt (Rn. 52 und Tenor).

Urteil vom 12. Mai 2021 (Große Kammer), Bundesrepublik Deutschland (Red Notice, Interpol) (C-505/19, EU:C:2021:376)

2012 gab die Internationale Kriminalpolizeiliche Organisation (Interpol) auf Antrag der Vereinigten Staaten eine WS betreffende Red Notice heraus. WS besitzt die deutsche Staatsangehörigkeit. Er sollte gegebenenfalls ausgeliefert werden. Grundlage der Red Notice war ein von den Behörden der Vereinigten Staaten ausgestellter Haftbefehl. Wird festgestellt, dass sich eine Person, die Gegenstand einer solchen Red Notice ist, in einem Mitgliedstaat von Interpol aufhält, muss dieser sie grundsätzlich vorläufig festnehmen oder ihre Bewegungen überwachen oder einschränken.

Noch vor der Herausgabe der WS betreffenden Red Notice war nach den Angaben des vorlegenden Gerichts gegen diese Person in Deutschland aber wegen derselben Taten, auf die sich die Red Notice bezieht, ein Ermittlungsverfahren eingeleitet worden. Dieses Verfahren wurde 2010 gegen Erfüllung einer Geldauflage rechtskräftig eingestellt. Dabei wurde von einer im deutschen Strafrecht vorgesehenen besonderen Möglichkeit der einvernehmlichen Verfahrensbeendigung Gebrauch gemacht. In der Folge teilte das Bundeskriminalamt (Deutschland) Interpol mit, dass es davon ausgehe, dass wegen dieses vorausgegangenen Verfahrens im vorliegenden Fall das Verbot der Doppelbestrafung greife. Nach diesem sowohl in Art. 54 des Übereinkommens zur Durchführung des Übereinkommens von Schengen[33] als auch in Art. 50 der Charta verankerten Grundsatz darf eine Person, die bereits rechtskräftig abgeurteilt worden ist, nicht noch einmal wegen derselben Tat verfolgt werden.

WS erhob 2017 beim Verwaltungsgericht Wiesbaden (Deutschland) Klage gegen Deutschland. Er beantragte, Deutschland zu verurteilen, alle geeigneten Maßnahmen zur Löschung der ihn betreffenden Red Notice zu ergreifen. Neben einem Verstoß gegen das Doppelbestrafungsverbot machte er eine Verletzung seines in Art. 21 AEUV garantierten Rechts auf Freizügigkeit geltend. Er könne sich nicht in einen Vertragsstaat des Übereinkommens von Schengen oder einen Mitgliedstaat begeben, ohne Gefahr zu laufen, festgenommen zu werden. Ferner trug er vor, dass die Verarbeitung der ihn betreffenden personenbezogenen Daten, die in der Red Notice enthalten seien, wegen dieser Verstöße gegen die Richtlinie 2016/680 zum

[33] Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen (ABl. 2000, L 239, S. 19) (im Folgenden: SDÜ).

Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in Strafsachen[34] verstoße.

Vor diesem Hintergrund beschloss das Verwaltungsgericht Wiesbaden, dem Gerichtshof Fragen zur Anwendung des Verbots der Doppelbestrafung vorzulegen, insbesondere zur Möglichkeit der vorläufigen Festnahme einer Person, die Gegenstand einer Red Notice ist, in einem Fall wie dem im Ausgangsverfahren in Rede stehenden. Darüber hinaus wollte das vorlegende Gericht wissen, welche Folgen sich daraus für die Verarbeitung der in einer Red Notice enthaltenen personenbezogenen Daten durch die Mitgliedstaaten ergeben.

Mit seinem Urteil hat der Gerichtshof (Große Kammer) u. a. entschieden, dass die Vorschriften der Richtlinie 2016/680 in Verbindung mit Art. 54 SDÜ und Art. 50 der Charta dahin auszulegen sind, dass sie der Verarbeitung der in einer von Interpol herausgegebenen Red Notice enthaltenen personenbezogenen Daten nicht entgegenstehen, solange nicht mit einer solchen gerichtlichen Entscheidung festgestellt worden ist, dass das Verbot der Doppelbestrafung bei den Taten, auf die sich die betreffende Red Notice bezieht, greift, und sofern die Verarbeitung der Daten die Voraussetzungen gemäß der Richtlinie 2016/680 erfüllt (Rn. 121 und Tenor 2).

Zu der Frage betreffend die personenbezogenen Daten, die in einer von Interpol herausgegebenen Red Notice enthalten sind, hat der Gerichtshof festgestellt, dass jeder Vorgang im Zusammenhang mit diesen Daten, wie etwa die Speicherung in den Fahndungsdatenbanken eines Mitgliedstaats, eine „Verarbeitung" darstellt, die unter die Richtlinie 2016/680[35] fällt. Mit einer solchen Verarbeitung wird ein rechtmäßiger Zweck verfolgt. Sie kann nicht allein deshalb als rechtswidrig angesehen werden, weil bei den Taten, auf die sich die Red Notice bezieht, das Verbot der Doppelbestrafung zum Tragen kommen könnte[36]. Die Verarbeitung solcher Daten durch die Behörden der Mitgliedstaaten kann sich im Übrigen gerade als unerlässlich erweisen, um zu überprüfen, ob das Verbot der Doppelbestrafung greift (Rn. 111, 114, 116, 117 und 119).

Der Gerichtshof ist deshalb zu dem Schluss gelangt, dass die Richtlinie 2016/680 in Verbindung mit Art. 54 SDÜ und Art. 50 der Charta der Verarbeitung der in einer von Interpol herausgegebenen Red Notice enthaltenen personenbezogenen Daten nicht entgegensteht, solange nicht mit einer rechtskräftigen gerichtlichen Entscheidung festgestellt worden ist, dass das Verbot der Doppelbestrafung in dem betreffenden Fall greift. Die Verarbeitung der betreffenden Daten muss jedoch die Voraussetzungen gemäß der Richtlinie 2016/680 erfüllen. Sie muss u. a. für die Erfüllung einer Aufgabe erforderlich sein, die von der zuständigen Behörde zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung wahrgenommen wird[37] (Rn. 121 und Tenor 2).

---

[34] 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. 2016, L 119, S. 89).

[35] Vgl. Art. 2 Abs. 1 und Art. 3 Nr. 2 der Richtlinie 2016/680.

[36] Vgl. Art. 4 Abs. 1 Buchst. b und Art. 8 Abs. 1 der Richtlinie 2016/680.

[37] Vgl. Art. 1 Abs. 1 und Art. 8 Abs. 1 der Richtlinie 2016/680.

Greift jedoch das Verbot der Doppelbestrafung, ist die Speicherung der in einer von Interpol herausgegebenen Red Notice enthaltenen personenbezogenen Daten in den Fahndungsdatenbanken der Mitgliedstaaten nicht mehr erforderlich, da die betreffende Person wegen der Taten, auf die sich die Red Notice bezieht, nicht mehr verfolgt und damit auch nicht mehr festgenommen werden darf. Folglich muss die betroffene Person die Löschung der sie betreffenden Daten verlangen können. Werden diese trotzdem weiter gespeichert, müssen sie mit dem Hinweis versehen werden, dass die betreffende Person in einem Vertragsstaat des Übereinkommens von Schengen oder einem Mitgliedstaat aufgrund des Verbots der Doppelbestrafung wegen derselben Taten nicht mehr verfolgt werden darf (Rn. 120).

Urteil vom 22. Juni 2021 (Große Kammer), Latvijas Republikas Saeima (Strafpunkte) (C-439/19, EU:C:2021:504)

In diesem Urteil (siehe auch Abschnitt II.3. „Begriff ‚Verarbeitung personenbezogener Daten'") hat der Gerichtshof entschieden, dass die DSGVO der lettischen Regelung entgegensteht, die die Ceļu satiksmes drošības direkcija (Direktion für Straßenverkehrssicherheit, Lettland) (im Folgenden: CSDD) verpflichtet, die Daten über Strafpunkte, die gegen Fahrzeugführer wegen Verkehrsverstößen verhängt wurden, der Öffentlichkeit zugänglich zu machen, ohne dass die Person, die den Zugang beantragt, ein besonderes Interesse am Erhalt dieser Daten nachzuweisen hat. Seiner Ansicht nach ist die Erforderlichkeit einer Übermittlung personenbezogener Daten über die für Verkehrsverstöße verhängten Strafpunkte insbesondere im Hinblick auf das von der lettischen Regierung geltend gemachte Ziel der Verbesserung der Straßenverkehrssicherheit nicht nachgewiesen. Weder das Recht der Öffentlichkeit auf Zugang zu amtlichen Dokumenten noch das Recht auf Informationsfreiheit rechtfertigen eine solche Regelung (Rn. 113, 120 bis 122 und Tenor 2).

In diesem Zusammenhang hat der Gerichtshof hervorgehoben, dass das mit der lettischen Regelung verfolgte Ziel der Verbesserung der Straßenverkehrssicherheit ein von der Union anerkanntes Ziel im allgemeinen Interesse darstellt und dass die Mitgliedstaaten somit die Straßenverkehrssicherheit als „Aufgabe …, die im öffentlichen Interesse liegt"[38], einstufen können. Allerdings ist nicht nachgewiesen, dass die lettische Regelung der Übermittlung personenbezogener Daten über Strafpunkte zur Gewährleistung des verfolgten Ziels erforderlich ist. Zum einen verfügt der lettische Gesetzgeber nämlich über eine Vielzahl von Handlungsmöglichkeiten, die es ihm ermöglicht hätten, dieses Ziel mit anderen Mitteln zu erreichen, die weniger in die Grundrechte der betroffenen Personen eingreifen. Zum anderen sind die Sensibilität der Daten über Strafpunkte und der Umstand zu berücksichtigen, dass ihre Übermittlung an die Öffentlichkeit einen schweren Eingriff in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen kann, da sie zu einer Missbilligung durch die Gesellschaft und zur Stigmatisierung der betroffenen Person führen kann (Rn. 109 bis 113).

Nach Ansicht des Gerichtshofs gehen diese beiden Grundrechte angesichts der Schwere des Eingriffs in diese Rechte sowohl dem Interesse der Öffentlichkeit am Zugang zu amtlichen

[38] Nach Art. 6 Abs. 1 Buchst. e DSGVO ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn sie „für die Wahrnehmung einer Aufgabe erforderlich [ist], die im öffentlichen Interesse liegt".

Dokumenten, wie dem nationalen Register für Fahrzeuge und Fahrzeugführer, als auch dem Recht auf Informationsfreiheit vor (Rn. 120 und 121).

Ferner hat der Gerichtshof aus denselben Gründen entschieden, dass die DSGVO der lettischen Regelung auch insoweit entgegensteht, als sie es der CSDD erlaubt, Daten über Strafpunkte, die gegen Fahrzeugführer wegen Verkehrsverstößen verhängt wurden, an Wirtschaftsteilnehmer zu übermitteln, damit diese sie weiterverwenden und an die Öffentlichkeit übermitteln können (Rn. 126 und Tenor 3).

Schließlich hat der Gerichtshof klargestellt, dass der Grundsatz des Vorrangs des Unionrechts es dem vorlegenden Gericht, das mit einem Rechtsbehelf gegen die lettische Regelung befasst ist, die vom Gerichtshof als unionsrechtswidrig eingestuft worden ist, verwehrt, die Rechtswirkungen dieser Regelung bis zum Zeitpunkt der Verkündung seines endgültigen Urteils aufrechtzuerhalten (Rn. 137 und Tenor 4).

III. Verarbeitung personenbezogener Daten im Sinne der Richtlinie 2002/58

Urteil vom 2. Oktober 2018 (Große Kammer), Ministerio Fiscal (C-207/16, EU:C:2018:788)[39]

Im Ausgangsrechtsstreit ging es um die Weigerung eines spanischen Ermittlungsrichters, einem im Rahmen von Ermittlungen wegen des Raubs einer Brieftasche und eines Mobiltelefons von der Kriminalpolizei gestellten Antrag stattzugeben, ihr Zugang zu Identifikationsdaten der Nutzer der Telefonnummern zu gewähren, die in einem Zeitraum von zwölf Tagen ab dem Tatzeitpunkt mit dem entwendeten Mobiltelefon aktiviert wurden. Der Antrag wurde mit der Begründung abgelehnt, dass der den strafrechtlichen Ermittlungen zugrunde liegende Sachverhalt keine „schwere" – d. h. eine nach spanischem Recht mit einer Freiheitsstrafe von mehr als fünf Jahren bedrohte – Straftat darstelle und der Zugang zu diesen Identifikationsdaten nur bei dieser Art von Straftaten möglich sei.

Der Gerichtshof hat zunächst darauf hingewiesen, dass der Zugang von Behörden zu von den Betreibern elektronischer Kommunikationsdienste gespeicherten Daten im Rahmen eines strafrechtlichen Ermittlungsverfahrens in den Geltungsbereich der Richtlinie 2002/58 fällt. Darüber hinaus stellt der Zugang zu den Daten, anhand deren die Inhaber der SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, identifiziert werden sollen, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in der Charta verankerte Grundrechte auf Achtung des Privatlebens und auf Datenschutz dar, auch wenn keine Umstände vorliegen, aufgrund deren dieser Eingriff als „schwer" eingestuft werden kann, und ohne dass es darauf ankommt, ob die betroffenen Informationen über das Privatleben als sensibel anzusehen sind oder die Betroffenen durch diesen Eingriff irgendwelche Nachteile erlitten haben. Der Gerichtshof hat jedoch festgestellt, dass dieser Eingriff nicht so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und

[39] Dieses Urteil wurde im Jahresbericht 2018, S. 91 und 92, dargestellt.

Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste. Denn die Richtlinie 2002/58 zählt zwar die Zwecke, die eine nationale Regelung, die den Zugang von Behörden zu diesen Daten betrifft und damit vom Grundsatz der Vertraulichkeit der elektronischen Kommunikation abweicht, rechtfertigen können, abschließend auf, so dass dieser Zugang tatsächlich strikt einem dieser Zwecke dienen muss. Der Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten ist nach dem Wortlaut der Richtlinie jedoch nicht auf die Bekämpfung schwerer Straftaten beschränkt, sondern betrifft „Straftaten" im Allgemeinen (Rn. 38, 42, 59 bis 63 und Tenor).

In diesem Zusammenhang hat der Gerichtshof erläutert, dass er im Urteil *Tele2 Sverige und Watson u. a.*[40] zwar entschieden hatte, dass allein die Bekämpfung der schweren Kriminalität einen Zugang der Behörden zu von den Betreibern von Kommunikationsdiensten gespeicherten personenbezogenen Daten rechtfertigen kann, aus deren Gesamtheit genaue Schlüsse auf das Privatleben der Personen gezogen werden können, deren Daten betroffen sind. Diese Auslegung war jedoch damit begründet worden, dass der mit einer solchen Zugangsregelung verfolgte Zweck im Verhältnis zur Schwere des damit einhergehenden Eingriffs in die betroffenen Grundrechte stehen muss. Nach dem Grundsatz der Verhältnismäßigkeit kann nämlich ein schwerer Eingriff in diesem Bereich nur durch den Zweck der Bekämpfung einer ebenfalls als „schwer" einzustufenden Kriminalität gerechtfertigt werden. Ist der Eingriff dagegen nicht schwer, kann dieser Zugang durch den Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von „Straftaten" im Allgemeinen gerechtfertigt werden (Rn. 54 bis 57).

In dem betreffenden Fall hat der Gerichtshof die Auffassung vertreten, dass der Zugang nur zu den Daten, auf die sich der im Ausgangsverfahren fragliche Antrag bezieht, nicht als „schwerer" Eingriff in die Grundrechte der Personen, deren Daten betroffen sind, eingestuft werden kann, da sich aus diesen Daten keine genauen Schlüsse auf ihr Privatleben ziehen lassen. Der Gerichtshof schließt daraus, dass der Eingriff, den ein Zugang zu solchen Daten mit sich bringen würde, mithin durch den Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von „Straftaten" im Allgemeinen gerechtfertigt sein kann, ohne dass es erforderlich wäre, dass diese Straftaten als „schwer" einzustufen sind (Rn. 61 und 62).

Urteile vom 6. Oktober 2020 (Große Kammer), Privacy International (C-623/17, EU:C:2020:790) und La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791)[41]

Die Rechtsprechung zur Vorratsspeicherung von und zum Zugang zu personenbezogenen Daten im Bereich elektronischer Kommunikationen, speziell das Urteil Tele2 Sverige und Watson u. a., in dem der Gerichtshof insbesondere ausgeführt hat, dass die Mitgliedstaaten den Betreibern elektronischer Kommunikationsdienste keine Pflicht zur allgemeinen und unterschiedslosen Speicherung von Verkehrs- und Standortdaten auferlegen dürfen, löste bei einigen Staaten die Besorgnis aus, eines Instruments beraubt worden zu sein, das sie zum Schutz der nationalen Sicherheit und zur Bekämpfung der Kriminalität für erforderlich halten.

---

40 Urteil des Gerichtshofs vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970).

41 Diese Urteile wurden im Jahresbericht 2020, S. 30 bis 33, dargestellt.

Vor diesem Hintergrund wurden das Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse, Vereinigtes Königreich) (Privacy International, C-623/17), der Conseil d'État (Staatsrat, Frankreich) (La Quadrature du Net u. a., verbundene Rechtssachen C-511/18 und C-512/18) sowie die Cour constitutionnelle (Verfassungsgerichtshof, Belgien) (Ordre des barreaux francophones et germanophone u. a., C-520/18) mit Rechtsstreitigkeiten befasst, bei denen es um die Rechtmäßigkeit von Regelungen einiger Mitgliedstaaten in diesen Bereichen ging, die insbesondere vorsehen, dass die Betreiber elektronischer Kommunikationsdienste die Verkehrs- und Standortdaten ihrer Nutzer einer öffentlichen Stelle übermitteln oder allgemein und unterschiedslos auf Vorrat speichern müssen.

Mit zwei Urteilen hat der Gerichtshof (Große Kammer) am 6. Oktober 2020 zunächst entschieden, dass die Richtlinie 2002/58 auf nationale Regelungen Anwendung findet, mit denen den Betreibern elektronischer Kommunikationsdienste zum Schutz der nationalen Sicherheit und zur Bekämpfung der Kriminalität Verarbeitungen personenbezogener Daten wie ihre Übermittlung an öffentliche Stellen oder ihre Vorratsspeicherung vorgeschrieben werden (Rn. 49 und Tenor 1 des Urteils Privacy International und Rn. 104 des Urteils La Quadrature du Net u. a.).

Sodann hat der Gerichtshof darauf hingewiesen, dass die Richtlinie 2002/58[42] es nicht gestattet, dass die Ausnahme von der grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Daten und insbesondere von dem Verbot, solche Daten zu speichern, zur Regel wird. Dies impliziert, dass die Richtlinie den Mitgliedstaaten den Erlass von Rechtsvorschriften, die die in ihr enthaltenen Rechte und Pflichten und insbesondere die Pflicht, die Vertraulichkeit der übertragenen Nachrichten und der damit verbundenen Verkehrsdaten sicherzustellen[43], beschränken sollen, nur dann gestattet, wenn sie die allgemeinen Grundsätze des Unionsrechts, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und die durch die Charta garantierten Grundrechte[44] beachten (Rn. 59 und 60 des Urteils Privacy International und Rn. 111 und 113 des Urteils La Quadrature du Net u. a.).

In diesem Rahmen hat der Gerichtshof zum einen in der Rechtssache Privacy International ausgeführt, dass die Richtlinie 2002/58 im Licht der Charta einer nationalen Regelung entgegensteht, mit der den Betreibern elektronischer Kommunikationsdienste zum Schutz der nationalen Sicherheit auferlegt wird, Verkehrs- und Standortdaten allgemein und unterschiedslos den Sicherheits- und Nachrichtendiensten zu übermitteln. Zum anderen hat er in den verbundenen Rechtssachen La Quadrature du Net u. a. sowie in der Rechtssache Ordre des barreaux francophones et germanophone u. a. festgestellt, dass die Richtlinie Rechtsvorschriften entgegensteht, mit denen den Betreibern elektronischer Kommunikationsdienste präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird.

Diese Pflichten zur allgemeinen und unterschiedslosen Vorratsspeicherung stellen nämlich besonders schwerwiegende Eingriffe in die durch die Charta garantierten Grundrechte dar,

---

42 Art. 15 Abs. 1 und 3 der Richtlinie 2002/58.

43 Art. 5 Abs. 1 der Richtlinie 2002/58.

44 Insbesondere Art. 7, 8 und 11 sowie Art. 52 Abs. 1 der Charta.

ohne dass zwischen dem Verhalten der Personen, deren Daten betroffen sind, und dem mit der fraglichen Regelung verfolgten Ziel eine Verbindung besteht. Analog dazu hat der Gerichtshof Art. 23 Abs. 1 DSGVO im Licht der Charta ausgelegt, dass er einer nationalen Regelung entgegensteht, mit der den Anbietern eines öffentlichen Online-Zugangs zu Kommunikationsdiensten und den Betreibern von Hosting-Diensten eine allgemeine und unterschiedslose Vorratsspeicherung insbesondere von personenbezogenen Daten im Zusammenhang mit diesen Diensten auferlegt wird (Rn. 71, 82 und Tenor 2 des Urteils Privacy International und Rn. 146, 168, 174, 177, 212, Tenor 1 und 3 des Urteils La Quadrature du Net u. a.).

Dagegen ist der Gerichtshof zu dem Ergebnis gelangt, dass die Richtlinie 2002/58 es im Licht der Charta gestattet, den Betreibern elektronischer Kommunikationsdienste eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten aufzuerlegen, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht. In diesem Kontext hat der Gerichtshof klargestellt, dass diese Anordnung, die nur für einen auf das absolut Notwendige begrenzten Zeitraum ergehen darf, Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein muss, deren Entscheidung bindend ist. Unter den gleichen Voraussetzungen steht die Richtlinie auch einer automatisierten Analyse insbesondere der Verkehrs- und Standortdaten aller Nutzer elektronischer Kommunikationsmittel nicht entgegen (Rn. 137 bis 139, 177 bis 179, Tenor 1 und 2 des Urteils La Quadrature du Net u. a.).

Der Gerichtshof hat weiter ausgeführt, dass die Richtlinie 2002/58 im Licht der Charta Rechtsvorschriften nicht entgegensteht, die auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten gestatten. Desgleichen steht die Richtlinie weder Rechtsvorschriften entgegen, die für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen, noch Rechtsvorschriften, die eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen, wobei die Mitgliedstaaten im letztgenannten Fall die Speicherung nicht zeitlich begrenzen müssen. Überdies steht die Richtlinie Rechtsvorschriften nicht entgegen, die es gestatten, den Betreibern von Diensten aufzuerlegen, ihnen zur Verfügung stehende Daten umgehend zu sichern, falls Situationen auftreten, die es erforderlich machen, die betreffenden Daten zur Aufklärung schwerer Straftaten oder von Beeinträchtigungen der nationalen Sicherheit über die gesetzlichen Fristen hinaus zu speichern, sofern die Taten oder Beeinträchtigungen bereits festgestellt wurden oder der begründete Verdacht besteht, dass sie vorliegen (Rn. 161, 163, 168 und Tenor 1 des Urteils La Quadrature du Net u. a.).

Darüber hinaus hat der Gerichtshof festgestellt, dass die Richtlinie 2002/58 im Licht der Charta einer nationalen Regelung nicht entgegensteht, mit der den Betreibern elektronischer Kommunikationsdienste auferlegt wird, insbesondere Verkehrs- und Standortdaten in Echtzeit zu erheben, sofern sich dies auf Personen beschränkt, bei denen ein triftiger Grund für den Verdacht besteht, dass sie auf irgendeine Weise in terroristische Aktivitäten verwickelt sind, und

einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegt, deren Entscheidung bindend ist, wobei dieses Gericht oder diese Stelle sich vergewissern muss, dass eine solche Erhebung in Echtzeit nur in den Grenzen des absolut Notwendigen gestattet wird. In Eilfällen muss die Kontrolle kurzfristig erfolgen (Rn. 192 und Tenor 2 des Urteils La Quadrature du Net u. a.).

Schließlich ist der Gerichtshof auf die Frage eingegangen, ob es zulässig ist, die Wirkungen einer als unvereinbar mit dem Unionsrecht eingestuften nationalen Regelung vorübergehend aufrechtzuerhalten. Dazu hat er ausgeführt, dass ein nationales Gericht eine Bestimmung seines nationalen Rechts nicht anwenden darf, die es ermächtigt, die ihm obliegende Feststellung, dass eine nationale Regelung, mit der den Betreibern elektronischer Kommunikationsdienste eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird, wegen ihrer Unvereinbarkeit mit der Richtlinie 2002/58 im Licht der Charta rechtswidrig ist, in ihren zeitlichen Wirkungen zu beschränken.

Um dem vorlegenden Gericht eine sachgerechte Antwort zu geben, hat der Gerichtshof darauf hingewiesen, dass es beim gegenwärtigen Stand des Unionsrechts allein Sache des nationalen Rechts ist, die Zulässigkeit und die Würdigung der durch eine unionsrechtswidrige Vorratsdatenspeicherung erlangten Beweise im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, schwere Straftaten begangen zu haben, zu regeln. Die Richtlinie 2002/58 verlangt jedoch bei einer Auslegung im Licht des Effektivitätsgrundsatzes, dass ein nationales Strafgericht Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines solchen Strafverfahrens ausschließt, wenn die Personen, die im Verdacht stehen, Straftaten begangen zu haben, nicht in der Lage sind, sachgerecht zu diesen Beweisen Stellung zu nehmen (Rn. 222, 228 und Tenor 4 des Urteils La Quadrature du Net u. a.).

Urteil vom 2. März 2021 (Große Kammer), Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152)

Gegen H. K. wurde in Estland ein Strafverfahren wegen Diebstahls, Verwendung der Bankkarte eines Dritten und Gewalttaten gegenüber Beteiligten an einem Gerichtsverfahren durchgeführt. Von einem erstinstanzlichen Gericht wurde sie wegen dieser Taten zu einer Freiheitsstrafe von zwei Jahren verurteilt. Diese Entscheidung wurde in der Berufungsinstanz bestätigt. Die Protokolle, auf die sich die Verurteilung wegen dieser Straftaten stützt, wurden u. a. anhand personenbezogener Daten erstellt, die im Rahmen der Erbringung elektronischer Kommunikationsdienste erhoben worden waren. Der Riigikohus (Oberster Gerichtshof, Estland), bei dem eine Kassationsbeschwerde von H. K. anhängig war, hegte Zweifel an der Vereinbarkeit der Voraussetzungen, unter denen die ermittelnden Dienststellen Zugang zu diesen Daten hatten, mit dem Unionsrecht[45].

Diese Zweifel betrafen erstens die Frage, ob die Länge des Zeitraums, in dem die ermittelnden Dienststellen Zugang zu den Daten hatten, ein Kriterium darstellt, anhand dessen sich beurteilen lässt, wie schwer dieser Zugang in die Grundrechte der Betroffenen eingreift. Das

[45] Genauer gesagt mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta.

vorlegende Gericht wollte wissen, ob das Ziel der Bekämpfung der Kriminalität im Allgemeinen und nicht nur der Bekämpfung schwerer Kriminalität einen solchen Eingriff rechtfertigen kann, wenn dieser Zeitraum sehr kurz oder die Menge der gesammelten Daten sehr begrenzt ist. Zweitens hatte das vorlegende Gericht Zweifel, ob die estnische Staatsanwaltschaft in Anbetracht der verschiedenen Aufgaben, die ihr nach nationalem Recht übertragen wurden, als „unabhängige" Verwaltungsbehörde im Sinne des Urteils Tele2 Sverige und Watson u. a.[46] angesehen werden kann, die befugt ist, den Zugang der Ermittlungsbehörde zu den betreffenden Daten zu genehmigen.

Mit seinem Urteil hat der Gerichtshof (Große Kammer) entschieden, dass die Richtlinie 2002/58 im Licht der Charta einer nationalen Regelung entgegensteht, die es Behörden zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten ermöglicht, Zugang zu Verkehrs- oder Standortdaten zu erlangen, die geeignet sind, Informationen über die von einem Nutzer eines elektronischen Kommunikationsmittels getätigten Kommunikationen oder über den Standort der von ihm verwendeten Endgeräte zu liefern und genaue Schlüsse auf sein Privatleben zuzulassen, ohne dass sich dieser Zugang auf Verfahren zur Bekämpfung schwerer Kriminalität oder zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit beschränken würde. Dies gilt unabhängig davon, für welchen Zeitraum der Zugang zu den betreffenden Daten begehrt wird und welche Menge oder Art von Daten für einen solchen Zeitraum verfügbar ist. Außerdem steht die Richtlinie im Licht der Charta einer nationalen Regelung entgegen, wonach die Staatsanwaltschaft dafür zuständig ist, einer Behörde für strafrechtliche Ermittlungen Zugang zu Verkehrs- und Standortdaten zu gewähren (Rn. 45, 59, Tenor 1 und 2).

Zu dem mit der fraglichen Regelung verfolgten Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten hat der Gerichtshof ausgeführt, dass im Einklang mit dem Grundsatz der Verhältnismäßigkeit nur die Bekämpfung schwerer Kriminalität oder die Verhütung ernster Bedrohungen der öffentlichen Sicherheit geeignet ist, den Zugang der Behörden zu einem Satz von Verkehrs- oder Standortdaten zu rechtfertigen, aus denen genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden können, ohne dass andere die Verhältnismäßigkeit eines Zugangsantrags betreffende Faktoren wie die Länge des Zeitraums, für den der Zugang zu solchen Daten begehrt wird, dazu führen können, dass das Ziel, Straftaten im Allgemeinen zu verhüten, zu ermitteln, festzustellen und zu verfolgen, einen solchen Zugang zu rechtfertigen vermag (Rn. 33 und 35).

Hinsichtlich der Befugnis der Staatsanwaltschaft, einer Behörde für strafrechtliche Ermittlungen Zugang zu Verkehrs- und Standortdaten zu gewähren, hat der Gerichtshof darauf hingewiesen, dass im nationalen Recht die Voraussetzungen festzulegen sind, unter denen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den Daten gewähren müssen, über die sie verfügen. Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss eine solche Regelung jedoch klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, damit die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken ermöglichen. Die Regelung muss nach innerstaatlichem Recht bindend sein und Angaben dazu enthalten, unter

[46] Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, Rn. 120).

welchen Umständen und unter welchen materiellen und prozeduralen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, um zu gewährleisten, dass sich der Eingriff auf das absolut Notwendige beschränkt (Rn. 48).

Um in der Praxis die vollständige Einhaltung dieser Voraussetzungen zu gewährleisten, ist es unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und dass dessen oder deren Entscheidung auf einen mit Gründen versehenen, von diesen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellten Antrag ergeht. In hinreichend begründeten Eilfällen muss die Kontrolle kurzfristig erfolgen (Rn. 51).

Die vorherige Kontrolle setzt u. a. voraus, dass das mit ihr betraute Gericht oder die mit ihr betraute Stelle über alle Befugnisse verfügt und alle Garantien aufweist, die erforderlich sind, um zu gewährleisten, dass die verschiedenen einander gegenüberstehenden Interessen und Rechte in Einklang gebracht werden. Im Fall strafrechtlicher Ermittlungen verlangt eine solche Kontrolle, dass dieses Gericht oder diese Stelle in der Lage ist, für einen gerechten Ausgleich zwischen den Interessen, die sich aus den Erfordernissen der Ermittlungen im Rahmen der Kriminalitätsbekämpfung ergeben, und den Grundrechten auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten der Personen, auf deren Daten zugegriffen wird, zu sorgen. Wird die Kontrolle nicht von einem Gericht, sondern von einer unabhängigen Verwaltungsstelle wahrgenommen, muss diese über eine Stellung verfügen, die es ihr erlaubt, bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorzugehen, ohne jede Einflussnahme von außen (Rn. 52 und 53).

Daraus folgt, dass das Erfordernis, wonach die mit der Wahrnehmung der vorherigen Kontrolle betraute Behörde unabhängig sein muss, es gebietet, dass es sich bei ihr um eine andere als die den Zugang zu den Daten begehrende Stelle handelt, damit Erstere in der Lage ist, diese Kontrolle objektiv und unparteiisch, ohne jede Einflussnahme von außen, auszuüben. Im strafrechtlichen Bereich impliziert das Erfordernis der Unabhängigkeit insbesondere, dass die mit der vorherigen Kontrolle betraute Behörde zum einen nicht an der Durchführung des fraglichen Ermittlungsverfahrens beteiligt ist und zum anderen eine Position der Neutralität gegenüber den Beteiligten am Strafverfahren hat. Bei einer Staatsanwaltschaft, die wie die estnische Staatsanwaltschaft das Ermittlungsverfahren leitet und gegebenenfalls die öffentliche Klage vertritt, ist dies nicht der Fall. Folglich ist die Staatsanwaltschaft nicht in der Lage, eine solche vorherige Kontrolle wahrzunehmen (Rn. 54, 55 und 57).

IV. Übermittlung personenbezogener Daten in Drittländer

Urteil vom 6. November 2003 (Große Kammer), Lindqvist (C-101/01, EU:C:2003:596)[47]

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 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 und Tenor 4).

Denn angesichts des Entwicklungsstands des Internets zur Zeit der Ausarbeitung der Richtlinie 95/46 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 und 68).

Urteil vom 6. Oktober 2015 (Große Kammer), Schrems (C-362/14, EU:C:2015:650)[48]

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[49] festgestellt habe, dass die Vereinigten Staaten im Rahmen der Safe-Harbor-Regelung[50] hinsichtlich der übermittelten personenbezogenen Daten ein angemessenes Schutzniveau gewährleisteten.

---

47 Dieses Urteil wurde im Jahresbericht 2003, S. 80 und 81, dargestellt.

48 Dieses Urteil wurde im Jahresbericht 2015, S. 54 und 55, dargestellt.

49 Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates 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. 2000, L 215, S. 7).

50 Die Safe-Harbour-Regelung enthält eine Reihe von Grundsätzen über den Schutz personenbezogener Daten, denen sich amerikanische Unternehmen freiwillig unterwerfen können.

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, 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 erlassenen Entscheidung 2000/520 befasst.

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 jedoch nicht getan hat, verstößt deren Art. 1 gegen die in Art. 25 Abs. 6 der Richtlinie 95/46 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 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 bis 89, 96 bis 98 und Tenor 2).

Der Gerichtshof hat auch Art. 3 der Entscheidung 2000/520 für ungültig erklärt, da sie den nationalen Datenschutzbehörden die Befugnisse entzieht, die ihnen nach Art. 28 der Richtlinie 95/46 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 bis 104). Der Gerichtshof hat festgestellt, dass die Ungültigkeit der Art. 1 und 3 der Entscheidung 2000/520 die Gültigkeit der gesamten Entscheidung berührt (Rn. 105 und 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 und 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 und 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 und 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 bis 207 und 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 und 224).

Urteil vom 16. Juli 2020 (Große Kammer), Facebook Ireland und Schrems (C–311/18, EU:C:2020:559)[51]

Die DSGVO bestimmt, dass personenbezogene Daten grundsätzlich nur dann in ein Drittland übermittelt werden dürfen, wenn das betreffende Land für die Daten ein angemessenes Schutzniveau gewährleistet. Nach dieser Verordnung kann die Kommission feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder seiner internationalen Verpflichtungen ein angemessenes Schutzniveau gewährleistet[52]. Liegt kein derartiger Angemessenheitsbeschluss vor, darf eine solche Übermittlung nur erfolgen, wenn der in der Union ansässige Exporteur der personenbezogenen Daten geeignete Garantien vorsieht, die sich u. a. aus von der Kommission erlassenen Standarddatenschutzklauseln ergeben können, und wenn die betroffenen Personen über durchsetzbare Rechte und wirksame Rechtsbehelfe verfügen[53]. Ferner ist in der DSGVO genau geregelt, unter welchen Voraussetzungen eine solche Übermittlung vorgenommen werden darf, falls weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen[54].

Herr Maximillian Schrems, ein in Österreich wohnhafter österreichischer Staatsangehöriger, ist seit 2008 Nutzer von Facebook. Wie bei allen anderen im Unionsgebiet wohnhaften Nutzern werden seine personenbezogenen Daten ganz oder teilweise von Facebook Ireland an Server der Facebook Inc., die sich in den Vereinigten Staaten befinden, übermittelt und dort verarbeitet. Herr Schrems legte bei der irischen Aufsichtsbehörde eine Beschwerde ein, die im

---

51 Dieses Urteil wurde im Jahresbericht 2020, S. 27 bis 30, dargestellt.
52 Art. 45 DSGVO.
53 Art. 46 Abs. 1 und 2 Buchst. c DSGVO.
54 Art. 49 DSGVO.

Wesentlichen darauf abzielte, diese Übermittlungen verbieten zu lassen. Er machte geltend, das Recht und die Praxis der Vereinigten Staaten böten keinen ausreichenden Schutz vor dem Zugriff der Behörden auf die dorthin übermittelten Daten. Seine Beschwerde wurde u. a. mit der Begründung zurückgewiesen, die Kommission habe in ihrer Entscheidung 2000/520[55] festgestellt, dass die Vereinigten Staaten ein angemessenes Schutzniveau gewährleisteten. Mit Urteil vom 6. Oktober 2015 erklärte der Gerichtshof auf ein Vorabentscheidungsersuchen des High Court (Hoher Gerichtshof, Irland) hin diese Entscheidung für ungültig (im Folgenden: Urteil Schrems I)[56] (Rn. 52 und 53).

Nachdem das Urteil Schrems I ergangen war und das irische Gericht daraufhin die Entscheidung, mit der die Beschwerde von Herrn Schrems zurückgewiesen worden war, aufgehoben hatte, forderte die irische Aufsichtsbehörde Herrn Schrems auf, seine Beschwerde unter Berücksichtigung der Ungültigerklärung der Entscheidung 2000/520 durch den Gerichtshof umzuformulieren. Mit seiner umformulierten Beschwerde macht Herr Schrems geltend, dass die Vereinigten Staaten keinen ausreichenden Schutz der dorthin übermittelten Daten gewährleisteten. Er beantragt, die von Facebook Ireland nunmehr auf der Grundlage der Standardschutzklauseln im Anhang des Beschlusses 2010/87/EU[57] vorgenommene Übermittlung seiner personenbezogenen Daten aus der Union in die Vereinigten Staaten für die Zukunft auszusetzen oder zu verbieten. Die irische Aufsichtsbehörde war der Auffassung, dass die Bearbeitung der Beschwerde von Herrn Schrems insbesondere von der Gültigkeit des Beschlusses 2010/87 abhänge, und strengte daher ein Verfahren vor dem High Court an, damit er den Gerichtshof mit einem Vorabentscheidungsersuchen befassen möge. Nachdem dieses Verfahren eingeleitet worden war, erließ die Kommission den Beschluss (EU) 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild („Privacy Shield“) gebotenen Schutzes[58] (Rn. 54, 55 und 57).

Mit seinem Vorabentscheidungsersuchen fragt das vorlegende Gericht den Gerichtshof nach der Anwendbarkeit der DSGVO auf Übermittlungen personenbezogener Daten, die auf die Standardschutzklauseln im Beschluss 2010/87 gestützt werden, sowie nach dem Schutzniveau, das diese Verordnung im Rahmen einer solchen Übermittlung verlangt, und den Pflichten, die den Aufsichtsbehörden in diesem Zusammenhang obliegen. Des Weiteren wirft der High Court die Frage der Gültigkeit sowohl des Beschlusses 2010/87 als auch des Beschlusses 2016/1250 auf.

Der Gerichtshof stellt fest, dass die Prüfung des Beschlusses 2010/87 anhand der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) nichts ergeben hat, was seine Gültigkeit berühren könnte. Den Beschluss 2016/1250 erklärt er hingegen für ungültig (Tenor 4 und 5).

Der Gerichtshof führt zunächst aus, dass das Unionsrecht, insbesondere die DSGVO, auf eine

---

55 Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates 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. 2000, L 215, S. 7).

56 Urteil des Gerichtshofs vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650 (vgl. auch Pressemitteilung Nr. 117/15).

57 Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (ABl. 2010, L 39, S. 5) in der Fassung des Durchführungsbeschlusses (EU) 2016/2297 der Kommission vom 16. Dezember 2016 (ABl. 2016, L 344, S. 100).

58 Durchführungsbeschluss der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (ABl. 2016 207, S. 1).

zu gewerblichen Zwecken erfolgende Übermittlung personenbezogener Daten durch einen in einem Mitgliedstaat ansässigen Wirtschaftsteilnehmer an einen anderen, in einem Drittland ansässigen Wirtschaftsteilnehmer Anwendung findet, auch wenn die Daten bei ihrer Übermittlung oder im Anschluss daran von den Behörden des betreffenden Drittlands für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates verarbeitet werden können. Eine derartige Datenverarbeitung durch die Behörden eines Drittlands kann nicht dazu führen, dass eine solche Übermittlung vom Anwendungsbereich der DSGVO ausgenommen wäre (Rn. 86, 88, 89 und Tenor 1).

In Bezug auf das im Rahmen einer solchen Übermittlung erforderliche Schutzniveau entscheidet der Gerichtshof, dass die insoweit in der DSGVO vorgesehenen Anforderungen, die sich auf geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe beziehen, dahin auszulegen sind, dass die Personen, deren personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden, ein Schutzniveau genießen müssen, das dem in der Union durch die DSGVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist. Bei der Beurteilung dieses Schutzniveaus sind sowohl die vertraglichen Regelungen zu berücksichtigen, die zwischen dem in der Union ansässigen Datenexporteur und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, als auch, was einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten Daten betrifft, die maßgeblichen Elemente der Rechtsordnung dieses Landes (Rn. 105 und Tenor 2).

Hinsichtlich der Pflichten, die den Aufsichtsbehörden im Zusammenhang mit einer solchen Übermittlung obliegen, befindet der Gerichtshof, dass diese Behörden, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, insbesondere verpflichtet sind, eine Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn sie im Licht der Umstände dieser Übermittlung der Auffassung sind, dass die Standarddatenschutzklauseln in diesem Land nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann, es sei denn, der in der Union ansässige Datenexporteur hat die Übermittlung selbst ausgesetzt oder beendet (Rn. 121 und Tenor 3).

Sodann prüft der Gerichtshof die Gültigkeit des Beschlusses 2010/87. Er sieht sie nicht schon dadurch in Frage gestellt, dass die in diesem Beschluss enthaltenen Standarddatenschutzklauseln aufgrund ihres Vertragscharakters die Behörden des Drittlands, in das möglicherweise Daten übermittelt werden, nicht binden. Vielmehr hängt sie davon ab, ob der Beschluss wirksame Mechanismen enthält, die in der Praxis gewährleisten können, dass das vom Unionsrecht verlangte Schutzniveau eingehalten wird und dass auf solche Klauseln gestützte Übermittlungen personenbezogener Daten ausgesetzt oder verboten werden, wenn gegen diese Klauseln verstoßen wird oder ihre Einhaltung unmöglich ist. Der Gerichtshof stellt fest, dass der Beschluss 2010/87 derartige Mechanismen vorsieht. Insoweit hebt er insbesondere hervor, dass gemäß diesem Beschluss der Datenexporteur und der Empfänger der Übermittlung vorab prüfen müssen, ob das erforderliche Schutzniveau im betreffenden Drittland eingehalten wird, und dass der Empfänger dem Datenexporteur gegebenenfalls mitteilen muss, dass er die Standardschutzklauseln nicht einhalten kann, woraufhin der Exporteur die Datenübermittlung aussetzen und/oder vom Vertrag mit dem Empfänger zurücktreten muss (Rn. 132, 136, 137, 142, 148 und Tenor 4).

Schließlich prüft der Gerichtshof die Gültigkeit des Beschlusses 2016/1250 anhand der Anforderungen der DSGVO im Licht der Bestimmungen der Charta, die die Achtung des Privat- und Familienlebens, den Schutz personenbezogener Daten und das Recht auf effektiven gerichtlichen Rechtsschutz verbürgen. Insoweit stellt er fest, dass in diesem Beschluss, ebenso wie in der Entscheidung 2000/520, den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts Vorrang eingeräumt wird, was Eingriffe in die Grundrechte der Personen ermöglicht, deren Daten in die Vereinigten Staaten übermittelt werden. Er kommt zu dem Ergebnis, dass die von der Kommission im Beschluss 2016/1250 bewerteten Einschränkungen des Schutzes personenbezogener Daten, die sich daraus ergeben, dass die amerikanischen Behörden nach dem Recht der Vereinigten Staaten auf solche Daten, die aus der Union in dieses Drittland übermittelt werden, zugreifen und sie verwenden dürfen, nicht dergestalt geregelt sind, dass damit Anforderungen erfüllt würden, die den im Unionsrecht nach dem Grundsatz der Verhältnismäßigkeit bestehenden Anforderungen der Sache nach gleichwertig wären, da die auf die amerikanischen Rechtsvorschriften gestützten Überwachungsprogramme nicht auf das zwingend erforderliche Maß beschränkt sind. Gestützt auf die Feststellungen in diesem Beschluss weist der Gerichtshof darauf hin, dass die betreffenden Vorschriften hinsichtlich bestimmter Überwachungsprogramme in keiner Weise erkennen lassen, dass für die darin enthaltene Ermächtigung zur Durchführung dieser Programme Einschränkungen bestehen; genauso wenig ist ersichtlich, dass für die potenziell von diesen Programmen erfassten Personen, die keine amerikanischen Staatsbürger sind, Garantien existieren. Der Gerichtshof fügt hinzu, dass diese Vorschriften zwar Anforderungen vorsehen, die von den amerikanischen Behörden bei der Durchführung der betreffenden Überwachungsprogramme einzuhalten sind, aber den betroffenen Personen keine Rechte verleihen, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können (Rn. 164, 165, 180 bis 182, 184 und 185).

In Bezug auf das Erfordernis des gerichtlichen Rechtsschutzes befindet der Gerichtshof, dass der im Beschluss 2016/1250 angeführte Ombudsmechanismus entgegen den darin von der Kommission getroffenen Feststellungen den betroffenen Personen keinen Rechtsweg zu einem Organ eröffnet, das Garantien böte, die den nach dem Unionsrecht erforderlichen Garantien der Sache nach gleichwertig wären, d. h. Garantien, die sowohl die Unabhängigkeit der durch diesen Mechanismus vorgesehenen Ombudsperson als auch das Bestehen von Normen gewährleisten, die die Ombudsperson dazu ermächtigen, gegenüber den amerikanischen Nachrichtendiensten verbindliche Entscheidungen zu erlassen. Aus all diesen Gründen erklärt der Gerichtshof den Beschluss 2016/1250 für ungültig (Rn. 195 bis 197, 201 und Tenor 5).

V. 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 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 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 und 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 und 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 und 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)[59]

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 (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")[60], 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft[61], 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums[62] und 2002/58 es den Mitgliedstaaten nicht gebieten, in einer Situation wie

---

59 Dieses Urteil wurde im Jahresbericht 2008, S. 48 und 49, dargestellt.

60 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. 2000, L 178, S. 1).

61 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. 2001, L 167, S. 10).

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

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).

Urteil vom 24. November 2011, Scarlet Extended (C-70/10, EU:C:2011:771)[63]

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 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, 2000/31, 2001/29, 2002/58 und 2004/48 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 festgelegten Verbot, einem solchen Provider allgemeine Überwachungspflichten aufzuerlegen, noch dem Erfordernis, ein angemessenes Gleichgewicht zwischen dem Schutz des Rechts des

[63] Dieses Urteil wurde im Jahresbericht 2011, S. 38 und 39, dargestellt.

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 und 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).

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 und 2004/48.

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 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 in Verbindung mit Art. 15 Abs. 1 der Richtlinie 2002/58 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 und 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 und 2004/48 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).

Urteil vom 17. Juni 2021, M.I.C.M. (C-597/19, EU:C:2021:492)

Das Unternehmen Mircom International Content Management & Consulting (M.I.C.M.) Limited (im Folgenden: Mircom) hatte bei der Ondernemingsrechtbank Antwerpen (Unternehmensgericht Antwerpen, Belgien, im Folgenden: vorlegendes Gericht) einen Auskunftsantrag gegen die Telenet BVBA, einen Internetzugangsanbieter, gestellt. Dieser Antrag war auf eine Entscheidung gerichtet, mit der Telenet verpflichtet wurde, die Daten zur Identifizierung ihrer Kunden auf der Grundlage der von einem spezialisierten Unternehmen im Auftrag von Mircom erhobenen IP-Adressen vorzulegen. Die Internetanschlüsse von Kunden von

Telenet waren dazu genutzt worden, in einem Peer-to-Peer-Netz über das BitTorrent-Protokoll Filme aus dem Repertoire von Mircom zu teilen. Telenet trat dem Antrag von Mircom entgegen.

Vor diesem Hintergrund stellte das vorlegende Gericht dem Gerichtshof erstens die Frage, ob das Teilen von Segmenten einer Mediendatei, die ein geschütztes Werk enthält, in einem Peer-to-Peer-Netz eine öffentliche Wiedergabe nach dem Unionsrecht darstellt. Zweitens wollte es wissen, ob einem Inhaber von Rechten des geistigen Eigentums wie Mircom, der sie nicht nutzt, sondern von mutmaßlichen Verletzern Schadensersatz verlangt, die im Unionsrecht vorgesehenen Maßnahmen, Verfahren und Rechtsbehelfe offenstehen, um die Durchsetzung dieser Rechte zu gewährleisten, z. B. durch die Einholung von Informationen. Drittens ersuchte das vorlegende Gericht den Gerichtshof um Klärung der Frage, ob die Art und Weise, in der die IP-Adressen der Kunden durch Mircom gesammelt werden, und die Übermittlung der von Mircom bei Telenet angefragten Daten zulässig sind.

Der Gerichtshof hat entschieden, dass das Unionsrecht[64] grundsätzlich weder den Inhaber von Rechten des geistigen Eigentums oder einen in dessen Auftrag handelnden Dritten daran hindert, IP-Adressen von Nutzern von Peer-to-Peer-Netzen, deren Internetanschlüsse für rechtsverletzende Tätigkeiten genutzt worden sein sollen, systematisch zu speichern (vorgelagerte Datenverarbeitung), noch dem entgegensteht, dass die Namen und Anschriften der Nutzer an den Rechtsinhaber oder an einen Dritten im Hinblick auf eine Schadensersatzklage übermittelt werden (nachgelagerte Datenverarbeitung). Die dahin gehenden Maßnahmen und Anträge müssen jedoch gerechtfertigt, verhältnismäßig, nicht missbräuchlich und in einer nationalen Rechtsvorschrift vorgesehen sein, die die Rechte und Pflichten aus dem Unionsrecht beschränkt. Der Gerichtshof hat klargestellt, dass das Unionsrecht keine Verpflichtung für eine Gesellschaft wie Telenet begründet, personenbezogene Daten an Privatpersonen zu übermitteln, damit diese vor den Zivilgerichten Urheberrechtsverstöße verfolgen können. Das Unionsrecht erlaubt es den Mitgliedstaaten jedoch, eine solche Verpflichtung vorzusehen (Rn. 97, 125 bis 127 und Tenor 3).

3. Auslistung personenbezogener Daten

Urteil vom 24. September 2019 (Große Kammer), GC u. a. (Auslistung sensibler Daten) (C-136/17, EU:C:2019:773)[65]

Mit diesem Urteil hat die Große Kammer des Gerichtshofs die Pflichten des Betreibers einer Suchmaschine im Zusammenhang mit einem Antrag auf Auslistung sensibler Daten konkretisiert.

Google hatte sich geweigert, den Anträgen von vier Personen stattzugeben, die darauf gerichtet waren, verschiedene Links zu Websites Dritter, u. a. Presseartikeln, aus der Ergebnisliste zu entfernen, die von der Suchmaschine im Anschluss an eine Suche anhand des Namens der Personen angezeigt wird. Auf die Beschwerden dieser vier Personen lehnte die Commission nationale de l'informatique et des libertés (CNIL, Nationaler Ausschuss für Informatik und

64 Art. 6 Abs. 1 Buchst. f DSGVO und Art. 15 Abs. 1 der Richtlinie 2002/58.
65 Dieses Urteil wurde im Jahresbericht 2019, S. 119 bis 121, dargestellt.

Freiheitsrechte, Frankreich) es ab, Google aufzufordern, die beantragten Auslistungen vorzunehmen. Der mit der Sache befasste Conseil d'État (Staatsrat, Frankreich) hat den Gerichtshof ersucht, die Pflichten des Betreibers einer Suchmaschine bei der Bearbeitung eines Auslistungsantrags gemäß der Richtlinie 95/46 zu konkretisieren.

Der Gerichtshof hat erstens darauf hingewiesen, dass die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben – vorbehaltlich bestimmter Abweichungen und Ausnahmen – verboten ist[66]. Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, darf grundsätzlich nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen[67] (Rn. 39 und 40).

Das Verbot und die Beschränkungen der Verarbeitung besonderer Kategorien personenbezogener Daten gelten für den Suchmaschinenbetreiber ebenso wie für jeden anderen für die Verarbeitung personenbezogener Daten Verantwortlichen. Zweck dieser Verbote und Beschränkungen ist es nämlich, einen erhöhten Schutz gegen solche Verarbeitungen zu gewährleisten, die aufgrund der besonderen Sensibilität der Daten einen besonders schweren Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen können (Rn. 42 bis 44).

Der Suchmaschinenbetreiber ist jedoch nicht dafür verantwortlich, dass personenbezogene Daten auf der Website eines Dritten vorhanden sind, wohl aber für die Aufnahme dieser Website in die Ergebnisliste. Daher gelten das Verbot und die Beschränkungen der Verarbeitung personenbezogener Daten für diesen Betreiber nur aufgrund dieser Aufnahme und somit über eine Prüfung, die auf der Grundlage eines Antrags der betroffenen Person unter der Aufsicht der zuständigen nationalen Behörden vorzunehmen ist (Rn. 46 und 47).

Der Gerichtshof hat zweitens festgestellt, dass der Suchmaschinenbetreiber, wenn er mit einem Antrag auf Auslistung sensibler Daten befasst ist, vorbehaltlich bestimmter Ausnahmen grundsätzlich verpflichtet ist, diesem Antrag stattzugeben. Was diese Ausnahmen betrifft, kann der Suchmaschinenbetreiber einen solchen Antrag insbesondere dann ablehnen, wenn er feststellt, dass die Links zu Daten führen, die die betroffene Person offenkundig öffentlich gemacht hat[68], sofern die Aufnahme der Links in die Ergebnisliste die weiteren Voraussetzungen für die Zulässigkeit einer Verarbeitung personenbezogener Daten erfüllt und die betroffene Person nicht das Recht hat, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die Aufnahme Widerspruch zu erheben[69] (Rn. 65 und 69).

In jedem Fall muss der Suchmaschinenbetreiber, wenn er mit einem Auslistungsantrag befasst ist, prüfen, ob sich die Aufnahme des Links zu einer Webseite, auf der sensible Daten veröffentlicht sind, in die Ergebnisliste, die im Anschluss an eine Suche nach dem Namen der betroffenen Person angezeigt wird, als unbedingt erforderlich erweist, um die

66 Art. 8 Abs. 1 der Richtlinie 95/46 und Art. 9 Abs. 1 der Verordnung 2016/679.
67 Art. 8 Abs. 5 der Richtlinie 95/46 und Art. 10 der Verordnung 2016/679.
68 Art. 8 Abs. 2 Buchst. e der Richtlinie 95/46 und Art. 9 Abs. 2 Buchst. e der Verordnung 2016/679
69 Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 und Art. 21 Abs. 1 der Richtlinie 2016/679.

Informationsfreiheit der Internetnutzer zu schützen, die potenziell daran interessiert sind, mittels einer solchen Suche Zugang zu dieser Website zu erhalten. Zwar überwiegen die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten im Allgemeinen gegenüber der Informationsfreiheit der Internetnutzer; der Ausgleich kann in besonders gelagerten Fällen aber von der Art der betreffenden Information, von deren Sensibilität für das Privatleben der betroffenen Person und vom Interesse der Öffentlichkeit am Zugang zu der Information abhängen, das u. a. je nach der Rolle, die diese Person im öffentlichen Leben spielt, variieren kann (Rn. 66 und 68).

Der Gerichtshof hat drittens entschieden, dass es Sache des Suchmaschinenbetreibers ist, im Rahmen eines Antrags auf Auslistung von Daten zu einem Strafverfahren gegen die betroffene Person, die sich auf einen früheren Verfahrensabschnitt beziehen und nicht mehr der aktuellen Situation entsprechen, zu beurteilen, ob diese Person unter Berücksichtigung sämtlicher Umstände des Einzelfalls ein Recht darauf hat, dass die betreffenden Informationen aktuell nicht mehr durch die Anzeige einer Ergebnisliste im Anschluss an eine Suche anhand ihres Namens mit ihrem Namen in Verbindung gebracht werden. Selbst wenn dies nicht der Fall ist, weil sich die Einbeziehung des betreffenden Links als absolut erforderlich erweist, um die Rechte der betroffenen Person auf Achtung des Privatlebens und auf Schutz ihrer Daten mit der Informationsfreiheit potenziell interessierter Internetnutzer in Einklang zu bringen, ist der Suchmaschinenbetreiber verpflichtet, spätestens anlässlich des Auslistungsantrags die Ergebnisliste so auszugestalten, dass das daraus für den Internetnutzer entstehende Gesamtbild die aktuelle Rechtslage widerspiegelt, was insbesondere voraussetzt, dass Links zu Websites mit entsprechenden Informationen auf dieser Liste an erster Stelle stehen (Rn. 77 und 78).

Urteil vom 24. September 2019 (Große Kammer), Google (Räumliche Reichweite der Auslistung) (C-507/17, EU:C:2019:772)[70]

Die Commission nationale de l'informatique et des libertés (CNIL, Nationaler Ausschuss für Informatik und Freiheitsrechte, Frankreich) forderte Google auf, in Fällen, in denen diese einem Auslistungsantrag stattgibt, aus der Ergebnisliste, die im Anschluss an eine Suche anhand des Namens der betroffenen Person angezeigt wird, Links, die auf Websites mit personenbezogenen Daten dieser Person führen, auf sämtlichen Domains ihrer Suchmaschine zu entfernen. Nachdem Google sich geweigert hatte, dieser Aufforderung nachzukommen, verhängte die CNIL eine Sanktion von 100 000 Euro gegen dieses Unternehmen. Der von Google angerufene Conseil d'État (Staatsrat) hat den Gerichtshof ersucht, die räumliche Reichweite der Verpflichtung des Suchmaschinenbetreibers, das Auslistungsrecht in Anwendung der Richtlinie 95/46 umzusetzen, zu konkretisieren.

Der Gerichtshof hat zunächst darauf hingewiesen, dass natürliche Personen auf der Grundlage des Unionsrechts ihr Auslistungsrecht gegenüber dem Suchmaschinenbetreiber geltend machen können, der eine oder mehrere Niederlassungen im Gebiet der Union besitzt, unabhängig davon, ob die Verarbeitung personenbezogener Daten (im vorliegenden Fall die Aufnahme von Links zu Websites, auf denen sich personenbezogene Daten der Person

[70] Dieses Urteil wurde im Jahresbericht 2019, S. 121 und 122, dargestellt.

befinden, die sich auf dieses Recht beruft, in die Ergebnisliste) in oder außerhalb der Union stattfindet[71].

Zur Reichweite des Auslistungsrechts hat der Gerichtshof festgestellt, dass der Suchmaschinenbetreiber die Auslistung nicht in allen Versionen seiner Suchmaschine vorzunehmen hat, sondern nur in den mitgliedstaatlichen Versionen. Zwar kann unter Berücksichtigung der Merkmale des Internets und von Suchmaschinen mit einer weltweiten Auslistung das Ziel des Unionsgesetzgebers, ein hohes Schutzniveau für personenbezogene Daten in der gesamten Union sicherzustellen, vollständig erreicht werden, doch ergibt sich aus dem Unionsrecht[72] nicht, dass der Gesetzgeber zur Erreichung eines solchen Ziels entschieden hätte, dem Auslistungsrecht eine Reichweite zu verleihen, die über das Hoheitsgebiet der Mitgliedstaaten hinausgeht. Während das Unionsrecht Mechanismen für die Zusammenarbeit zwischen Aufsichtsbehörden der Mitgliedstaaten zur Verfügung stellt, um eine gemeinsame Entscheidung zu treffen, die auf einer Abwägung zwischen dem Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten einerseits und dem öffentlichen Interesse der verschiedenen Mitgliedstaaten am Zugang zu einer Information andererseits beruht, sind solche Mechanismen im Hinblick auf die Reichweite einer Auslistung über die Union hinaus derzeit nicht vorgesehen (Rn. 62 und 73).

Nach dem derzeitigen Stand des Unionsrechts hat der Suchmaschinenbetreiber die beantragte Auslistung nicht nur in der Version der Suchmaschine für den Wohnsitzmitgliedstaat desjenigen, der die Auslistung verlangen kann, sondern auch in den mitgliedstaatlichen Versionen der Suchmaschine vorzunehmen, und dies u. a. mit dem Ziel, ein gleichmäßiges und hohes Datenschutzniveau in der gesamten Union zu gewährleisten. Darüber hinaus obliegt es einem Suchmaschinenbetreiber, erforderlichenfalls hinreichend wirksame Maßnahmen zu ergreifen, um Internetnutzer in der Union daran zu hindern oder zumindest ernsthaft davon abzuhalten, gegebenenfalls über eine Version der Suchmaschine für einen Drittstaat auf die von der Auslistung erfassten Links zuzugreifen. Es ist Sache des nationalen Gerichts, zu prüfen, ob die vom Suchmaschinenbetreiber getroffenen Maßnahmen diese Anforderung erfüllen (Rn. 70).

Schließlich hat der Gerichtshof darauf hingewiesen, dass das Unionsrecht den Suchmaschinenbetreiber zwar nicht verpflichtet, die Auslistung in allen Versionen seiner Suchmaschine vorzunehmen, dies aber auch nicht verbietet. Daher bleibt eine Aufsichts- oder Justizbehörde eines Mitgliedstaats befugt, anhand von nationalen Schutzstandards für die Grundrechte eine Abwägung zwischen dem Recht der betroffenen Person auf Achtung ihres Privatlebens und auf Schutz ihrer personenbezogenen Daten einerseits und dem Recht auf freie Information andererseits vorzunehmen und nach erfolgter Abwägung gegebenenfalls dem Suchmaschinenbetreiber aufzugeben, eine Auslistung in allen Versionen seiner Suchmaschine vorzunehmen (Rn. 65 und 72).

---

71 Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 und Art. 3 Abs. 1 der Verordnung 2016/679.

72 Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 und Art. 17 Abs. 1 der Verordnung 2016/679.

4. Einwilligung des Nutzers einer Website in die Speicherung von Informationen

Urteil vom 1. Oktober 2019 (Große Kammer), Planet49 (C-673/17, EU:C:2019:801)[73]

Mit diesem Urteil hat der Gerichtshof entschieden, dass keine wirksame Einwilligung vorliegt, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies durch ein mit einem voreingestellten Häkchen versehenes Ankreuzkästchen erlaubt wird, und zwar unabhängig davon, ob es sich bei den betreffenden Informationen um personenbezogene Daten handelt oder nicht. Der Gerichtshof hat ferner klargestellt, dass der Diensteanbieter dem Nutzer mitteilen muss, welche Funktionsdauer die Cookies haben und ob Dritte Zugriff auf sie erhalten können.

Im Ausgangsrechtsstreit geht es um ein Gewinnspiel, das von Planet49 über die Website www.dein-macbook.de zu Werbezwecken veranstaltet wurde. Teilnahmewillige Internetnutzer mussten auf einer Seite mit Ankreuzkästchen ihren Namen und ihre Adresse eingeben. Das Ankreuzkästchen, mit dem das Setzen von Cookies erlaubt wurde, war mit einem voreingestellten Häkchen versehen. Der Bundesgerichtshof (Deutschland), bei dem eine Klage des deutschen Bundesverbands der Verbraucherverbände anhängig war, hatte Zweifel hinsichtlich der Wirksamkeit der mittels des mit einem voreingestellten Häkchen versehenen Ankreuzkästchens erlangten Einwilligung der Nutzer und hinsichtlich des Umfangs der Informationspflicht des Diensteanbieters.

Das Vorabentscheidungsersuchen betraf im Wesentlichen die Auslegung des Begriffs der Einwilligung im Sinne der Richtlinie 2002/58[74] in Verbindung mit der Richtlinie 95/46[75] und der DSGVO[76].

Der Gerichtshof hat erstens festgestellt, dass der Ausdruck „Einwilligung der betroffenen Person“ nach Art. 2 Buchst. h der Richtlinie 95/46, auf die Art. 2 Buchst. f der Richtlinie 2002/58 verweist, „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden“, bezeichnet. Das Erfordernis einer „Willensbekundung“ der betroffenen Person deutet klar auf ein aktives und nicht passives Verhalten hin. Eine Einwilligung, die durch ein voreingestelltes Ankreuzkästchen erteilt wird, impliziert aber kein aktives Verhalten des Nutzers einer Website. Die Entstehungsgeschichte von Art. 5 Abs. 3 der Richtlinie 2002/58, der nach der Änderung durch die Richtlinie 2009/136 vorsieht, dass der Nutzer „seine Einwilligung“ in die Speicherung von Cookies „gegeben“ hat, deutet darauf hin, dass die Einwilligung des Nutzers nun nicht mehr vermutet werden darf und sich aus einem aktiven Verhalten des Nutzers ergeben muss. Außerdem sieht die DSGVO[77] nunmehr

---

73 Dieses Urteil wurde im Jahresbericht 2019, S. 122 und 123, dargestellt.

74 Art. 2 Buchst. f und Art. 5 Abs. 3 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung.

75 Art. 2 Buchst. h der Richtlinie 95/46.

76 Art. 6 Abs. 1 Buchst. a der Verordnung 2016/679.

77 Ebd.

ausdrücklich eine aktive Einwilligung vor. Ihr Art. 4 Nr. 11 verlangt eine Willensbekundung etwa in Form „einer sonstigen eindeutigen bestätigenden Handlung". Und in ihrem 32. Erwägungsgrund wird ausdrücklich ausgeschlossen, dass „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit" eine Einwilligung darstellen können (Rn. 49, 52, 56 und 62).

Der Gerichtshof ist deshalb zu dem Schluss gelangt, dass keine wirksame Einwilligung vorliegt, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss, und dass die Tatsache, dass der Nutzer der Website die Schaltfläche für die Teilnahme an dem betreffenden Gewinnspiel betätigt, nicht ausreicht, um von einer wirksamen Einwilligung des Nutzers zur Speicherung von Cookies auszugehen (Rn. 63).

Zweitens hat der Gerichtshof festgestellt, dass Art. 5 Abs. 3 der Richtlinie 2002/58 den Nutzer vor jedem Eingriff in seine Privatsphäre schützen soll, unabhängig davon, ob dabei personenbezogene Daten oder andere Daten betroffen sind. Der Begriff der Einwilligung ist daher nicht unterschiedlich auszulegen, je nachdem, ob es sich bei den im Endgerät des Nutzers einer Website gespeicherten oder abgerufenen Informationen um personenbezogene Daten handelt oder nicht (Rn. 69 und 71).

Drittens hat der Gerichtshof festgestellt, dass Art. 5 Abs. 3 der Richtlinie 2002/58 verlangt, dass der Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Die klaren und umfassenden Informationen müssen den Nutzer in die Lage versetzen, die Konsequenzen einer etwaigen von ihm erteilten Einwilligung leicht zu ermitteln, und gewährleisten, dass die Einwilligung in voller Kenntnis der Sachlage erteilt wird. Angaben zur Funktionsdauer der Cookies und dazu, ob Dritte Zugriff auf die Cookies erhalten können, zählen zu den klaren und umfassenden Informationen, die der Diensteanbieter dem Nutzer einer Website zu geben hat (Rn. 73 bis 75 und 81).

VI. Nationale Kontrollstellen

1. Tragweite des Unabhängigkeitserfordernisses

Urteil vom 9. März 2010 (Große Kammer), Kommission/Deutschland (C-518/07, EU:C:2010:125)[78]

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 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.

[78] Dieses Urteil wurde im Jahresbericht 2010, S. 35, dargestellt.

Die Bundesrepublik Deutschland war dagegen der Auffassung, dass Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 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 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 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 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 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 bis 43 und 52).

Der Gerichtshof hat erläutert, dass eine nationale Kontrollstelle nicht über eine eigene Haushaltslinie, wie sie Art. 43 Abs. 3 der Verordnung Nr. 45/2001 vorsieht, verfügen muss, um das Unabhängigkeitskriterium des Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 erfüllen zu können. Die Mitgliedstaaten sind nämlich nicht verpflichtet, in ihr innerstaatliches Recht ähnliche Vorschriften wie die des Kapitels V der Verordnung 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 wahrzunehmen (Rn. 58).

Urteil vom 8. April 2014 (Große Kammer), Kommission/Ungarn (C-288/12, EU:C:2014:237)[79]

In dieser Rechtssache hatte die Kommission beantragt, festzustellen, dass Ungarn dadurch gegen seine Verpflichtungen aus der Richtlinie 95/46 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 verstößt (Rn. 62 und 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

[79] Dieses Urteil wurde im Jahresbericht 2014, S. 64, dargestellt.

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 bis 55).

2. Bestimmung des anwendbaren Rechts und der zuständigen Kontrollstelle

Urteil vom 1. Oktober 2015, Weltimmo (C-230/14, EU:C:2015:639)[80]

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 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. Sie richtete daher mehrere Vorabentscheidungsfragen an den Gerichtshof.

Zum anwendbaren nationalen Recht hat der Gerichtshof festgestellt, dass Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 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

[80] Dieses Urteil wurde im Jahresbericht 2015, S. 55 und 56, dargestellt.

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 und Tenor 1).

Zur Zuständigkeit und zu den Befugnissen der mit Beschwerden befassten Kontrollstelle nach Art. 28 Abs. 4 der Richtlinie 95/46 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 und 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 IV „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 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 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 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 und 47).

Urteil vom 5. Juni 2018 (Große Kammer), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)

In diesem Urteil (vgl. auch Abschnitt II.5 „Begriff ‚für die Verarbeitung [personenbezogener Daten] Verantwortlicher'"), das u. a. die Auslegung der Art. 4 und 28 der Richtlinie 95/46 betrifft, hat sich der Gerichtshof zum Umfang der Einwirkungsbefugnisse der nationalen Kontrollstellen bei einer Verarbeitung personenbezogener Daten, an der mehrere Akteure beteiligt sind, geäußert.

Der Gerichtshof hat entschieden, dass dann, wenn ein außerhalb der Europäischen Union ansässiges Unternehmen (wie das amerikanische Unternehmen Facebook) mehrere Niederlassungen in verschiedenen Mitgliedstaaten unterhält, die Kontrollstelle eines Mitgliedstaats zur Ausübung der ihr durch Art. 28 Abs. 3 dieser Richtlinie übertragenen Befugnisse gegenüber einer im Hoheitsgebiet dieses Mitgliedstaats gelegenen Niederlassung dieses Unternehmens (hier Facebook Germany) auch dann befugt ist, wenn nach der konzerninternen Aufgabenverteilung zum einen diese Niederlassung allein für den Verkauf von Werbeflächen und sonstige Marketingtätigkeiten im Hoheitsgebiet dieses Mitgliedstaats zuständig ist und zum anderen die ausschließliche Verantwortung für die Erhebung und Verarbeitung personenbezogener Daten für das gesamte Gebiet der Europäischen Union einer in einem anderen Mitgliedstaat gelegenen Niederlassung (hier Facebook Ireland) obliegt (Rn. 64 und Tenor 2).

Der Gerichtshof hat weiter entschieden, dass die Kontrollstelle eines Mitgliedstaats, wenn sie beabsichtigt, gegenüber einer im Hoheitsgebiet dieses Mitgliedstaats ansässigen Stelle wegen Verstößen gegen die Vorschriften über den Schutz personenbezogener Daten, die von einem Dritten begangen wurden, der für die Verarbeitung dieser Daten verantwortlich ist und seinen Sitz in einem anderen Mitgliedstaat hat (hier Facebook Ireland), die Einwirkungsbefugnisse nach Art. 28 Abs. 3 der Richtlinie 95/46 auszuüben, zuständig ist, die Rechtmäßigkeit einer solchen Datenverarbeitung unabhängig von der Kontrollstelle des letztgenannten Mitgliedstaats (Irland) zu beurteilen und ihre Einwirkungsbefugnisse gegenüber der in ihrem Hoheitsgebiet ansässigen Stelle auszuüben, ohne zuvor die Kontrollstelle des anderen Mitgliedstaats um ein Eingreifen zu ersuchen (Rn. 74 und Tenor 3).

Urteil vom 15. Juni 2021 (Große Kammer), Facebook Ireland u. a. (C-645/19, EU:C:2021:483)

Am 11. September 2015 erhob der Präsident des belgischen Ausschusses für den Schutz des Privatlebens bei der Nederlandstalige rechtbank van eerste aanleg Brussel (niederländischsprachiges Gericht erster Instanz Brüssel, Belgien) eine Unterlassungsklage gegen Facebook Ireland, Facebook Inc. und Facebook Belgium mit dem Ziel, Verstöße gegen Datenschutzvorschriften, die Facebook begangen haben sollte, abzustellen. Diese Verstöße bestanden u. a. in der Sammlung und Nutzung von Informationen über das Surfverhalten von

belgischen Internetnutzern, von denen nicht alle über ein Facebook-Konto verfügen, mittels verschiedener Technologien wie Cookies, Social Plugins[81] oder Pixeln.

Am 16. Februar 2018 erklärte sich dieses Gericht für zuständig, über diese Klage zu befinden, und entschied in der Sache, dass das soziale Netzwerk Facebook die belgischen Internetnutzer nicht ausreichend über die Erhebung und Nutzung der betreffenden Informationen informiert habe. Im Übrigen wurde die Einwilligung der Internetnutzer zur Sammlung und Verarbeitung dieser Informationen als nicht wirksam angesehen.

Am 2. März 2018 legten Facebook Ireland, Facebook Inc. und Facebook Belgium gegen dieses Urteil Berufung beim Hof van beroep te Brussel (Berufungsgericht Brüssel, Belgien), dem vorlegenden Gericht in der vorliegenden Rechtssache, ein. Vor diesem Gericht trat die belgische Datenschutzbehörde (im Folgenden: GBA) als Rechtsnachfolgerin des Präsidenten der CBLP auf. Das vorlegende Gericht erklärte sich lediglich für die Entscheidung über die von Facebook Belgium eingelegte Berufung für zuständig.

Das vorlegende Gericht war sich nicht sicher, welche Auswirkung das in der DSGVO vorgesehene Verfahren der Zusammenarbeit und Kohärenz[82] auf die Befugnisse der GBA hat, und es warf insbesondere die Frage auf, ob die GBA in Bezug auf Sachverhalte nach dem 25. Mai 2018, ab dem die DSGVO gilt, gegen Facebook Belgium vorgehen kann, da Facebook Ireland als für die Verarbeitung der betreffenden Daten Verantwortlicher festgestellt worden ist. Seit diesem Zeitpunkt und insbesondere gemäß dem in der DSGVO vorgesehenen Verfahren der Zusammenarbeit und Kohärenz sei nämlich nur der irische Datenschutzbeauftragte befugt, unter der Kontrolle der irischen Gerichte eine Unterlassungsklage zu erheben (Rn. 36 und 37).

In seinem Urteil hat der Gerichtshof (Große Kammer) die Befugnisse der nationalen Aufsichtsbehörden im Rahmen der DSGVO präzisiert. Insbesondere hat er entschieden, dass die Verordnung unter bestimmten Voraussetzungen einer Aufsichtsbehörde eines Mitgliedstaats gestattet, von ihrer Befugnis Gebrauch zu machen, vermeintliche Verstöße gegen die DSGVO einem Gericht dieses Mitgliedstaats zur Kenntnis zu bringen und in Bezug auf eine grenzüberschreitende Datenverarbeitung[83] die Einleitung eines gerichtlichen Verfahrens zu betreiben, obgleich sie für diese Verarbeitung nicht die federführende Behörde ist (Tenor 1).

Erstens hat der Gerichtshof festgelegt, unter welchen Voraussetzungen eine nationale Aufsichtsbehörde, die hinsichtlich einer grenzüberschreitenden Verarbeitung nicht als federführende Behörde fungiert, ihre Befugnis auszuüben hat, vermeintliche Verstöße gegen die DSGV einem Gericht eines Mitgliedstaats zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben. So muss zum einen die DSGVO dieser Aufsichtsbehörde eine Zuständigkeit für den Erlass einer Entscheidung, mit der festgestellt wird, dass die fragliche Verarbeitung gegen die in dieser Verordnung vorgesehenen Regeln verstößt, verleihen, und zum anderen muss diese Befugnis unter Beachtung der in der DSGVO

---

81 Z. B. die Buttons „Gefällt mir“ oder „Teilen“.

82 „Unbeschadet des Artikels 55 ist die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters gemäß dem Verfahren nach Artikel 60 die zuständige federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung.“

83 Im Sinne von Art. 4 Nr. 23 DSGVO.

vorgesehenen Verfahren der Zusammenarbeit und Kohärenz ausgeübt werden[84] (Rn. 75 und Tenor 1).

Für grenzüberschreitende Verarbeitungen sieht die DSGVO nämlich ein Verfahren der Zusammenarbeit und Kohärenz[85] vor, das auf einer Zuständigkeitsverteilung zwischen einer „federführenden Aufsichtsbehörde" und den anderen betroffenen nationalen Aufsichtsbehörden beruht. Dieser Mechanismus erfordert eine enge, loyale und wirksame Zusammenarbeit zwischen den genannten Behörden, um zu gewährleisten, dass die Vorschriften über den Schutz personenbezogener Daten kohärent und einheitlich geschützt werden, und um somit die praktische Wirksamkeit dieses Mechanismus zu wahren. Die DSGVO sieht insoweit vor, dass grundsätzlich die federführende Aufsichtsbehörde dafür zuständig ist, einen Beschluss zu erlassen, mit dem festgestellt wird, dass eine grenzüberschreitende Verarbeitung gegen die Vorschriften der Verordnung verstößt[86], wohingegen die Zuständigkeit der anderen nationalen Aufsichtsbehörden für den Erlass eines solchen, wenn auch nur vorläufigen, Beschlusses die Ausnahme darstellt[87]. Indessen muss die federführende Aufsichtsbehörde bei der Wahrnehmung ihrer Zuständigkeiten insbesondere den gebotenen Dialog führen und loyal und wirksam mit den anderen betroffenen Aufsichtsbehörden zusammenarbeiten. Bei dieser Zusammenarbeit kann daher die federführende Aufsichtsbehörde die Ansichten der anderen betroffenen Aufsichtsbehörden nicht außer Acht lassen und hat ein maßgeblicher und begründeter Einspruch, der von einer anderen betroffenen Aufsichtsbehörde eingelegt wird, zur Folge, dass die Annahme des Beschlussentwurfs der federführenden Aufsichtsbehörde zumindest vorübergehend blockiert wird (Rn. 50 bis 53, 56 bis 59 und 63 bis 65).

Der Gerichtshof hat ferner klargestellt, dass es mit den Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union, die das Recht auf den Schutz der personenbezogenen Daten einer Person bzw. auf einen wirksamen Rechtsbehelf garantieren, in Einklang steht, dass eine Aufsichtsbehörde eines Mitgliedstaats, die in Bezug auf eine grenzüberschreitende Datenverarbeitung nicht die federführende Aufsichtsbehörde ist, von der Befugnis zur Geltendmachung eines vermeintlichen Verstoßes gegen die DSGVO vor einem Gericht dieses Staates nur unter Beachtung der Regeln über die Verteilung der Entscheidungsbefugnisse zwischen der federführenden Aufsichtsbehörde und den anderen Aufsichtsbehörden[88] Gebrauch machen kann (Rn. 67).

Zweitens hat der Gerichtshof entschieden, dass im Fall einer grenzüberschreitenden Datenverarbeitung die Ausübung der Befugnis zur Klageerhebung[89], die einer Aufsichtsbehörde eines Mitgliedstaats zusteht, die nicht die federführende Aufsichtsbehörde ist, nicht voraussetzt, dass der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter, auf den sich diese Klage bezieht, über eine Hauptniederlassung oder eine andere Niederlassung im Hoheitsgebiet dieses Mitgliedstaats verfügt. Die Ausübung dieser Befugnis muss jedoch in den räumlichen

---

84 In den Art. 56 und 60 DSGVO vorgesehen.

85 Art. 56 Abs. 1 DSGVO.

86 Art. 60 Abs. 7 DSGVO.

87 Art. 56 Abs. 2 und Art. 66 DSGVO betreffen die Ausnahmen vom Grundsatz der Entscheidungsbefugnis der federführenden Aufsichtsbehörde.

88 Vgl. Art. 55 und 56 DSGVO in Verbindung mit Art. 60 DSGVO.

89 Nach Art. 58 Abs. 5 DSGVO.

Anwendungsbereich der DSGVO[90] fallen, was voraussetzt, dass der für die grenzüberschreitende Verarbeitung Verantwortliche oder der Auftragsverarbeiter über eine Niederlassung im Gebiet der Union verfügt (Rn. 80, 83, 84 und Tenor 2).

Drittens hat der Gerichtshof für Recht erkannt, dass im Fall einer grenzüberschreitenden Datenverarbeitung die Befugnis einer Aufsichtsbehörde eines Mitgliedstaats, die nicht die federführende Aufsichtsbehörde ist, vermeintliche Verstöße gegen die DSGVO dem Gericht dieses Staates zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben, sowohl in Bezug auf die Hauptniederlassung des für die Verarbeitung Verantwortlichen, die sich in dem Mitgliedstaat, dem diese Behörde angehört, befindet, als auch gegenüber einer anderen Niederlassung dieses Verantwortlichen ausgeübt werden kann, sofern Gegenstand der Klage eine Datenverarbeitung ist, die im Rahmen der Tätigkeiten dieser Niederlassung erfolgt, und die genannte Behörde dafür zuständig ist, die genannte Befugnis auszuüben.

Der Gerichtshof hat jedoch klargestellt, dass diese Befugnis nur ausgeübt werden kann, soweit die DSGVO gilt. Da im vorliegenden Fall die Tätigkeiten der Niederlassung des Facebook-Konzerns in Belgien untrennbar mit der Verarbeitung der im Ausgangsverfahren in Rede stehenden personenbezogenen Daten verbunden sind, für die Facebook Ireland hinsichtlich des Unionsgebiets der Verantwortliche ist, erfolgt diese Verarbeitung „im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen“ und fällt daher in den Anwendungsbereich der DSGVO (Rn. 94 bis 96 und Tenor 3).

Viertens hat der Gerichtshof entschieden, dass, wenn eine Aufsichtsbehörde eines Mitgliedstaats, die nicht die „federführende Aufsichtsbehörde“ ist, wegen einer grenzüberschreitenden Verarbeitung personenbezogener Daten, bevor die DSGVO galt, eine Klage erhoben hat, diese Klage unionsrechtlich auf der Grundlage der Vorschriften der Richtlinie 95/46 aufrechterhalten werden kann, die für Verstöße gegen die in ihr enthaltenen Vorschriften, die bis zu dem Zeitpunkt begangen worden sind, zu dem die Richtlinie aufgehoben wurde, weiter gilt. Darüber hinaus kann eine solche Klage von der genannten Aufsichtsbehörde wegen Verstößen erhoben werden, die begangen wurden, nachdem die DSGVO anwendbar wurde, sofern es sich dabei um einen derjenigen Fälle handelt, in denen diese Aufsichtsbehörde nach der Verordnung ausnahmsweise befugt ist, einen Beschluss zu erlassen, mit dem festgestellt wird, dass die betreffende Datenverarbeitung gegen die in der Verordnung enthaltenen Vorschriften verstößt, und die in der Verordnung vorgesehenen Verfahren der Zusammenarbeit eingehalten werden (Rn. 105 und Tenor 4).

Fünftens und letztens hat der Gerichtshof die unmittelbare Wirkung der Bestimmung der DSGVO anerkannt, wonach jeder Mitgliedstaat durch Rechtsvorschriften vorsieht, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben. Folglich kann sich eine Aufsichtsbehörde auf diese Vorschrift berufen, um gegen Private eine Klage zu erheben oder ein entsprechendes Verfahren fortzuführen, auch wenn die genannte

[90] Nach Art. 3 Abs. 1 DSGVO findet diese Verordnung Anwendung auf die Verarbeitung personenbezogener Daten, „soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet“.

Vorschrift in der Rechtsordnung des betreffenden Mitgliedstaats nicht speziell umgesetzt worden ist (Rn. 113 und Tenor 5).

VII. 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 V.1. „Recht, der Verarbeitung personenbezogener Daten zu widersprechen [‚Recht auf Vergessenwerden']") hat sich der Gerichtshof zum räumlichen Anwendungsbereich der Richtlinie 95/46 geäußert.

Er hat entschieden, dass im Sinne der Richtlinie 95/46 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 und 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).

VIII. 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 Nr. 45/2001 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 Nr. 1049/2001[91] über den Zugang zu Dokumenten gestellten Antrag auf Gewährung des Zugangs zu Dokumenten, die personenbezogene Daten enthalten, die Bestimmungen der Verordnung 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).

[91] 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. 2001, L 145, S. 43).

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 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 Nr. 45/2001 prüfen, ob Gründe für die Annahme bestehen, dass durch diese Übermittlung möglicherweise die berechtigten Interessen der Betroffenen beeinträchtigt werden (Rn. 78)[92].

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[93] 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 Nr. 45/2001, unkenntlich gemacht habe. Die Verbreitung der Namen der Sachverständigen stelle eine Übermittlung personenbezogener Daten im Sinne von Art. 8 der Verordnung Nr. 45/2001 dar. Die dort genannten Voraussetzungen für eine Übermittlung dieser Daten seien im vorliegenden Fall aber nicht erfüllt.

[92] Dieses Urteil wurde im Jahresbericht 2010, S. 14 und 15, dargestellt.

[93] 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. 2009, L 309, S. 1).

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[94] 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 Nr. 45/2001 handelt. Da sich der Begriff der personenbezogenen Daten im Sinne von Art. 2 Buchst. a der Verordnung 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 und 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 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 bis 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 und 73).

* * *

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

Die in dieser Übersicht angeführten Urteile sind im Repertorium der Rechtsprechung unter den Rubriken 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07. und 4.11.11.01 indexiert.