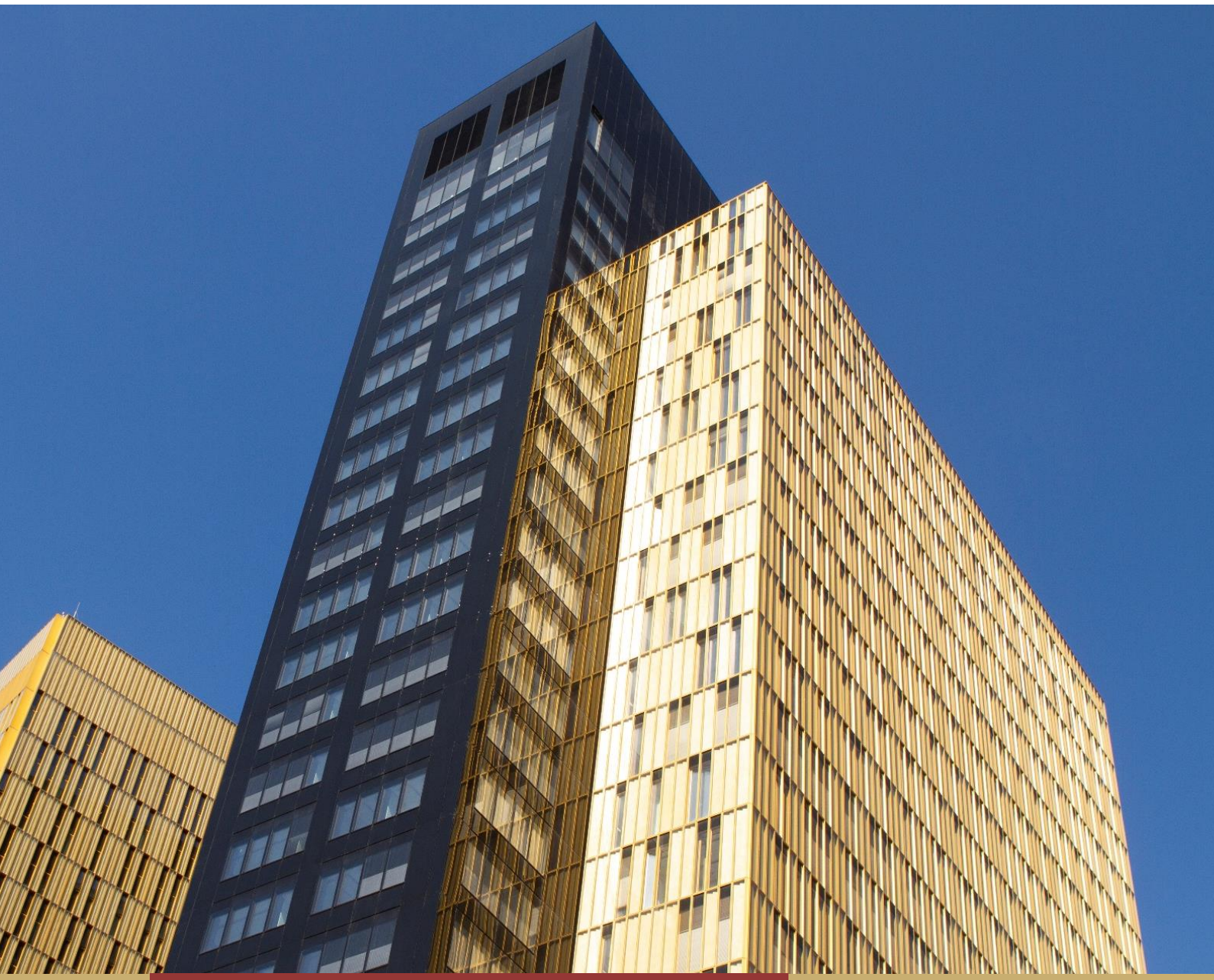
GERICHTSHOF
DER EUROPÄISCHEN UNION

DE



Thematische Übersicht

Schutz personenbezogener Daten

Direktion Wissenschaftlicher Dienst und Dokumentation

curia.europa.eu

Einleitung

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

Es ist im Primärrecht verankert, insbesondere in Art. 8 der Charta der Grundrechte der Europäischen Union (im Folgenden die „Charta“) und in Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Dieses Grundrecht ist ferner eng mit dem in Art. 7 der Charta verbürgten Recht auf Achtung des Privat- und Familienlebens verbunden.

Was das Sekundärrecht angeht, so hat die Europäische Gemeinschaft ab Mitte der 1990er Jahre verschiedene Instrumente eingeführt, mit denen der Schutz personenbezogener Daten sichergestellt werden soll. Der wichtigste Rechtsakt der Union auf diesem Gebiet war die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1].

Die Richtlinie 2002/58/EG[2] hat sodann 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]. Um neuen technologischen und kommerziellen Entwicklungen Rechnung zu tragen, hat der Unionsgesetzgeber 2017 eine Überprüfung dieser Richtlinie eingeleitet[4], die bis heute nicht abgeschlossen ist[5].

2016 reformierte die Europäische Union die einschlägigen allgemeinen Regelungen. Zu diesem Zweck hat sie die Verordnung (EU) 2016/679[6] zum Schutz personenbezogener

---

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. 6).

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 Die Kommission hat am 10. Januar 2017 einen Vorschlag vorgelegt, um diese Richtlinie durch eine Verordnung über Privatsphäre und elektronische Kommunikation zu ersetzen.

5 Am 10. Februar 2021 billigte der Rat der Europäischen Union ein Verhandlungsmandat für die Überarbeitung der Vorschriften zum Schutz der Privatsphäre und der Vertraulichkeit bei der Nutzung elektronischer Kommunikationsdienste, das die Aufnahme von Verhandlungen mit dem Europäischen Parlament ermöglicht. Der Text des Vorschlags für eine Verordnung 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) ist unter diesem Link abrufbar: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*.

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).

Daten (Datenschutz-Grundverordnung, 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, deren Bestimmungen seit dem 6. Mai 2018 gelten.

Bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU wird der Datenschutz seit dem 11. Dezember 2018 insbesondere durch die Verordnung (EU) 2018/1725[8] gewährleistet. Im Interesse eines einheitlichen Ansatzes zum Schutz personenbezogener Daten in der gesamten Union zielt diese Verordnung darauf ab, die Vorschriften in diesem Bereich so weit wie möglich an die Regelung in der DSGVO anzupassen.

Um den Herausforderungen der neuen Technologien zu begegnen, hat der Unionsgesetzgeber schließlich seit 2020 den Erlass neuer Rechtsvorschriften in die Wege geleitet[9], die mit den unionsrechtlichen Bestimmungen über den Schutz personenbezogener Daten in Einklang stehen.

In Anbetracht der umfangreichen Rechtsprechung des Gerichtshofs zum Schutz personenbezogener Daten soll diese thematische Übersicht eine Auswahl grundlegender Urteile in diesem Bereich sowie von Urteilen präsentieren, die einen wichtigen Beitrag zur Weiterentwicklung dieser Rechtsprechung geleistet haben, mit besonderem Augenmerk auf die Urteile der Großen Kammer des Gerichtshofs. Insbesondere soll diese Übersicht sowohl die Rechtsprechung zur allgemeinen Regelung im Bereich des Schutzes personenbezogener Daten, die sich aus der Auslegung der Richtlinie 95/46 und der DSGVO ergibt, als auch die Rechtsprechung zur sektorbezogenen Regelung, die u. a. den Sektor der elektronischen Kommunikation und das Strafrecht betrifft, abdecken. Im Übrigen möchte sie eine Auswahl von Urteilen präsentieren, die sich auf Regelungen beziehen, die übergreifend anwendbar sind, wobei zuallererst die entscheidende Rolle der Charta bei der Entwicklung der Rechtsprechung beleuchtet wird.

---

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).

8 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).

9 In diesem Zusammenhang sind insbesondere drei Gesetzesinitiativen zu erwähnen: i) Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt) (ABl. 2022, L 152, S 1) und Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung) (ABl. 2023, L 2854, S. 1); ii) ein Legislativpaket über digitale Dienste und Märkte, bestehend aus der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. 2022, L 277, S. 1) und der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) (ABl. 2022, L 265, S. 1); und iii) der allererste Legislativvorschlag zur Schaffung eines Rechtsrahmens für künstliche Intelligenz, der in einer Verordnung über künstliche Intelligenz (ABl. 2024, L, 1689) resultierte.

Inhaltsverzeichnis

I. Das in der Charta 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), EU:C:2010:662)

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

n 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 ihres Privatlebens im Allgemeinen und auf Schutz

[10] 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).

[11] Verordnung (EG) Nr. 259/2008 der Kommission vom 18. März 2008 mit Durchführungsbestimmungen zur Verordnung Nr. 1290/2005 hinsichtlich der Veröffentlichung von Informationen über die Empfänger von Mitteln aus dem Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) (ABl. 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).

ihrer personenbezogenen Daten im Besonderen darstellt, da Dritte Zugang zu diesen Daten erhalten.

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. 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.

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. Er hat allerdings nicht die Wirkungen der Veröffentlichung der Listen von Empfängern von EGFL- und ELER-Mitteln in Frage gestellt, die die nationalen Behörden in der Zeit vor dem Tag der Verkündung des Urteils vorgenommen haben.

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

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.

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.

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. 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. 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. 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.

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.

Urteil vom 21. Juni 2022 (Große Kammer), Ligue des droits humains (C-817/19, EU:C:2022:491)

Bei den PNR-Daten (Passenger Name Record) handelt es sich um Buchungsdaten, die von den Fluggesellschaften in ihren Buchungs- und Abfertigungssystemen gespeichert werden. Die PNR-Richtlinie[12] verpflichtet die Fluggesellschaften, zur Bekämpfung von Terrorismus und schwerer Kriminalität die Daten aller Fluggäste von Flügen zwischen einem Drittstaat und der Europäischen Union (Drittstaatsflüge) an die PNR-Zentralstelle des Mitgliedstaats, in dem der betreffende Flug angekommen bzw. von dem er abgegangen ist, zu übermitteln. Die übermittelten PNR-Daten werden einer Vorabüberprüfung durch die PNR-Zentralstelle[13] unterzogen und anschließend im Hinblick auf eine etwaige nachträgliche Überprüfung durch die zuständigen Behörden des betreffenden Mitgliedstaats oder eines anderen Mitgliedstaats gespeichert. Die Mitgliedstaaten können beschließen, die Richtlinie auch auf Flüge innerhalb der Union (EU-Flüge) anzuwenden.[14]

Die Ligue des droits humains (Liga für Menschenrechte) hat beim belgischen Verfassungsgerichtshof eine Nichtigkeitsklage gegen das Gesetz erhoben, mit dem die

[12] Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (ABl. 2016, L 119, S. 132) (im Folgenden: PNR-Richtlinie).

[13] Die Vorabüberprüfung dient dazu, diejenigen Personen zu ermitteln, die von den zuständigen Behörden genauer überprüft werden müssen, da sie möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind. Sie wird systematisch und automatisiert durchgeführt, indem die PNR-Daten mit „maßgeblichen" Datenbanken abgeglichen oder anhand im Voraus festgelegter Kriterien verarbeitet werden (Art. 6 Abs. 2 Buchst. a und Abs. 3 der PNR-Richtlinie).

[14] In Anwendung der in Art. 2 der PNR-Richtlinie vorgesehenen Möglichkeit.

PNR-Richtlinie und die API-Richtlinie[15] in belgisches Recht umgesetzt wurden. Sie macht geltend, dieses Gesetz verletze das Recht auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten. Sie rügt den sehr großen Umfang der PNR-Daten sowie den allgemeinen Charakter ihrer Erhebung, Übermittlung und Verarbeitung. Außerdem schränke das Gesetz die Freizügigkeit ein, da mit ihm durch die Ausdehnung des PNR-Systems auf EU-Flüge sowie auf Beförderungen mit anderen Mitteln innerhalb der Union indirekt wieder Grenzkontrollen eingeführt würden.

In diesem Kontext hat der belgische Verfassungsgerichtshof dem Gerichtshof zehn Fragen zur Vorabentscheidung vorgelegt, die u. a. die Gültigkeit und die Auslegung der PNR-Richtlinie betreffen.

Die Große Kammer des Gerichtshofs bestätigt in ihrem Urteil die Gültigkeit der PNR-Richtlinie, da sie im Einklang mit der Charta ausgelegt werden kann.

Der Gerichtshof hat insoweit entschieden, dass die Prüfung der vorgelegten Fragen nichts ergeben hat, was die Gültigkeit der PNR-Richtlinie berühren könnte, da seine Auslegung ihrer Bestimmungen im Licht der Grundrechte, die in den Art. 7, 8 und 21 sowie in Art. 52 Abs. 1 der Charta[16] verankert sind, die Vereinbarkeit dieser Richtlinie mit den genannten Artikeln gewährleistet.

Zunächst weist der Gerichtshof darauf hin, dass ein Rechtsakt der Union so weit wie möglich in einer seine Gültigkeit nicht in Frage stellenden Weise und im Einklang mit dem gesamten Primärrecht und insbesondere mit den Bestimmungen der Charta auszulegen ist. Dabei müssen die Mitgliedstaaten darauf achten, dass sie sich nicht auf eine Auslegung des Rechtsakts stützen, die mit den durch die Rechtsordnung der Union geschützten Grundrechten oder mit anderen in dieser Rechtsordnung anerkannten allgemeinen Grundsätzen kollidiert. Zur PNR-Richtlinie führt der Gerichtshof aus, dass eine ganze Reihe ihrer Erwägungsgründe und Bestimmungen eine solche Auslegung erfordern, und hebt die Bedeutung hervor, die der Unionsgesetzgeber – unter Bezugnahme auf ein hohes Datenschutzniveau – der uneingeschränkten Achtung der in der Charta verankerten Grundrechte beimisst.

Der Gerichtshof stellt fest, dass die PNR-Richtlinie mit fraglos schwerwiegenden Eingriffen in die durch die Art. 7 und 8 der Charta garantierten Rechte verbunden ist, insbesondere soweit sie auf die Schaffung eines Systems kontinuierlicher, nicht zielgerichteter und systematischer Überwachung abzielt, das die automatisierte

---

15 Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln (ABl. 2004, L 261, S. 24, im Folgenden: API-Richtlinie). Diese Richtlinie regelt die Vorabübermittlung von Angaben über die beförderten Personen (wie Nummer und Art des mitgeführten Reisedokuments sowie die Staatsangehörigkeit) durch die Fluggesellschaften an die zuständigen nationalen Behörden als Mittel zur Verbesserung der Grenzkontrollen und zur Bekämpfung der illegalen Einwanderung.

16 Nach dieser Vorschrift muss jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und deren Wesensgehalt achten. Außerdem dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

Überprüfung personenbezogener Daten sämtlicher Personen einschließt, die Flugreisen unternehmen. Er weist darauf hin, dass die Möglichkeit für die Mitgliedstaaten, einen solchen Eingriff zu rechtfertigen, zu beurteilen ist, indem seine Schwere bestimmt und geprüft wird, ob die verfolgte dem Gemeinwohl dienende Zielsetzung dazu in angemessenem Verhältnis steht.

Der Gerichtshof kommt zu dem Schluss, dass die in der PNR-Richtlinie vorgesehene Übermittlung, Verarbeitung und Speicherung von PNR-Daten als auf das für die Bekämpfung terroristischer Straftaten und schwerer Kriminalität absolut Notwendige beschränkt angesehen werden kann, sofern die in der Richtlinie vorgesehenen Befugnisse eng ausgelegt werden. Hierzu enthält sein Urteil unter anderem folgende Ausführungen:

- Das durch die PNR-Richtlinie eingeführte System darf sich nur auf die in den Rubriken ihres Anhangs I aufgeführten, klar identifizierbaren und umschriebenen Informationen erstrecken, die in Zusammenhang mit dem durchgeführten Flug und dem betreffenden Fluggast stehen. Dies bedeutet bei einigen Rubriken dieses Anhangs, dass nur die dort ausdrücklich genannten Angaben erfasst werden[17].

- Die Anwendung des durch die PNR-Richtlinie geschaffenen Systems muss auf terroristische Straftaten und auf schwere Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen beschränkt werden. Sie darf sich nicht auf strafbare Handlungen erstrecken, die zwar das in der Richtlinie vorgesehene Kriterium in Bezug auf den Schweregrad erfüllen und in ihrem Anhang II aufgeführt sind, angesichts der Besonderheiten des nationalen Strafrechtssystems aber zur gewöhnlichen Kriminalität gehören.

- Die etwaige Ausdehnung der Anwendung der PNR-Richtlinie auf alle oder einen Teil der EU-Flüge aufgrund der den Mitgliedstaaten in der Richtlinie eingeräumten Befugnis muss sich auf das absolut Notwendige beschränken. Sie muss Gegenstand einer wirksamen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein können, deren Entscheidung bindend ist. Hierzu führt der Gerichtshof aus:

    - Nur in einer Situation, in der es nach der Einschätzung des betreffenden Mitgliedstaats hinreichend konkrete Umstände für die Annahme gibt, dass er mit einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung konfrontiert ist, werden die Grenzen des absolut Notwendigen nicht überschritten, wenn die PNR-Richtlinie für einen auf das

[17] So müssen sich die „Zahlungsinformationen“ (Rubrik 6 des Anhangs) auf die Modalitäten der Zahlung und die Abrechnung des Flugscheins beschränken, unter Ausschluss anderer Informationen ohne direkten Bezug zum Flug, und die „Allgemeinen Hinweise“ (Rubrik 12) dürfen sich nur auf die in dieser Rubrik ausdrücklich aufgezählten Angaben zu minderjährigen Fluggästen erstrecken.

absolut Notwendige begrenzten, aber verlängerbaren Zeitraum auf alle EU-Flüge aus oder nach diesem Mitgliedstaat angewandt wird[18].

- Ohne eine solche terroristische Bedrohung darf die Anwendung der Richtlinie nicht auf alle EU-Flüge ausgedehnt werden, sondern muss sich auf EU-Flüge beschränken, die etwa bestimmte Flugverbindungen, bestimmte Reisemuster oder bestimmte Flughäfen betreffen, für die es nach der Einschätzung des betreffenden Mitgliedstaats Anhaltspunkte gibt, die eine Anwendung der Richtlinie rechtfertigen können. Die absolute Notwendigkeit ihrer Anwendung auf die ausgewählten EU-Flüge muss nach Maßgabe der Entwicklung der Bedingungen, die ihre Auswahl gerechtfertigt haben, regelmäßig überprüft werden.

- Für die Zwecke der Vorabüberprüfung der PNR-Daten, die dazu dient, diejenigen Personen zu ermitteln, die vor ihrer Ankunft oder ihrem Abflug genauer überprüft werden müssen, und deren erster Schritt in automatisierten Verarbeitungen besteht, darf die PNR-Zentralstelle diese Daten zum einen nur mit Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind[19], abgleichen. Diese Datenbanken müssen frei von Diskriminierung sein und von den zuständigen Behörden im Zusammenhang mit der Bekämpfung terroristischer Straftaten und schwerer Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen betrieben werden. Zum anderen darf die PNR-Zentralstelle bei der Vorabüberprüfung anhand im Voraus festgelegter Kriterien keine Technologien der künstlichen Intelligenz im Rahmen selbstlernender Systeme (machine learning) heranziehen, die – ohne menschliche Einwirkung und Kontrolle – den Bewertungsprozess und insbesondere die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien ändern können. Die genannten Kriterien sind so festzulegen, dass sie speziell auf Personen abzielen, bei denen der begründete Verdacht einer Beteiligung an terroristischen Straftaten oder schwerer Kriminalität bestehen könnte, und dass sowohl „belastende“ als auch „entlastende“ Gesichtspunkte berücksichtigt werden; sie dürfen nicht zu unmittelbaren oder mittelbaren Diskriminierungen führen[20].

---

18 Das Vorliegen einer derartigen Bedrohung ist nämlich als solches geeignet, einen Zusammenhang zwischen der Übermittlung und Verarbeitung der betreffenden Daten und der Bekämpfung des Terrorismus herzustellen. Daher werden die Grenzen des absolut Notwendigen nicht überschritten, wenn die PNR-Richtlinie für begrenzte Zeit Anwendung auf alle EU-Flüge aus oder nach dem betreffenden Mitgliedstaat findet; die Anordnung ihrer Anwendung muss Gegenstand einer Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein können.

19 Das heißt mit Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind (Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie). Dagegen könnten Analysen anhand verschiedener Datenbanken die Form einer Datenexploration (data mining) annehmen und zu einer unverhältnismäßigen Nutzung dieser Daten führen, die es ermöglichen würde, ein genaues Profil der betreffenden Personen zu erstellen, nur weil sie eine Flugreise unternehmen wollen.

20 Die im Voraus festgelegten Kriterien müssen zielgerichtet, verhältnismäßig und bestimmt sein und regelmäßig überprüft werden (Art. 6 Abs. 4 der PNR-Richtlinie). Die Vorabüberprüfung anhand im Voraus festgelegter Kriterien muss in nicht diskriminierender Weise erfolgen.

- Angesichts der Fehlerquote, die solchen automatisierten Verarbeitungen der PNR-Daten innewohnt, und der erheblichen Zahl „falsch positiver“ Ergebnisse, die in den Jahren 2018 und 2019 bei ihrer Anwendung auftraten, hängt die Eignung des durch die PNR-Richtlinie geschaffenen Systems zur Erreichung der verfolgten Ziele im Wesentlichen vom ordnungsgemäßen Ablauf der Überprüfung der im Rahmen dieser Verarbeitungen erzielten Treffer ab, die von der PNR-Zentralstelle in einem zweiten Schritt mit nicht automatisierten Mitteln vorgenommen wird. Insoweit müssen die Mitgliedstaaten klare und präzise Regeln vorsehen, die Leitlinien und einen Rahmen für die von den Bediensteten der PNR-Zentralstelle, die mit der individuellen Überprüfung betraut sind, vorzunehmende Analyse vorgeben, um für die uneingeschränkte Achtung der in den Art. 7, 8 und 21 der Charta verankerten Grundrechte zu sorgen und insbesondere eine dem Diskriminierungsverbot Rechnung tragende kohärente Verwaltungspraxis innerhalb der PNR-Zentralstelle zu gewährleisten. Insbesondere müssen sie sich vergewissern, dass die PNR-Zentralstelle Kriterien für die objektive Überprüfung aufstellt, die es ihren Bediensteten ermöglichen, zum einen zu prüfen, ob und inwieweit ein Treffer (hit) tatsächlich eine Person betrifft, die möglicherweise an terroristischen Straftaten oder an schwerer Kriminalität beteiligt ist, und zum anderen, ob die automatisierten Verarbeitungen keinen diskriminierenden Charakter haben. Dabei müssen sich die zuständigen Behörden vergewissern, dass der Betroffene die Funktionsweise der im Voraus festgelegten Prüfkriterien und der Programme zu ihrer Anwendung verstehen und deshalb in Kenntnis aller Umstände entscheiden kann, ob er von seinem Recht auf Einlegung von Rechtsbehelfen Gebrauch macht. Desgleichen müssen im Rahmen eines solchen Rechtsbehelfs das mit der Rechtmäßigkeitsprüfung der Entscheidung der zuständigen Behörden betraute Gericht sowie, außer in Fällen einer Bedrohung der Sicherheit des Staates, der Betroffene selbst sowohl von allen Gründen als auch von den Beweisen, auf deren Grundlage diese Entscheidung getroffen wurde, Kenntnis erlangen können, einschließlich der im Voraus festgelegten Prüfkriterien und der Funktionsweise der Programme, mit denen diese Kriterien angewandt werden.

- Nachträglich, d. h. nach der Ankunft oder dem Abflug der betreffenden Person, darf eine Zurverfügungstellung und Überprüfung der PNR-Daten nur aufgrund neuer Umstände und objektiver Anhaltspunkte erfolgen, die entweder geeignet sind, den begründeten Verdacht einer Beteiligung dieser Person an schwerer Kriminalität, die – zumindest mittelbar – einen objektiven Zusammenhang mit der Beförderung von Fluggästen aufweist, zu wecken, oder den Schluss zulassen, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur

Nach Art. 6 Abs. 4 Satz 4 der PNR-Richtlinie dürfen die rassische oder ethnische Herkunft, die politischen Meinungen, die religiösen oder weltanschaulichen Überzeugungen, die Mitgliedschaft in einer Gewerkschaft, der Gesundheitszustand, das Sexualleben oder die sexuelle Orientierung einer Person unter keinen Umständen als Grundlage für diese Kriterien dienen.

Bekämpfung terroristischer Straftaten, die einen solchen Zusammenhang aufweisen, leisten könnten. Die Zurverfügungstellung der PNR-Daten zum Zweck einer solchen nachträglichen Überprüfung muss grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle im Anschluss an einen mit Gründen versehenen Antrag der zuständigen Behörden unterworfen werden, unabhängig davon, ob der Antrag vor oder nach Ablauf der Frist von sechs Monaten ab der Übermittlung dieser Daten an die PNR-Zentralstelle gestellt wurde[21].

Urteil vom 22. November 2022 (Große Kammer), Luxembourg Business Registers (Verbundene Rechtssachen C-37/20 und C-601/20, EU:C:2022:912)

Zum Zweck der Bekämpfung und Verhinderung der Geldwäsche und der Terrorismusfinanzierung verpflichtet die Geldwäscherichtlinie[22] die Mitgliedstaaten, ein Register mit Informationen über die wirtschaftlichen Eigentümer[23] von in ihrem Gebiet eingetragenen Gesellschaften oder sonstigen juristischen Personen zu führen. Nach einer Änderung dieser Richtlinie durch die Richtlinie 2018/843[24] müssen einige dieser Informationen jedem Mitglied der Öffentlichkeit in allen Fällen zugänglich gemacht werden. Gemäß der so geänderten Geldwäscherichtlinie (im Folgenden: geänderte Geldwäscherichtlinie) wurde mit den luxemburgischen Rechtsvorschriften ein Registre des bénéficiaires effectifs (Register der wirtschaftlichen Eigentümer, im Folgenden: RBE) eingerichtet, das dazu dient, eine Reihe von Informationen über die wirtschaftlichen Eigentümer der eingetragenen Einrichtungen, zu denen jedermann Zugang hat, zu speichern und zur Verfügung zu stellen.

In diesem Zusammenhang wurde das Tribunal d'arrondissement de Luxembourg (Bezirksgericht Luxemburg) mit zwei von WM und der Sovim SA anhängig gemachten Rechtssachen befasst, die die Ablehnung ihrer Anträge auf Beschränkung des Zugangs der breiten Öffentlichkeit zu Informationen in der ersten Rechtssache betreffend WM als wirtschaftlichen Eigentümer einer Immobiliengesellschaft und in der zweiten Rechtssache betreffend den wirtschaftlichen Eigentümer der Sovim SA anfechten. Im Rahmen dieser beiden Rechtssachen hat das Tribunal d'arrondissement de Luxembourg (Bezirksgericht Luxemburg), da es u. a. Zweifel an der Gültigkeit der Unionsrechtsbestimmungen hegte, mit denen das System für den Zugang der

[21] Nach Art. 12 Abs. 1 und 3 der PNR-Richtlinie ist eine solche Kontrolle nur für Anfragen zwecks Zurverfügungstellung der PNR-Daten, die nach Ablauf der Sechsmonatsfrist ab der Übermittlung dieser Daten an die PNR-Zentralstelle gestellt werden, ausdrücklich vorgesehen.

[22] Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission (ABl. 2015, L 141, S. 73, im Folgenden: Geldwäscherichtlinie).

[23] Nach Art. 3 Nr. 6 der Geldwäscherichtlinie sind wirtschaftliche Eigentümer alle natürlichen Personen, in deren Eigentum oder unter deren Kontrolle der Kunde letztlich steht, und/oder die natürliche(n) Person(en), in deren Auftrag eine Transaktion oder Tätigkeit ausgeführt wird.

[24] Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU (ABl. 2018, L 156, S. 43).

Öffentlichkeit zu den Informationen über die wirtschaftlichen Eigentümer geschaffen wird, dem Gerichtshof eine Vorlagefrage zur Beurteilung der Gültigkeit vorgelegt.

Mit seinem Urteil erklärt der Gerichtshof (Große Kammer) die Richtlinie 2018/843 für ungültig, soweit mit ihr die Geldwäscherichtlinie dahin geändert wurde, dass die Mitgliedstaaten sicherstellen, dass die Informationen über die wirtschaftlichen Eigentümer der in ihrem Gebiet eingetragenen Gesellschaften oder anderen juristischen Personen in allen Fällen für alle Mitglieder der Öffentlichkeit zugänglich sind[25].

In erster Linie stellt der Gerichtshof fest, dass der durch die geänderte Geldwäscherichtlinie vorgesehene Zugang aller Mitglieder der Öffentlichkeit zu den Informationen über die wirtschaftlichen Eigentümer einen schwerwiegenden Eingriff in die in den Art. 7 bzw. 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) verankerten Grundrechte auf Privatleben und auf Schutz personenbezogener Daten darstellt.

Hierzu weist der Gerichtshof darauf hin, dass, da die betreffenden Daten Informationen über bestimmte natürliche Personen, und zwar die wirtschaftlichen Eigentümer von im Gebiet der Mitgliedstaaten eingetragenen Gesellschaften und anderen juristischen Personen, enthalten, der Zugang von allen Mitgliedern der Öffentlichkeit dazu das Grundrecht auf Achtung des Privatlebens berührt. Außerdem stellt die öffentliche Zugänglichmachung dieser Daten eine Verarbeitung personenbezogener Daten dar. Zudem ist eine solche öffentliche Zugänglichmachung unabhängig von der späteren Verwendung der übermittelten Informationen ein Eingriff in die oben genannten Grundrechte.

Zur Schwere dieses Eingriffs weist der Gerichtshof darauf hin, dass sich die der breiten Öffentlichkeit zur Verfügung gestellten Informationen auf die Identität des wirtschaftlichen Eigentümers sowie die Art und den Umfang seines wirtschaftlichen Interesses an Gesellschaften oder anderen juristischen Personen beziehen und sich anhand dieser Informationen ein Profil mit bestimmten persönlichen Identifizierungsdaten, der Vermögenslage des Betroffenen sowie den Wirtschaftssektoren, Ländern und spezifischen Unternehmen, in die er investiert hat, erstellen lässt. Außerdem sind diese Angaben einer potenziell unbegrenzten Zahl von Personen zugänglich, so dass durch eine solche Verarbeitung personenbezogener Daten auch Personen, die sich aus nicht mit der Zielsetzung, die mit dieser Maßnahme verfolgt wird, zusammenhängenden Gründen u. a. über die materielle und finanzielle Situation eines wirtschaftlichen Eigentümers Kenntnis verschaffen wollen, ungehindert auf diese Angaben zugreifen können. Diese Möglichkeit erweist sich als umso leichter, wenn die Daten im Internet abgerufen werden können. Außerdem werden die möglichen Folgen einer etwaigen missbräuchlichen Verwendung ihrer personenbezogenen Daten für die

[25] Ungültigkeit von Art. 1 Nr. 15 Buchst. c der Richtlinie 2018/843, durch den Art. 30 Abs. 5 Unterabs. 1 Buchst. c der Geldwäscherichtlinie geändert wurde.

betroffenen Personen dadurch verschärft, dass diese Daten, sobald sie der breiten Öffentlichkeit zur Verfügung gestellt worden sind, nicht nur frei abgerufen, sondern auch gespeichert und verbreitet werden können und es für diese Personen umso schwieriger, wenn nicht sogar illusorisch wird, sich wirksam gegen Missbräuche zur Wehr zu setzen.

In zweiter Linie stellt der Gerichtshof im Rahmen der Prüfung der Rechtfertigung des fraglichen Eingriffs erstens fest, dass im vorliegenden Fall der Grundsatz der Gesetzmäßigkeit gewahrt ist. Denn die Beschränkung der Ausübung der genannten Grundrechte, die sich aus dem Zugang der breiten Öffentlichkeit zu Informationen über die wirtschaftlichen Eigentümer ergibt, ist in einem Gesetzgebungsakt vorgesehen, nämlich der geänderten Geldwäscherichtlinie. Außerdem stellt die Richtlinie zum einen klar, dass diese Informationen angemessen, richtig und aktuell sein müssen, und führt ausdrücklich bestimmte Daten auf, zu denen der öffentliche Zugang zu gewähren ist. Zum anderen legt sie die Voraussetzungen fest, unter denen die Mitgliedstaaten Ausnahmen von einem solchen Zugang vorsehen können.

Zweitens berührt dieser Eingriff nicht den Wesensgehalt der in den Art. 7 und 8 der Charta verankerten Grundrechte. Es trifft zwar zu, dass die geänderte Geldwäscherichtlinie keine erschöpfende Aufzählung der Daten enthält, zu denen jedem Mitglied der Öffentlichkeit der Zugang erlaubt werden muss, und dass die Mitgliedstaaten den Zugang zu weiteren Informationen vorsehen können, gleichwohl aber dürfen nur angemessene Angaben über die wirtschaftlichen Eigentümer und das wirtschaftliche Interesse eingeholt, aufbewahrt und somit potenziell der Öffentlichkeit zugänglich gemacht werden, was insbesondere Angaben ausschließt, die keinen angemessenen Bezug zu den Zielsetzungen der geänderten Geldwäscherichtlinie aufweisen. Es ist daher nicht ersichtlich, dass die öffentliche Zugänglichmachung von Angaben, die einen solchen Bezug aufweisen, in irgendeiner Weise den Wesensgehalt der betreffenden Grundrechte beeinträchtigen würde.

Drittens betont der Gerichtshof, dass der Unionsgesetzgeber dadurch, dass er den Zugang der breiten Öffentlichkeit zu den Informationen über die wirtschaftlichen Eigentümer vorsieht, die Geldwäsche und die Terrorismusfinanzierung verhindern will, indem er mit erhöhter Transparenz ein Umfeld schafft, das weniger leicht für diese Zwecke genutzt werden kann, was eine dem Gemeinwohl dienende Zielsetzung darstellt, die auch schwere Eingriffe in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte rechtfertigen kann.

Viertens stellt der Gerichtshof im Rahmen der Prüfung der Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit des in Rede stehenden Eingriffs fest, dass zwar der Zugang der breiten Öffentlichkeit zu den Informationen über die wirtschaftlichen Eigentümer geeignet ist, zur Verwirklichung dieser Zielsetzung beizutragen.

Dieser Eingriff kann jedoch nicht auf das absolut Erforderliche beschränkt angesehen werden. Zum einen lässt sich die absolute Erforderlichkeit dieses Eingriffs nicht mit der

Begründung belegen, dass das Kriterium des „berechtigten Interesses“, über das nach der Geldwäscherichtlinie in ihrer vor ihrer Änderung durch die Richtlinie 2018/843 geltenden Fassung jede Person verfügen musste, die Zugang zu den Informationen über die wirtschaftlichen Eigentümer wünschte, schwer umzusetzen wäre und seine Anwendung zu willkürlichen Entscheidungen führen könnte. Das etwaige Bestehen von Schwierigkeiten bei der genauen Festlegung der Fälle und Bedingungen, in bzw. unter denen die Öffentlichkeit Zugang zu den Informationen über die wirtschaftlichen Eigentümer hat, kann es nämlich nicht rechtfertigen, dass der Unionsgesetzgeber den Zugang der breiten Öffentlichkeit zu diesen Informationen vorsieht.

Zum anderen vermögen auch die Erwägungen in der Richtlinie 2018/843 nicht die absolute Erforderlichkeit des fraglichen Eingriffs zu belegen[26]. Soweit es in diesen Erwägungen heißt, dass durch den Zugang der breiten Öffentlichkeit zu den Angaben über die wirtschaftlichen Eigentümer eine größere Kontrolle der Informationen durch die Zivilgesellschaft, insbesondere die Presse und zivilgesellschaftliche Organisationen, ermöglicht werde, betont der Gerichtshof, dass sowohl die Presse als auch die zivilgesellschaftlichen Organisationen, die einen Bezug zur Verhinderung und zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung aufweisen, ein berechtigtes Interesse am Zugang zu den betreffenden Informationen haben. Gleiches gilt für die Personen, die die Identität der wirtschaftlichen Eigentümer einer Gesellschaft oder einer anderen juristischen Person in Erfahrung bringen möchten, da sie mit dieser Geschäfte abschließen könnten, oder für Finanzinstitute und Behörden, die an der Bekämpfung von Straftaten im Bereich der Geldwäsche oder der Terrorismusfinanzierung mitarbeiten.

Außerdem ist der fragliche Eingriff auch nicht verhältnismäßig. Insoweit stellt der Gerichtshof fest, dass die materiellen Regeln für diesen Eingriff nicht dem Erfordernis der Klarheit und Präzision genügen. Die geänderte Geldwäscherichtlinie sieht nämlich den Zugang jedes Mitglieds der Öffentlichkeit „mindestens“ zu den darin genannten Daten vor und räumt den Mitgliedstaaten die Möglichkeit ein, zu zusätzlichen Informationen Zugang zu gewähren, worunter „mindestens“ das Geburtsdatum oder die Kontaktdaten des betreffenden wirtschaftlichen Eigentümers fallen. Aus der Verwendung des Ausdrucks „mindestens“ ergibt sich aber, dass diese Bestimmungen die öffentliche Zugänglichmachung von Daten gestatten, die weder hinreichend bestimmt noch identifizierbar sind.

Was im Übrigen die Gewichtung der Schwere dieses Eingriffs und der Bedeutung der verfolgten dem Gemeinwohl dienenden Zielsetzung betrifft, erkennt der Gerichtshof an, dass diese Zielsetzung angesichts ihrer Bedeutung selbst schwerwiegende Eingriffe in die in den Art. 7 und 8 der Charta verankerten Grundrechte zu rechtfertigen vermag.

[26] Gemeint sind die Erwägungen im 30. Erwägungsgrund der Richtlinie 2018/843.

Zum einen obliegt die Bekämpfung der Geldwäsche und der Terrorismusfinanzierung aber vorrangig den Behörden sowie Einrichtungen wie etwa Kreditinstituten oder Finanzinstituten, denen aufgrund ihrer Tätigkeiten spezifische Pflichten in diesem Bereich auferlegt sind. Aus diesem Grund müssen nach der geänderten Geldwäscherichtlinie die Informationen über die wirtschaftlichen Eigentümer in jedem Fall den zuständigen Behörden und den zentralen Meldestellen ohne Einschränkung sowie den Verpflichteten im Rahmen der Erfüllung der Sorgfaltspflichten gegenüber Kunden zugänglich sein[27].

Zum anderen stellt im Vergleich zu der früheren Regelung, die neben dem Zugang der zuständigen Behörden und bestimmter Einrichtungen zu den Informationen über die wirtschaftlichen Eigentümer den Zugang aller Personen oder Organisationen vorsah, die ein berechtigtes Interesse nachweisen konnten, die mit der Richtlinie 2018/843 eingeführte Regelung einen erheblich schwereren Eingriff in die in den Art. 7 und 8 der Charta verbürgten Grundrechte dar, ohne dass diese zusätzliche Schwere durch etwaige Vorteile kompensiert würde, die sich aus der letztgenannten Regelung im Vergleich zur früheren hinsichtlich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung ergeben könnten.

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)

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

[27] Art. 30 Abs. 5 Unterabs. 1 Buchst. a und b der geänderten Geldwäscherichtlinie.

gegen die britische Regelung über die Vorratsdatenspeicherung geklagt, die den Innenminister ermächtigt, die Betreiber öffentlicher Telekommunikationsdienste zu verpflichten, sämtliche Kommunikationsdaten für bis zu zwölf Monate auf Vorrat zu speichern, wobei die Speicherung des Inhalts der Kommunikationsvorgänge ausgeschlossen ist.

Der Gerichtshof wurde vom Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm,

Schweden) und vom Court of Appeal (England and Wales) (Civil Division) (Berufungsgericht [England & Wales] [Abteilung für Zivilsachen], Vereinigtes Königreich) um Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 (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.

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.

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.

II. Verarbeitung personenbezogener Daten im Sinne der allgemeinen Datenschutzregelung

1. Anwendungsbereich der allgemeinen Regelung

Urteil vom 30. Mai 2006 (Große Kammer), Parlament/Rat (Verbundene Rechtssachen 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[28], 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[29], 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 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.

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

---

[28] 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)

[29] 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).

sie eine davon ausgenommene Verarbeitung personenbezogener Daten betraf. Er hat sie daher für nichtig erklärt.

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.

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.

In diesem Urteil hat sich der Gerichtshof auch zum räumlichen Anwendungsbereich der Richtlinie 95/46 geäußert.

So hat er entschieden, dass eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung ausgeführt wird, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats im Sinne der Richtlinie 95/46 besitzt, wenn der Suchmaschinenbetreiber 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.

Unter solchen Umständen sind nämlich die Tätigkeiten des Suchmaschinenbetreibers und die seiner Niederlassung in einem Mitgliedstaat, auch wenn verschieden, untrennbar miteinander verbunden, da die die Werbeflächen betreffenden Tätigkeiten das Mittel darstellen, um die in Rede stehende Suchmaschine wirtschaftlich rentabel zu machen, und die Suchmaschine gleichzeitig das Mittel ist, das die Durchführung dieser Tätigkeiten ermöglicht.

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.

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. 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.

Urteil vom 16. Januar 2024 (Große Kammer), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Zur Untersuchung einer möglichen politischen Einflussnahme auf das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Österreich)[30] setzte der Nationalrat (Österreich) einen Untersuchungsausschuss (im Folgenden: BVT-Untersuchungsausschuss) ein. WK wurde von diesem Untersuchungsausschuss als Auskunftsperson befragt. Obwohl er eine Anonymisierung beantragt hatte, wurde auf der Webseite des Österreichischen Parlaments das Protokoll seiner Befragung unter vollständiger Nennung seines Vor- und Familiennamens veröffentlicht. WK machte geltend, dass die Preisgabe seiner Identität gegen die DSGVO und gegen österreichisches Recht verstoße und erhob eine Beschwerde bei der Österreichischen Datenschutzbehörde (im Folgenden: Datenschutzbehörde). Mit Bescheid vom 18. September 2019 erklärte sich die Datenschutzbehörde für eine Entscheidung über die Beschwerde unzuständig und führte aus, dass der Grundsatz der Gewaltenteilung ausschließe, dass sie als Organ der Verwaltung die Tätigkeit des BVT-Untersuchungsausschusses kontrolliere, der der Gesetzgebung zuzurechnen sei.

Im Anschluss an das Erkenntnis des Bundesverwaltungsgerichts (Österreich), mit dem der von WK erhobenen Beschwerde stattgegeben und der Bescheid der Datenschutzbehörde aufgehoben wurde, rief die Datenschutzbehörde im Wege einer Revision gegen das Erkenntnis des Bundesverwaltungsgerichts den Verwaltungsgerichtshof an.

In diesem Zusammenhang möchte das vorlegende Gericht vom Gerichtshof wissen, ob die Tätigkeiten eines vom Parlament eines Mitgliedstaats eingesetzten Untersuchungsausschusses in den Anwendungsbereich der DSGVO fallen und ob diese Verordnung anwendbar ist, wenn die fraglichen Tätigkeiten den Schutz der nationalen Sicherheit betreffen.

[30] Seit 1. Dezember 2021 „Direktion Staatsschutz und Nachrichtendienst" (Österreich).

Als Erstes weist der Gerichtshof darauf hin, dass mit Art. 2 Abs. 2 Buchst. a DSGVO, der vorsieht, dass die Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit findet, die nicht in den Anwendungsbereich des Unionsrechts fällt, allein Verarbeitungen vom Anwendungsbereich der Verordnung ausgenommen werden sollen, die von staatlichen Stellen im Rahmen einer Tätigkeit, die der Wahrung der nationalen Sicherheit dient oder derselben Kategorie zugeordnet werden kann, vorgenommen werden. Der bloße Umstand, dass eine Tätigkeit eine spezifische Tätigkeit des Staates oder einer Behörde ist, reicht also nicht aus, um eine solche Tätigkeit automatisch von der Anwendbarkeit der DSGVO auszunehmen.

Diese Auslegung, die sich bereits daraus ergibt, dass nicht danach unterschieden wird, wer Urheber der betreffenden Verarbeitung ist, wird durch Art. 4 Nr. 7 DSGVO[31] bestätigt.

Der Gerichtshof stellt klar, dass der Umstand, dass der BVT-Untersuchungsausschuss parlamentarisch tätig ist, nicht bedeutet, dass seine Tätigkeiten vom Anwendungsbereich der DSGVO ausgenommen sind. Die in Art. 2 Abs. 2 Buchst. a DSGVO vorgesehene Ausnahme bezieht sich nämlich ausschließlich auf Kategorien von Tätigkeiten, die aufgrund ihrer Natur nicht in den Anwendungsbereich des Unionsrechts fallen, und nicht auf Kategorien von Personen. Somit ermöglicht der Umstand, dass die Verarbeitung von personenbezogenen Daten durch einen vom Parlament eines Mitgliedstaats in Ausübung seines Kontrollrechts der Vollziehung eingesetzten Untersuchungsausschuss erfolgt, für sich genommen nicht den Schluss, dass diese Verarbeitung im Rahmen einer Tätigkeit stattfindet, die nicht in den Anwendungsbereich des Unionsrechts fällt.

Als Zweites stellt der Gerichtshof fest, dass es zwar Sache der Mitgliedstaaten ist, ihre wesentlichen Sicherheitsinteressen festzulegen und die geeigneten Maßnahmen zu ergreifen, um die Sicherheit zu gewährleisten[32], doch kann die bloße Tatsache, dass eine nationale Maßnahme zum Schutz der nationalen Sicherheit getroffen wurde, nicht dazu führen, dass das Unionsrecht unanwendbar ist und die Mitgliedstaaten von der erforderlichen Beachtung dieses Rechts entbunden werden. Die in Art. 2 Abs. 2 Buchst. a DSGVO vorgesehene Ausnahme bezieht sich ausschließlich auf Kategorien von Tätigkeiten, die aufgrund ihrer Natur nicht in den Anwendungsbereich des Unionsrechts fallen. Insoweit reicht der Umstand, dass der Verantwortliche eine Behörde ist, deren Haupttätigkeit in der Gewährleistung der nationalen Sicherheit besteht, als solcher nicht aus, um Verarbeitungen personenbezogener Daten, die diese Behörde im Rahmen ihrer anderen Tätigkeiten vornimmt, vom Anwendungsbereich der DSGVO auszunehmen.

---

31 Dieser definiert den Begriff „Verantwortlicher“ als „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

32 Gemäß Art. 4 Abs. 2 EUV.

Im vorliegenden Fall scheint die vom BVT-Untersuchungsausschuss ausgeübte politische Kontrolle als solche keine Tätigkeit darzustellen, die der Wahrung der nationalen Sicherheit dient oder derselben Kategorie zugeordnet werden kann. Vorbehaltlich einer Überprüfung durch das vorlegende Gericht ist diese Tätigkeit folglich nicht vom Anwendungsbereich der DSGVO ausgenommen.

Allerdings kann ein parlamentarischer Untersuchungsausschuss Zugang zu personenbezogenen Daten haben, die aus Gründen der nationalen Sicherheit besonders zu schützen sind. In diesem Zusammenhang können die sich aus der DSGVO ergebenden Rechte und Pflichten im Wege von Gesetzgebungsmaßnahmen beschränkt werden, um u. a. die nationale Sicherheit zu gewährleisten[33]. Auf dieser Grundlage können also Beschränkungen in Bezug auf die Erhebung personenbezogener Daten, die Unterrichtung der betroffenen Personen und ihren Zugang zu diesen Daten oder deren Offenlegung an andere Personen als den Verantwortlichen ohne Zustimmung der betroffenen Personen gerechtfertigt werden, soweit solche Beschränkungen den Wesensgehalt der Grundrechte und Grundfreiheiten der betroffenen Personen wahren und eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellen.

Der Gerichtshof führt jedoch aus, dass sich aus den ihm vorliegenden Informationen nicht ergibt, dass der BVT-Untersuchungsausschuss dargetan hätte, dass die Offenlegung der personenbezogenen Daten der betroffenen Person für die Gewährleistung der nationalen Sicherheit erforderlich gewesen sei und auf einer dafür vorgesehenen nationalen Gesetzgebungsmaßnahme beruht habe. Dies wird gegebenenfalls vom vorlegenden Gericht zu überprüfen sein.

2. Begriff „personenbezogene Daten“

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

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

[33] Gemäß Art. 23 DSGVO.

einem Computer und dem vom Internetzugangsanbieter verwendeten physischen Netzanschluss herzustellen. Die aufgezeichneten Daten bieten für sich genommen dem Anbieter nicht die Möglichkeit, den Nutzer zu bestimmen. Er verfügt jedoch über Zusatzinformationen, die – in Verbindung mit dieser IP-Adresse – eine Bestimmung des Nutzers ermöglichen würden.

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

Der Gerichtshof hat zunächst ausgeführt, dass 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.

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.

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.

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

Viertens hat der Gerichtshof entschieden, dass die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung und etwaige Anmerkungen des Prüfers dazu somit – insbesondere im Hinblick auf ihre Richtigkeit und die Notwendigkeit ihrer

Aufbewahrung – einer Überprüfung im Sinne von Art. 6 Abs. 1 Buchst. d und e der Richtlinie 95/46 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.

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.

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. 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.

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.1 „Anwendungsbereich der allgemeinen Regelung“) hatte Gerichtshof 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.

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

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 familiärer Tätigkeiten vorgenommen werden, im Sinne von Art. 3 Abs. 2 zweiter Gedankenstrich der Richtlinie handelt.

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[34] 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“[35] darstellt, für die die DSGVO wegen der besonderen Sensibilität der betreffenden Daten einen erhöhten Schutz vorsieht.

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.

---

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

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[36]. 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.

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[37]. Die CSDD kann nämlich bei der entsprechenden Übermittlung nicht als eine solche „zuständige Behörde“[38] angesehen werden.

Um zu bestimmen, ob der Zugang zu personenbezogenen Daten über Verkehrsverstöße, etwa Strafpunkten, eine Verarbeitung personenbezogener Daten über „Straftaten“[39] 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 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

---

36 Art. 2 Abs. 2 Buchst. a DSGVO.

37 Art. 2 Abs. 2 Buchst. d DSGVO.

38 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).

39 Art. 10 DSGVO.

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.

Urteil vom 5. Dezember 2023 (Große Kammer), Nacionalinis visuomenės sveikatos centras (C-683/21,* EU:C:2023:949*)

Im Jahr 2020 beschlossen die litauischen Behörden, den Erwerb einer mobilen IT-Anwendung zu organisieren, um so die Covid-19-Pandemie besser zu bewältigen. Diese Anwendung sollte zur epidemiologischen Überwachung beitragen und es ermöglichen, die Daten der dem Covid-19-Virus ausgesetzten Personen zu erfassen und zu überwachen.

Zu diesem Zweck wandte sich das Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Nationales Zentrum für öffentliche Gesundheit beim Gesundheitsministerium, Litauen, im Folgenden: NZÖG), das mit diesem Erwerb beauftragt worden war, an das Unternehmen UAB „IT sprendimai sėkmei“ (im Folgenden: ITSS) und forderte es auf, eine solche mobile Anwendung zu entwickeln. In der Folge sandten Mitarbeiter des NZÖG E- Mails an das Unternehmen, in denen es insbesondere um die Fragen ging, die in dieser Anwendung gestellt werden sollten.

Im April und Mai 2020 wurde die von ITSS entwickelte Anwendung für die Öffentlichkeit freigegeben. Sie wurde von 3 802 Personen genutzt, die verschiedene, von der Anwendung geforderte personenbezogene Daten bereitstellten. Aufgrund fehlender Finanzmittel vergab das NZÖG jedoch keinen öffentlichen Auftrag zum offiziellen Erwerb dieser Anwendung an ITSS und beendete das entsprechende Verfahren.

Zwischenzeitlich leitete die nationale Aufsichtsbehörde eine Untersuchung betreffend die sich aus der Verwendung dieser Anwendung ergebende Verarbeitung personenbezogener Daten ein. Mit einem am Ende der Untersuchung ergangenen Beschluss verhängte die Aufsichtsbehörde Geldbußen sowohl gegen das NZÖG als auch gegen ITSS, die als gemeinsam Verantwortliche angesehen wurden.

Das NZÖG hat diesen Beschluss vor dem Vilniaus apygardos administracinis teismas (Regionales Verwaltungsgericht Vilnius, Litauen) angefochten, das Zweifel hinsichtlich der Auslegung mehrerer Bestimmungen der DSGVO hegt und dem Gerichtshof daher ein Vorabentscheidungsersuchen vorgelegt hat.

In seinem Urteil erläutert der Gerichtshof (Große Kammer) u. a. den Begriff „Verarbeitung“. Er weist hierzu darauf hin, dass die Verwendung von personenbezogenen Daten für IT-Tests im Zusammenhang mit einer mobilen Anwendung eine „Verarbeitung“ darstellt. Anders verhält es sich jedoch, wenn diese Daten in einer Weise anonymisiert wurden, dass die Person, auf die sich die Daten beziehen, nicht oder nicht mehr identifiziert werden kann, oder es sich um fiktive Daten handelt, die sich nicht auf eine existierende natürliche Person beziehen.

Zum einen ist es nämlich für die Frage, ob der Vorgang als „Verarbeitung“ einzustufen ist, ohne Belang, ob personenbezogene Daten für IT-Tests oder einen anderen Zweck verwendet werden. Zum anderen kann nur eine Verarbeitung, die personenbezogene Daten betrifft, als „Verarbeitung“ im Sinne der DSGVO eingestuft werden. Fiktive oder anonyme Daten sind dagegen keine personenbezogenen Daten.

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.

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 die 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.

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

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.

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.

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.

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.

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.

Urteil vom 5. Dezember 2023 (Große Kammer), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In dieser Rechtssache (vgl. auch Abschnitt II.3 „Begriff ‚Verarbeitung personenbezogener Daten'") stellt der Gerichtshof fest, dass eine Einrichtung, die ein Unternehmen damit beauftragt hat, eine mobile IT-Anwendung zu entwickeln, und in diesem Zusammenhang an der Entscheidung über die Zwecke und Mittel der mittels dieser Anwendung vorgenommenen Verarbeitung personenbezogener Daten mitwirkt, als Verantwortlicher[40] angesehen werden kann. Diese Feststellung wird nicht dadurch in Frage gestellt, dass die Einrichtung selbst keine personenbezogene Daten betreffenden Verarbeitungsvorgänge durchgeführt, keine ausdrückliche Einwilligung zur Durchführung der konkreten Verarbeitungsvorgänge oder zur Bereitstellung dieser mobilen Anwendung für die Öffentlichkeit gegeben und die mobile Anwendung nicht erworben hat, es sei denn, sie hat, bevor die Anwendung der Öffentlichkeit bereitgestellt wurde, dieser Bereitstellung und der sich daraus ergebenden Verarbeitung personenbezogener Daten ausdrücklich widersprochen.

6. Begriff „gemeinsam für die Verarbeitung Verantwortliche"

Urteil vom 5. Dezember 2023 (Große Kammer), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In dieser Rechtssache (vgl. auch die Abschnitte II.3 „Begriff ‚Verarbeitung personenbezogener Daten'" und II.5 „Begriff ‚für die Verarbeitung [personenbezogener Daten] Verantwortlicher'") weist der Gerichtshof darauf hin, dass die Einstufung von zwei Einrichtungen als gemeinsam Verantwortliche nicht voraussetzt, dass zwischen diesen Einrichtungen eine Vereinbarung über die Festlegung der Zwecke und Mittel der fraglichen Verarbeitung personenbezogener Daten oder eine Vereinbarung besteht, in der die Bedingungen der gemeinsamen Verantwortlichkeit für die Verarbeitung festgelegt sind. Zwar müssen gemeinsam Verantwortliche nach der DSGVO[41] in einer Vereinbarung festlegen, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt. Das Vorliegen einer solchen Vereinbarung stellt jedoch keine Voraussetzung für eine Einstufung von zwei oder mehr Einrichtungen als „gemeinsam Verantwortliche" dar, sondern eine Pflicht, die die DSGVO den gemeinsam Verantwortlichen, sobald sie als solche eingestuft sind, auferlegt, um die Einhaltung der ihnen obliegenden

[40] Im Sinne von Art. 4 Nr. 7 DSGVO.
[41] Art. 26 Abs. 1 DSGVO in Verbindung mit dem 79. Erwägungsgrund der DSGVO.

Anforderungen der DSGVO sicherzustellen. Diese Einstufung ergibt sich somit allein daraus, dass mehrere Einrichtungen an der Entscheidung über die Zwecke und Mittel der Verarbeitung mitgewirkt haben.

Zur gemeinsamen Entscheidung über die Zwecke und Mittel der Verarbeitung führt der Gerichtshof aus, dass die Mitwirkung der gemeinsam Verantwortlichen verschiedene Formen annehmen und sich sowohl aus einer gemeinsamen Entscheidung als auch aus mehreren, aber übereinstimmenden Entscheidungen ergeben kann. In letzterem Fall müssen sich diese Entscheidungen jedoch in einer Weise ergänzen, dass sich jede von ihnen konkret auf die Entscheidung über die Verarbeitungszwecke und - mittel auswirkt.

7. Voraussetzungen für die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

Urteil vom 11. November 2020, Orange Romania (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[42] 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[43]. Die Einwilligung wird bei Stillschweigen, bereits angekreuzten Kästchen oder Untätigkeit nicht gültig erteilt.

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.

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.

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

---

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

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.

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 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.

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

In diesem Urteil (vgl. 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.

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“[44], 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.

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 Dokumenten, wie dem nationalen Register für Fahrzeuge und Fahrzeugführer, als auch dem Recht auf Informationsfreiheit vor.

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.

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.

[44] 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“.

III. Verarbeitung personenbezogener Daten im Sinne der sektorbezogenen Regelung

1. Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation

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

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 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.

In diesem Zusammenhang hat der Gerichtshof erläutert, dass er im Urteil Tele2 Sverige und Watson u. a.[45] 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.

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.

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 et C-520/18, EU:C:2020:791)

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.

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

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

(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.

Sodann hat der Gerichtshof darauf hingewiesen, dass die Richtlinie 2002/58[46] 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[47], 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[48] beachten.

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

---

46 Art. 15 Abs. 1 und 3 der Richtlinie 2002/58.
47 Art. 5 Abs. 1 der Richtlinie 2002/58.
48 Insbesondere Art. 7, 8 und 11 sowie Art. 52 Abs. 1 der Charta.

Grundrechte dar, 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.

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.

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.

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.

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.

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[49].

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 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.[50] 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.

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

[49] 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.
[50] Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, Rn. 120).

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.

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 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.

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.

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.

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.

Urteil vom 5. April 2022 (Große Kammer), Commissioner of An Garda Síochána u. a. (C-140/20, EU:C:2022:258)

In der vorliegenden Rechtssache wurde das Vorabentscheidungsersuchen vom Supreme Court (Oberster Gerichtshof, Irland) im Rahmen eines Zivilverfahrens eingereicht, das von einer wegen eines in Irland begangenen Mordes zu lebenslanger Freiheitsstrafe verurteilten Person angestrengt wurde. Diese Person stellte die Vereinbarkeit bestimmter Vorschriften des nationalen Gesetzes über die Vorratsspeicherung von im Rahmen elektronischer Kommunikationen erzeugter Daten mit dem Unionsrecht in Abrede. Gemäß diesem Gesetz wurden Verkehrs- und Standortdaten im Zusammenhang mit Telefonanrufen des Beschuldigten von den Betreibern elektronischer Kommunikationsdienste gespeichert und den Polizeibehörden zugänglich gemacht. Die Zweifel, die das vorlegende Gericht äußerte, betrafen u. a. die Vereinbarkeit einer Regelung der allgemeinen und unterschiedslosen Vorratsspeicherung dieser Daten im Zusammenhang mit der Bekämpfung schwerer Kriminalität mit der Datenschutzrichtlinie für elektronische Kommunikation im Licht der Charta.

Mit seinem Urteil hat der Gerichtshof (Große Kammer) die auf das Urteil La Quadrature du Net u. a.[51] zurückgehende Rechtsprechung bestätigt und deren Tragweite präzisiert, indem er darauf hingewiesen hat, dass die allgemeine und unterschiedslose Vorratsspeicherung der Verkehrs- und Standortdaten im Zusammenhang mit elektronischer Kommunikation zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit unzulässig ist. Er hat außerdem die auf das Urteil Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation)[52] zurückgehende Rechtsprechung bestätigt, insbesondere hinsichtlich der Verpflichtung, den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten von einer vorherigen Kontrolle durch

[51] Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791).
[52] Urteil vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152).

ein Gericht oder eine gegenüber einem Polizeibeamten unabhängige Verwaltungsstelle abhängig zu machen.

Der Gerichtshof hat als Erstes festgestellt, dass die Datenschutzrichtlinie für elektronische Kommunikation im Licht der Charta Rechtsvorschriften entgegensteht, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrs- und der Standortdaten vorsehen. In Anbetracht zum einen der abschreckenden Wirkungen, die diese Speicherung auf die Ausübung der Grundrechte[53] haben kann, und zum anderen der Schwere des mit ihr verbundenen Eingriffs muss eine solche Speicherung in Bezug auf das durch diese Richtlinie geschaffene System nämlich die Ausnahme und nicht die Regel darstellen, so dass solche Daten nicht Gegenstand einer systematischen und kontinuierlichen Speicherung sein dürfen. Kriminalität – auch besonders schwere Kriminalität – kann nicht mit einer Bedrohung der nationalen Sicherheit gleichgesetzt werden, da eine solche Gleichsetzung eine Zwischenkategorie zwischen der nationalen Sicherheit und der öffentlichen Sicherheit einführen könnte, um auf die zweite Kategorie die Voraussetzungen der ersten Kategorie anzuwenden.

Dagegen steht die Datenschutzrichtlinie für elektronische Kommunikation im Licht der Charta Rechtsvorschriften nicht entgegen, die zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit 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, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Der Gerichtshof hat weiter ausgeführt, dass eine solche Maßnahme der Vorratsspeicherung in Bezug auf Orte oder Infrastrukturen, die regelmäßig von einer sehr großen Zahl von Personen frequentiert werden, oder auf strategische Orte wie Flughäfen, Bahnhöfe, Seehäfen oder Mautstellen es den zuständigen Behörden ermöglichen kann, zum Zweck der Bekämpfung schwerer Kriminalität Informationen über die Anwesenheit der Personen, die dort ein elektronisches Kommunikationsmittel benutzen, zu erlangen, und daraus Schlüsse über ihre Anwesenheit und ihre Tätigkeit an diesen Orten oder in diesen geografischen Gebieten zu ziehen. Jedenfalls kann das etwaige Bestehen von Schwierigkeiten bei der genauen Bestimmung der Fälle und Bedingungen, in bzw. unter denen eine gezielte Vorratsspeicherung durchgeführt werden kann, nicht rechtfertigen, dass Mitgliedstaaten eine allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten vorsehen.

Diese Richtlinie, ausgelegt im Licht der Charta, steht auch Rechtsvorschriften nicht entgegen, die zum gleichen Zweck für einen auf das absolut Notwendige begrenzten

[53] Die in den Art. 7 bis 11 der Charta verankerten Grundrechte.

Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, sowie der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen. Was diesen letztgenannten Gesichtspunkt anbelangt, so hat der Gerichtshof insbesondere klargestellt, dass weder die Datenschutzrichtlinie für elektronische Kommunikation noch irgendein anderer Unionsrechtsakt nationalen Rechtsvorschriften entgegenstehen, die die Bekämpfung schwerer Kriminalität zum Gegenstand haben und nach denen der Erwerb eines elektronischen Kommunikationsmittels wie einer vorausbezahlten SIM-Karte von der Überprüfung amtlicher Dokumente, die die Identität des Käufers belegen, und der Erfassung der sich daraus ergebenden Informationen durch den Verkäufer abhängig ist, wobei der Verkäufer gegebenenfalls verpflichtet ist, den zuständigen nationalen Behörden Zugang zu diesen Informationen zu gewähren.

Gleiches gilt auch für Rechtsvorschriften, die – ebenfalls zum Zweck der Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit – vorsehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben werden kann, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern (quick freeze). Nur die Bekämpfung schwerer Kriminalität und, a fortiori, der Schutz der nationalen Sicherheit sind nämlich geeignet, eine solche Speicherung zu rechtfertigen, sofern diese Maßnahme sowie der Zugang zu den auf Vorrat gespeicherten Daten die Grenzen des absolut Notwendigen einhalten. Eine solche Maßnahme der umgehenden Sicherung kann auf die Verkehrs- und Standortdaten anderer als der Personen erstreckt werden, die im Verdacht stehen, eine schwere Straftat oder eine Beeinträchtigung der nationalen Sicherheit geplant oder begangen zu haben, sofern diese Daten auf der Grundlage objektiver und nicht diskriminierender Kriterien zur Aufdeckung einer solchen Straftat oder einer solchen Beeinträchtigung der nationalen Sicherheit beitragen können. Dazu gehören die Daten des Opfers sowie seines sozialen oder beruflichen Umfelds.

Alle vorgenannten Rechtsvorschriften müssen allerdings durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen. Die verschiedenen Maßnahmen der Vorratsspeicherung der Verkehrs- und Standortdaten können je nach der Wahl des nationalen Gesetzgebers und unter Einhaltung der Grenzen des absolut Notwendigen zusammen angewandt werden.

Außerdem hat der Gerichtshof klargestellt, dass es mit der Hierarchie der dem Gemeinwohl dienenden Ziele, die eine Maßnahme nach der Datenschutzrichtlinie für elektronische Kommunikation rechtfertigen können, unvereinbar wäre, für die Zwecke der Bekämpfung schwerer Kriminalität Zugang zu solchen Daten zu gestatten, die allgemein und unterschiedslosen auf Vorrat gespeichert wurden, um einer ernsten

Bedrohung für die nationale Sicherheit zu begegnen. Dies liefe nämlich darauf hinaus, es zuzulassen, dass der Zugang für ein Ziel von geringerer Bedeutung als das Ziel, das die Speicherung rechtfertigte, nämlich der Schutz der nationalen Sicherheit, gerechtfertigt sein könnte, was die Gefahr begründen würde, dass das Verbot einer allgemeinen und unterschiedslosen Vorratsspeicherung zum Zweck der Bekämpfung schwerer Straftaten seine praktische Wirksamkeit verliert.

Als Zweites hat der Gerichtshof festgestellt, dass die Datenschutzrichtlinie für elektronische Kommunikation, ausgelegt im Licht der Charta, einer nationalen Regelung entgegensteht, nach der die zentralisierte Bearbeitung von Ersuchen um Zugang zu von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten, die von der Polizei im Rahmen der Ermittlung und Verfolgung schwerer Straftaten gestellt werden, einem Polizeibeamten obliegt, auch wenn dieser von einer innerhalb der Polizei eingerichteten Einheit, die bei der Wahrnehmung ihrer Aufgaben über einen gewissen Grad an Autonomie verfügt, unterstützt wird und seine Entscheidungen später gerichtlich überprüft werden können. Zum einen erfüllt ein solcher Beamter nämlich nicht die Erfordernisse der Unabhängigkeit und Unparteilichkeit, die für eine Verwaltungsbehörde gelten, die die vorherige Kontrolle bezüglich der Anträge der zuständigen nationalen Behörden auf Zugang zu den Daten ausübt, da er in Bezug auf diese Behörden nicht die Eigenschaft eines Dritten hat. Zum anderen kann die Entscheidung eines solchen Beamten zwar Gegenstand einer nachträglichen Kontrolle sein, doch kann diese Kontrolle eine unabhängige und – mit Ausnahme von hinreichend begründeten Eilfällen – vorherige Kontrolle nicht ersetzen.

Als Drittes schließlich hat der Gerichtshof seine Rechtsprechung bestätigt, wonach das Unionsrecht dem entgegensteht, dass ein nationales Gericht die Wirkungen einer ihm nach nationalem Recht in Bezug auf nationale Rechtsvorschriften, die den Betreibern elektronischer Kommunikationsdienste eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorschreiben, obliegenden Ungültigerklärung wegen Unvereinbarkeit dieser Rechtsvorschriften mit der Datenschutzrichtlinie für elektronische Kommunikation zeitlich begrenzt. Der Gerichtshof hat allerdings darauf hingewiesen, dass die Zulässigkeit der durch eine solche Vorratsspeicherung erlangten Beweismittel nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität dem nationalen Recht unterliegt.

Urteil vom 20. September 2022 (Große Kammer), VD und SR (C-339/20 und C-397/20, EU:C:2022:703)

Gegen VD und SR wurden auf Ermittlungen der Autorité des marchés financiers (AMF, Finanzaufsichtsbehörde, Frankreich) hin Strafverfahren wegen Insiderhandel, Hehlerei im Zusammenhang mit Insiderhandel, Beihilfe, Bestechung und Geldwäsche eingeleitet. Bei diesen Ermittlungen wurden von der AMF personenbezogene Daten betreffend Telefongespräche von VD und SR herangezogen, die im Rahmen der Erbringung von

Diensten der elektronischen Kommunikation auf der Grundlage des Code des postes et des communications électroniques (Gesetzbuch betreffend das Postwesen und die elektronische Kommunikation) generiert worden waren.

Da bei den Entscheidungen über die Eröffnung des Hauptverfahrens die von der AMF vorgelegten Verkehrsdaten verwertet wurden, legten VD und SR dagegen bei der Cour d'appel de Paris (Berufungsgericht Paris, Frankreich) jeweils ein Rechtsmittel ein. Sie rügten insbesondere einen Verstoß gegen Art. 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation im Licht der Art. 7, 8, 11 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta). Sie beriefen sich insbesondere auf die durch das Urteil Tele2 Sverige und Watson u. a[54] begründete Rechtsprechung. Die AMF habe sich bei der Erhebung der Daten zu Unrecht auf die in Rede stehenden innerstaatlichen Rechtsvorschriften gestützt. Diese Vorschriften seien, soweit sie eine allgemeine und unterschiedslose Vorratsspeicherung der Verbindungsdaten vorsähen, unionsrechtswidrig. Zudem werde in ihnen die Befugnis der Ermittler der AMF, gespeicherte Daten anzufordern, nicht begrenzt.

Die Rechtsmittel von VD und SR wurden von der Cour d'appel de Paris (Berufungsgericht Paris) mit Urteilen vom 20. Dezember 2018 bzw. 7. März 2019 zurückgewiesen. Die Cour d'appel de Paris (Berufungsgericht Paris) hat das Vorbringen von VD und SR hauptsächlich mit der Begründung zurückgewiesen, dass die zuständigen Behörden nach der Marktmissbrauchsverordnung[55] bestehende Datenverkehrsaufzeichnungen im Besitz eines Anbieters von Diensten der elektronischen Kommunikation anfordern könnten, wenn der begründete Verdacht eines Verstoßes gegen das Verbot von Insidergeschäften bestehe und wenn diese Aufzeichnungen für die Untersuchung eines solchen Verstoßes relevant sein könnten, soweit dies nach nationalem Recht zulässig sei.

VD und SR haben gegen diese Urteile bei der Cour de cassation (Kassationsgerichtshof, Frankreich), dem vorlegenden Gericht, jeweils Kassationsbeschwerde eingelegt.

Das vorlegende Gericht fragt sich in diesem Zusammenhang im Hinblick auf die gesetzliche Regelung, um die es in den Ausgangsverfahren geht, die zur Bekämpfung von Straftaten des Marktmissbrauchs, u. a. von Insidergeschäften, präventiv vorsieht, dass die Anbieter von Diensten der elektronischen Kommunikation die Verkehrsdaten ab dem Zeitpunkt der Speicherung ein Jahr lang allgemein und unterschiedslos auf Vorrat speichern, ob Art. 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation in Verbindung mit der Charta mit den Anforderungen von Art. 12 Abs. 2

---

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

55 Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission (ABl. 2014, L 173, S. 1).

Buchst. a und d der Marktmissbrauchsrichtlinie[56] und Art. 23 Abs. 2 Buchst. g und h der Marktmissbrauchsverordnung vereinbar ist. Für den Fall, dass der Gerichtshof zu der Einschätzung gelangen sollte, dass die Regelung über die Vorratsspeicherung der Verbindungsdaten, um die es in den Ausgangsverfahren geht, unionsrechtswidrig ist, fragt sich das vorlegende Gericht, ob die Wirkungen dieser Regelung vorläufig aufrechtzuerhalten seien, um Rechtsunsicherheit zu vermeiden und es zu ermöglichen, dass die zuvor erhobenen und auf Vorrat gespeicherten Daten zur Aufdeckung und Verfolgung von Insidergeschäften verwendet würden.

Mit seinem Urteil entscheidet der Gerichtshof (Große Kammer), dass es nicht zulässig ist, dass die Anbieter von Diensten der elektronischen Kommunikation die Verkehrsdaten zur Bekämpfung von Straftaten des Marktmissbrauchs ab dem Zeitpunkt der Speicherung ein Jahr lang präventiv allgemein und unterschiedslos auf Vorrat speichern. Außerdem hält der Gerichtshof an seiner Rechtsprechung fest, wonach das Unionsrecht dem entgegensteht, dass ein nationales Gericht die von ihm zu treffende Feststellung, dass unionsrechtswidrige innerstaatliche Rechtsvorschriften ungültig sind, in ihren zeitlichen Wirkungen beschränkt.

Der Gerichtshof stellt zunächst fest, dass bei der Auslegung einer Vorschrift des Unionsrechts neben dem Wortlaut auch der Kontext der Vorschrift und die Ziele zu berücksichtigen sind, die mit der Regelung verfolgt werden, zu der die Vorschrift gehört.

Was den Wortlaut der Vorschriften angeht, auf die in den Vorabentscheidungsersuchen Bezug genommen wird, stellt der Gerichtshof fest, dass in Art. 12 Abs. 2 Buchst. d der Marktmissbrauchsrichtlinie von der Befugnis der zuständigen Finanzaufsichtsbehörde die Rede ist, „bereits existierende Aufzeichnungen von Telefongesprächen und Datenübermittlungen anzufordern“, und in Art. 23 Abs. 2 Buchst. g und h der Marktmissbrauchsverordnung von der Befugnis dieser Behörde, „Datenverkehrsaufzeichnungen im Besitz von Wertpapierfirmen, Kreditinstituten oder Finanzinstituten“ bzw. „bestehende Datenverkehrsaufzeichnungen im Besitz einer Telekommunikationsgesellschaft …, soweit dies nach nationalem Recht zulässig ist“, anzufordern. Aus dem Wortlaut der Bestimmungen ergibt sich eindeutig, dass lediglich die Befugnis der AMF geregelt ist, die Daten, über die die betreffenden Anbieter verfügen, „anzufordern“, was einem Zugang zu diesen Daten entspricht. Auch, dass von „bestehenden“ Aufzeichnungen die Rede ist, die sich „im Besitz“ der betreffenden Anbieter befinden, deutet darauf hin, dass der Unionsgesetzgeber nicht die Möglichkeit des nationalen Gesetzgebers regeln wollte, eine Verpflichtung zur Vorratsspeicherung solcher Aufzeichnungen einzuführen. Diese Auslegung wird sowohl durch den Kontext der genannten Bestimmungen als auch durch die Ziele, die mit der Regelung verfolgt werden, zu der sie gehören, gestützt.

[56] Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates vom 28. Januar 2003 über Insider-Geschäfte und Marktmanipulation (Marktmissbrauch) (ABl. 2003, L 96, S. 16).

Zum Kontext der Bestimmungen, auf die sich die Vorlagefragen beziehen, stellt der Gerichtshof fest, dass der Unionsgesetzgeber nach dem Wortlaut der einschlägigen Bestimmungen der Marktmissbrauchsrichtlinie und der Marktmissbrauchsverordnung[57] die Mitgliedstaaten zwar verpflichten wollte, die erforderlichen Maßnahmen zu ergreifen, damit die zuständigen Finanzaufsichtsbehörden über eine Reihe wirksamer Instrumente, Befugnisse und Ressourcen und über die erforderlichen Aufsichts- und Untersuchungsbefugnisse verfügen, damit sie ihre Aufgaben wirksam erledigen können. In den genannten Bestimmungen sind aber weder eine Möglichkeit der Mitgliedstaaten, den Anbietern von Diensten der elektronischen Kommunikation zu diesem Zweck eine Verpflichtung zur allgemeinen und unterschiedslosen Vorratsspeicherung der Verkehrsdaten aufzuerlegen, noch die Bedingungen, unter denen die Daten von den Anbietern von Diensten der elektronischen Kommunikation auf Vorrat gespeichert werden müssten, um gegebenenfalls den zuständigen Behörden übermittelt zu werden, geregelt.

Was die Ziele angeht, die mit der in Rede stehenden Regelung verfolgt werden, stellt der Gerichtshof fest, dass sowohl aus der Marktmissbrauchsrichtlinie als auch aus der Marktmissbrauchsverordnung[58] hervorgeht, dass mit diesen Rechtsakten die Integrität der Finanzmärkte in der Union sichergestellt und das Vertrauen der Anleger in diese Märkte gestärkt werden soll, das insbesondere darauf beruht, dass die Anleger gleich behandelt werden und gegen die unzulässige Verwendung von Insiderinformationen geschützt werden. Das in den genannten Rechtsakten[59] normierte Verbot von Insidergeschäften soll somit die Gleichheit der Vertragspartner bei einem Börsengeschäft gewährleisten, indem es verhindert, dass einer von ihnen, der über eine Insiderinformation verfügt und deshalb einen Vorteil gegenüber den anderen Anlegern hat, daraus zum Nachteil der anderen, die diese Information nicht haben, einen Nutzen zieht. Zwar stellen Aufzeichnungen von Verbindungsdaten der Marktmissbrauchsverordnung[60] zufolge entscheidende und manchmal die einzigen Belege für die Aufdeckung und den Nachweis des Bestehens von Insiderhandel und Marktmanipulation dar. Die Marktmissbrauchsverordnung bezieht sich aber lediglich auf die Aufzeichnungen, die „im Besitz“ der Anbieter von Diensten der elektronischen Kommunikation sind, und auf die Befugnis der zuständigen Finanzaufsichtsbehörde, von den Anbietern von Diensten der elektronischen Kommunikation „bestehende“ Daten „anzufordern“. Aus ihr kann daher nicht abgeleitet werden, dass der Unionsgesetzgeber den Mitgliedstaaten mit ihr die Befugnis hätte einräumen wollen, den Anbietern von Diensten der elektronischen Kommunikation eine allgemeine Verpflichtung zur Vorratsspeicherung der Daten aufzuerlegen. Somit ist festzustellen, dass weder die Marktmissbrauchsrichtlinie noch die Marktmissbrauchsverordnung im Hinblick auf die

---

57 Art. 12 Abs. 1 der Richtlinie 2003/6 bzw. Art. 23 Abs. 3 der Verordnung Nr. 596/2014 im Licht des 62. Erwägungsgrundes dieser Verordnung.

58 Erwägungsgründe 2 und 12 der Richtlinie 2003/6 bzw. Art. 1 der Verordnung Nr. 596/2014 im Licht der Erwägungsgründe 2 und 24 dieser Verordnung.

59 Art. 2 Abs. 1 der Richtlinie 2003/6 und Art. 8 Abs. 1 der Verordnung Nr. 596/2014.

60 62. Erwägungsgrund der Verordnung Nr. 596/2014.

Ausübung der der zuständigen Finanzaufsichtsbehörde durch sie übertragenen Befugnisse eine Rechtsgrundlage für eine allgemeine Verpflichtung zur Aufbewahrung der Datenverkehrsaufzeichnungen im Besitz der Anbieter von Diensten der elektronischen Kommunikation bilden.

Sodann stellt der Gerichtshof fest, dass es sich bei der Datenschutzrichtlinie für elektronische Kommunikation um den Referenzrechtsakt im Bereich der Speicherung und allgemein der Verarbeitung personenbezogener Daten in der elektronischen Kommunikation handelt. Ihre Auslegung ist daher auch für die Datenverkehrsaufzeichnungen im Besitz der Anbieter von Diensten der elektronischen Kommunikation maßgeblich, die die zuständigen Finanzaufsichtsbehörden im Sinne der Marktmissbrauchsrichtlinie und der Marktmissbrauchsverordnung[61] bei Letzteren anfordern können. Für die Beurteilung der Frage, ob die Verarbeitung der Aufzeichnungen im Besitz der Anbieter von Diensten der elektronischen Kommunikation[62] zulässig ist, sind mithin die Voraussetzungen gemäß der Datenschutzrichtlinie für elektronische Kommunikation und die Auslegung dieser Richtlinie durch die Rechtsprechung des Gerichtshofs maßgeblich.

Der Gerichtshof gelangt deshalb zu dem Schluss, dass die Marktmissbrauchsrichtlinie und die Marktmissbrauchsverordnung in Verbindung mit der Datenschutzrichtlinie für elektronische Kommunikation im Licht der Charta einer gesetzlichen Regelung entgegenstehen, nach der die Anbieter von Diensten der elektronischen Kommunikation die Verkehrsdaten zur Bekämpfung von Straftaten des Marktmissbrauchs, u. a. von Insidergeschäften, präventiv für einen bestimmten Zeitraum, nämlich ein Jahr ab dem Zeitpunkt der Speicherung, allgemein und unterschiedslos auf Vorrat speichern.

Schließlich hält der Gerichtshof an seiner Rechtsprechung fest, wonach das Unionsrecht dem entgegensteht, dass ein nationales Gericht die nach nationalem Recht zu treffende Feststellung, dass innerstaatliche Rechtsvorschriften, mit denen die Anbieter von Diensten der elektronischen Kommunikation zur allgemeinen und unterschiedslosen Vorratsspeicherung der Verkehrsdaten verpflichtet werden und nach denen solche Daten ohne vorherige Genehmigung durch ein Gericht oder eine unabhängige Behörde an die zuständige Finanzaufsichtsbehörde übermittelt werden können, wegen ihrer Unvereinbarkeit mit der Datenschutzrichtlinie für elektronische Kommunikation im Licht der Charta ungültig sind, in ihren zeitlichen Wirkungen beschränkt. Der Gerichtshof weist jedoch darauf hin, dass die Verwertbarkeit von Beweisen, die durch eine solche Vorratsspeicherung von Daten erlangt wurden, nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten – vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität – dem nationalen Recht unterliegt. Der Effektivitätsgrundsatz verpflichtet ein nationales Strafgericht dazu, Informationen und

---

61 Art. 11 der Richtlinie 2003/6 bzw. Art. 22 der Verordnung Nr. 596/2014.

62 Im Sinne von Art. 12 Abs. 2 Buchst. d der Richtlinie 2003/6 und Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014.

Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung erlangt wurden, auszuschließen, sofern die betreffenden Personen nicht in der Lage sind, sachgerecht zu den Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen.

Urteil vom 30. April 2024 (Plenum), La Quadrature du Net u. a. (Personenbezogene Daten und Bekämpfung von Verletzungen der Rechte des geistigen Eigentums) (C-470/21, EU:C:2024:370)

Aufgrund eines Vorabentscheidungsersuchens des Conseil d'État (Staatsrat, Frankreich) hat das Plenum des Gerichtshofs seine Rechtsprechung zur Richtlinie 2002/58 fortentwickelt und Klarstellungen zum einen zu den Voraussetzungen vorgenommen, unter denen davon ausgegangen werden kann, dass eine allgemeine Vorratsspeicherung von IP- Adressen durch die Betreiber elektronischer Kommunikationsdienste nicht zu einem schweren Eingriff in die durch die Charta gewährleisteten Rechte auf Achtung des Privatlebens, auf den Schutz personenbezogener Daten und auf freie Meinungsäußerung[63] führt, und zum anderen zu der Möglichkeit einer Behörde, im Rahmen der Bekämpfung online begangener Verletzungen der Rechte des geistigen Eigentums Zugang zu bestimmten personenbezogenen Daten zu erhalten, die unter Einhaltung dieser Voraussetzungen auf Vorrat gespeichert wurden.

Im vorliegenden Fall haben vier Verbände beim Premier ministre (Premierminister, Frankreich) einen Antrag auf Aufhebung des Dekrets über die automatisierte Verarbeitung personenbezogener Daten[64] gestellt. Da ihr Antrag implizit abgelehnt wurde, erhoben sie beim Conseil d'État (Staatsrat, Frankreich) Klage auf Nichtigerklärung dieser impliziten ablehnenden Entscheidung. Sie machen geltend, das Dekret und die Bestimmungen, die seine Rechtsgrundlage bildeten[65], verstießen gegen das Unionsrecht.

Nach den französischen Rechtsvorschriften darf die Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (Hohe Behörde für die Verbreitung von Werken und den Schutz von Rechten im Internet, Hadopi), um die Verantwortlichen für online begangene Verletzungen des Urheberrechts oder verwandter Schutzrechte

63 Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).

64 Décret no 2010- 236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331- 29 du code de la propriété intellectuelle dénommé „Système de gestion des mesures pour la protection des œuvres sur Internet" (Dekret Nr. 2010-236 vom 5. März 2010 über die nach Art. L. 331-29 des Gesetzbuchs über das geistige Eigentum gestattete automatisierte Verarbeitung personenbezogener Daten mit der Bezeichnung „System zur Verwaltung von Maßnahmen zum Schutz von Werken im Internet") (JORF Nr. 56 vom 7. März 2010, Text Nr. 19) in der durch das Décret no 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (Dekret Nr. 2017-924 vom 6. Mai 2017 über die Verwaltung von Urheberrechten und verwandten Schutzrechten durch eine Verwertungsgesellschaft und zur Änderung des Gesetzbuchs über das geistige Eigentum) (JORF Nr. 109 vom 10. Mai 2017, Text Nr. 176) geänderten Fassung.

65 Insbesondere Art. L. 331-21 Abs. 3 bis 5 des Code de la propriété intellectuelle (Gesetzbuch über das geistige Eigentum).

identifizieren zu können, auf bestimmte Daten zugreifen, die von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert werden müssen. Dabei handelt es sich um die Identitätsdaten einer Person, die ihrer zuvor von Einrichtungen der Rechteinhaber gesammelten IP- Adresse zuzuordnen sind. Sobald der Inhaber einer für solche rechtsverletzende Aktivitäten genutzten IP- Adresse identifiziert wurde, führt die Hadopi das Verfahren der „abgestuften Reaktion“ durch. Konkret ist sie befugt, an diese Person zwei Empfehlungen zu richten, die Warnungen gleichkommen, und, falls die Aktivitäten fortdauern, ein Schreiben, in dem ihr mitgeteilt wird, dass ihre Aktivitäten strafrechtlich verfolgt werden können. Schließlich ist die Hadopi berechtigt, die Staatsanwaltschaft mit der Verfolgung dieser Person zu befassen[66].

In diesem Kontext ersucht der Conseil d’État (Staatsrat) den Gerichtshof um die Auslegung der Datenschutzrichtlinie für elektronische Kommunikation im Licht der Charta[67].

Erstens hebt der Gerichtshof hinsichtlich der Vorratsspeicherung von Identitätsdaten und der ihnen zuzuordnenden IP- Adressen hervor, dass nicht jede allgemeine und unterschiedslose Vorratsspeicherung von IP- Adressen zwangsläufig einen schweren Eingriff in die durch die Charta garantierten Rechte auf Achtung des Privatlebens, auf Schutz personenbezogener Daten und auf freie Meinungsäußerung darstellt.

Die Pflicht, eine solche Vorratsspeicherung sicherzustellen, kann durch das Ziel der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt sein, wenn tatsächlich ausgeschlossen ist, dass diese Speicherung schwere Eingriffe in das Privatleben des Betroffenen zur Folge haben kann, die darauf beruhen, dass insbesondere durch eine Verknüpfung der IP- Adressen mit einem Satz von Verkehrs- oder Standortdaten die Möglichkeit besteht, genaue Schlüsse in Bezug auf ihn zu ziehen.

Daher muss sich ein Mitgliedstaat, der den Betreibern elektronischer Kommunikationsdienste eine solche Pflicht auferlegen möchte, vergewissern, dass die Modalitäten der Vorratsspeicherung dieser Daten ausschließen, dass genaue Schlüsse auf das Privatleben der Betroffenen gezogen werden können.

Dabei müssen die Modalitäten der Vorratsspeicherung deren Struktur selbst betreffen, die im Wesentlichen so gestaltet sein muss, dass eine wirksame strikte Trennung der verschiedenen Kategorien auf Vorrat gespeicherter Daten gewährleistet ist. Somit müssen die nationalen Vorschriften über diese Modalitäten sicherstellen, dass jede Datenkategorie, einschließlich der Identitätsdaten und der IP-Adressen, völlig getrennt von den übrigen Kategorien auf Vorrat gespeicherter Daten gespeichert wird und dass eine wirksame strikte Trennung durch eine abgesicherte und zuverlässige

66 Zum 1. Januar 2022 fusionierte die Hadopi mit dem Conseil supérieur de l’audiovisuel (Aufsichtsbehörde für die audiovisuellen Medien, CSA), einer anderen unabhängigen Behörde, zur Autorité de régulation de la communication audiovisuelle et numérique (Regulierungsbehörde für die audiovisuelle und digitale Kommunikation, ARCOM). Das Verfahren der abgestuften Reaktion blieb jedoch im Wesentlichen unverändert.

67 Art. 15 Abs. 1 der Richtlinie 2002/58.

Datenverarbeitungseinrichtung stattfindet. Außerdem dürfen die Regeln, soweit sie die Möglichkeit vorsehen, die auf Vorrat gespeicherten IP- Adressen mit der Identität des Betroffenen zu verknüpfen, eine solche Verknüpfung nur unter Verwendung eines leistungsfähigen technischen Verfahrens erlauben, das die Wirksamkeit der strikten Trennung dieser Datenkategorien nicht in Frage stellt. Die Zuverlässigkeit der Trennung muss regelmäßig Gegenstand einer Kontrolle durch eine dritte Behörde sein. Soweit im anwendbaren nationalen Recht solche strengen Anforderungen vorgesehen sind, kann der Eingriff, der sich aus dieser Speicherung der IP- Adressen ergibt, nicht als „schwer" eingestuft werden.

Der Gerichtshof kommt daher zu dem Ergebnis, dass die Datenschutzrichtlinie für elektronische Kommunikation im Licht der Charta einen Mitgliedstaat nicht daran hindert, mit dem Ziel der Bekämpfung von Straftaten im Allgemeinen eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung von IP- Adressen aufzustellen, sofern es eine gesetzliche Regelung gibt, die gewährleistet, dass keine Kombination von Daten genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert werden, zulassen wird, und sofern die Dauer der Speicherung nicht über das absolut Notwendige hinausgeht.

Zweitens entscheidet der Gerichtshof in Bezug auf den Zugang zu Identitätsdaten, die IP- Adressen zuzuordnen sind, dass die Datenschutzrichtlinie für elektronische Kommunikation im Licht der Charta grundsätzlich einer nationalen Regelung nicht entgegensteht, mit der einer Behörde Zugang zu diesen Daten, die von den Betreibern elektronischer Kommunikationsdienste wirksam strikt getrennt auf Vorrat gespeichert wurden, allein deshalb gewährt wird, damit die Behörde die Inhaber dieser Adressen identifizieren kann, die im Verdacht stehen, für Verletzungen des Urheberrechts und verwandter Schutzrechte im Internet verantwortlich zu sein, und Maßnahmen gegen sie ergreifen kann. In einem solchen Fall muss die nationale Regelung es den Bediensteten, die über einen solchen Zugang verfügen, untersagen, erstens Informationen über den Inhalt der von den Inhabern der IP- Adressen konsultierten Dateien – außer zum alleinigen Zweck der Befassung der Staatsanwaltschaft – in welcher Form auch immer offenzulegen, zweitens die von diesen Personen besuchten Internetseiten nachzuverfolgen und drittens die IP- Adressen zu anderen Zwecken als dem des Erlasses derartiger Maßnahmen zu nutzen.

In diesem Kontext weist der Gerichtshof insbesondere darauf hin, dass die Freiheit der Meinungsäußerung und die Vertraulichkeit personenbezogener Daten zwar vorrangige Anliegen sind, doch sind diese Grundrechte nicht absolut. Im Rahmen einer Abwägung der in Rede stehenden Rechte und Interessen müssen sie nämlich bisweilen hinter anderen Grundrechten und Erfordernissen des Allgemeininteresses wie der Verteidigung der öffentlichen Ordnung und der Verhütung von Straftaten oder dem Schutz der Rechte und Freiheiten anderer zurücktreten. Dies ist insbesondere dann der Fall, wenn die diesen vorrangigen Anliegen beigemessene Priorität geeignet ist, die Wirksamkeit strafrechtlicher Ermittlungen zu beeinträchtigen, etwa indem die

tatsächliche Identifizierung eines Straftäters und die Verhängung einer Sanktion gegen ihn unmöglich gemacht oder übermäßig erschwert werden.

Im gleichen Kontext verweist der Gerichtshof ferner auf seine Rechtsprechung, wonach bei der Bekämpfung online begangener Straftaten, mit denen Urheberrechte oder verwandte Schutzrechte verletzt werden, der Umstand, dass der Zugang zu den IP- Adressen die einzige Ermittlungsmaßnahme darstellen kann, die eine Identifizierung der betreffenden Person ermöglicht, dafür spricht, dass die Vorratsspeicherung dieser Adressen und der Zugang zu ihnen zur Erreichung des verfolgten Ziels zwingend erforderlich sind und daher dem Erfordernis der Verhältnismäßigkeit entsprechen. Würde ein solcher Zugang nicht gewährt, bestünde im Übrigen eine echte Gefahr der systemischen Straflosigkeit von Straftaten, die online begangen werden oder deren Begehung oder Vorbereitung durch die Merkmale des Internets erleichtert wird. Das Bestehen einer solchen Gefahr ist ein relevanter Umstand, wenn im Rahmen einer Abwägung der verschiedenen betroffenen Rechte und Interessen beurteilt wird, ob ein Eingriff in die Rechte auf Achtung des Privatlebens, auf Schutz personenbezogener Daten und auf freie Meinungsäußerung eine gemessen am Ziel der Bekämpfung von Straftaten verhältnismäßige Maßnahme ist.

Drittens führt der Gerichtshof zu der Frage, ob der Zugang der Behörde zu Identitätsdaten, die einer IP- Adresse zuzuordnen sind, von einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängig gemacht werden muss, aus, dass eine solche Kontrolle geboten ist, wenn dieser Zugang im Kontext einer nationalen Regelung die Gefahr eines schweren Eingriffs in die Grundrechte des Betroffenen in dem Sinne birgt, dass er es der Behörde ermöglichen könnte, genaue Schlüsse auf das Privatleben des Betroffenen zu ziehen und gegebenenfalls sein detailliertes Profil zu erstellen. Umgekehrt besteht dieses Erfordernis einer vorherigen Kontrolle nicht, wenn der Eingriff in die Grundrechte nicht als schwerwiegend eingestuft werden kann.

Insoweit stellt der Gerichtshof klar, dass dann, wenn eine Vorratsspeicherung eingeführt wird, die eine wirksame strikte Trennung der verschiedenen Kategorien auf Vorrat gespeicherter Daten gewährleistet, der Zugang der Behörde zu den Identitätsdaten, die IP- Adressen zuzuordnen sind, im Prinzip nicht vom Erfordernis einer vorherigen Kontrolle abhängt. Ein solcher Zugang allein zu dem Zweck, den Inhaber einer IP- Adresse zu identifizieren, stellt nämlich in der Regel keinen schweren Eingriff in die genannten Rechte dar.

Der Gerichtshof schließt jedoch nicht aus, dass in atypischen Situationen die Gefahr besteht, dass die Behörde in einem Verfahren wie dem im Ausgangsverfahren in Rede stehenden Verfahren der abgestuften Reaktion genaue Schlüsse auf das Privatleben der betreffenden Person ziehen könnte, insbesondere wenn diese Person wiederholt oder in großem Umfang in Peer-to-Peer-Netzen Aktivitäten, die Urheberrechte oder verwandte Schutzrechte verletzen, im Zusammenhang mit geschützten Werken

besonderer Arten entfaltet, durch die Informationen, unter Umständen sensibler Art, über das Privatleben dieser Person offenbar werden können.

Im vorliegenden Fall kann ein Inhaber einer IP- Adresse in besonderem Maß einer solchen Gefahr ausgesetzt sein, wenn die Behörde darüber zu entscheiden hat, ob sie die Staatsanwaltschaft mit seiner Verfolgung befasst. Die Intensität der Verletzung des Rechts auf Achtung des Privatlebens kann nämlich allmählich zunehmen, während das Verfahren der abgestuften Reaktion, das als sequentieller Prozess abläuft, die verschiedenen Stufen durchläuft, aus denen es besteht. Der Zugang der zuständigen Behörde zu allen im Lauf der verschiedenen Stufen dieses Verfahrens zusammengetragenen Daten über die betreffende Person kann es ermöglichen, genaue Schlüsse auf ihr Privatleben zu ziehen. Deshalb muss die nationale Regelung eine vorherige Kontrolle vorsehen, die erfolgen muss, bevor die Behörde die Identitätsdaten mit einem solchen Datensatz verknüpfen kann und vor der etwaigen Versendung des Notifizierungsschreibens, mit dem festgestellt wird, dass diese Person Handlungen vorgenommen hat, die strafrechtlich verfolgt werden können. Die Kontrolle muss überdies die Wirksamkeit des Verfahrens der abgestuften Reaktion wahren, indem sie es insbesondere ermöglicht, Fälle einer etwaigen Wiederholung der fraglichen Zuwiderhandlung zu identifizieren. Zu diesem Zweck muss das Verfahren so organisiert und strukturiert sein, dass die Identitätsdaten einer Person, die den zuvor im Internet gesammelten IP- Adressen zuzuordnen sind, von den bei der zuständigen Behörde mit der Prüfung des Sachverhalts betrauten Personen nicht automatisch mit Elementen verknüpft werden können, über die die Behörde bereits verfügt und die es ermöglichen könnten, genaue Schlüsse auf das Privatleben dieser Person zu ziehen.

Zum Gegenstand der vorherigen Kontrolle stellt der Gerichtshof ferner fest, dass in Fällen, in denen die betreffende Person im Verdacht steht, eine Zuwiderhandlung begangen zu haben, die zu den Straftaten im Allgemeinen gehört, das mit dieser Kontrolle betraute Gericht oder die mit ihr betraute unabhängige Verwaltungsstelle den Zugang verweigern muss, wenn er es der Behörde erlauben würde, genaue Schlüsse auf das Privatleben der betreffenden Person zu ziehen. Dagegen sollte in Fällen, in denen die betreffende Person im Verdacht steht, Delikte begangen zu haben, in denen der betreffende Mitgliedstaat die Beeinträchtigung eines Grundinteresses der Gesellschaft sieht und die er daher der schweren Kriminalität zurechnet, auch dann ein Zugang gewährt werden, wenn er es erlaubt, solche genauen Schlüsse zu ziehen.

Der Gerichtshof stellt zudem klar, dass eine vorherige Kontrolle in keinem Fall vollständig automatisiert sein kann, da eine solche Kontrolle bei strafrechtlichen Ermittlungen eine Abwägung zwischen den berechtigten Interessen im Zusammenhang mit der Bekämpfung der Kriminalität einerseits sowie der Achtung des Privatlebens und des Schutzes personenbezogener Daten andererseits erfordert. Diese Abwägung erfordert das Tätigwerden einer natürlichen Person, das umso notwendiger ist, als der automatisierte Ablauf und der große Umfang der in Rede stehenden Datenverarbeitung Gefahren für das Privatleben mit sich bringen.

Der Gerichtshof kommt daher zu dem Ergebnis, dass die Möglichkeit für die bei der Behörde mit der Prüfung des Sachverhalts betrauten Personen, Identitätsdaten einer Person, die einer IP- Adresse zuzuordnen sind, mit Dateien zu verknüpfen, die Elemente enthalten, denen sich der Titel geschützter Werke entnehmen lässt, deren Bereitstellung im Internet die Sammlung der IP- Adressen durch Einrichtungen der Rechteinhaber gerechtfertigt hat, in Fällen der erneuten Entfaltung einer Aktivität, mit der dieselbe Person Urheberrechte oder verwandte Schutzrechte verletzt, von einer Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängig gemacht werden muss. Diese Kontrolle darf nicht vollständig automatisiert sein und muss vor einer solchen Verknüpfung erfolgen, da diese es in derartigen Fällen ermöglichen kann, genaue Schlüsse auf das Privatleben der Person zu ziehen, deren IP- Adresse für Aktivitäten genutzt wurde, die möglicherweise Urheberrechte oder verwandte Schutzrechte verletzen.

Viertens schließlich stellt der Gerichtshof fest, dass das von der Behörde verwendete Datenverarbeitungssystem in regelmäßigen Abständen einer Kontrolle durch eine unabhängige Stelle unterzogen werden muss, bei der es sich im Verhältnis zu dieser Behörde um einen Dritten handelt. Diese Kontrolle dient zur Überprüfung der Integrität des Systems, einschließlich wirksamer Garantien zum Schutz vor den Gefahren eines missbräuchlichen oder unberechtigten Zugangs zu den Daten und ihrer missbräuchlichen oder unberechtigten Nutzung, sowie seiner Wirksamkeit und Zuverlässigkeit bei der Aufdeckung etwaiger Verstöße.

In diesem Rahmen stellt der Gerichtshof fest, dass im vorliegenden Fall die automatisierte Verarbeitung personenbezogener Daten durch die Behörde auf der Grundlage der Informationen über die von den Einrichtungen der Rechteinhaber festgestellten Nachahmungen eine Reihe falsch positiver Ergebnisse mit sich bringen kann sowie vor allem die Gefahr, dass eine potenziell sehr große Zahl von Daten Dritter zu missbräuchlichen oder unrechtmäßigen Zwecken zweckentfremdet wird; dies erklärt die Notwendigkeit einer solchen Kontrolle. Außerdem fügt er hinzu, dass bei dieser Verarbeitung die besonderen Vorschriften zum Schutz personenbezogener Daten der Richtlinie 2016/680 eingehalten werden müssen. Im vorliegenden Fall ist die Behörde, auch wenn sie im Rahmen des Verfahrens der abgestuften Reaktion nicht über eigene Entscheidungsbefugnisse verfügt, nämlich als eine an der Verhütung und Ermittlung von Straftaten beteiligte „Behörde“ einzustufen und fällt daher in den Anwendungsbereich dieser Richtlinie. Somit müssen die an einem solchen Verfahren beteiligten Personen in den Genuss einer Reihe durch die Richtlinie 2016/680 vorgeschriebener materieller und prozeduraler Garantien kommen, wobei es Sache des vorlegenden Gerichts ist, zu prüfen, ob sie in den nationalen Rechtsvorschriften vorgesehen sind.

2. Verarbeitung personenbezogener Daten im Strafrecht

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 desvorlegenden 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[68] 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 Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in Strafsachen[69] verstoße

[68] 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).

[69] 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).

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.

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[70] 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[71]. 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.

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[72].

---

70 Vgl. Art. 2 Abs. 1 und Art. 3 Nr. 2 der Richtlinie 2016/680.
71 Vgl. Art. 4 Abs. 1 Buchst. b und Art. 8 Abs. 1 der Richtlinie 2016/680.
72 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.

Urteil vom 21. Juni 2022 (Große Kammer), Ligue des droits humains (C-817/19, EU:C:2022:491)

In dieser Rechtssache (vgl. auch Abschnitt I.1 „Vereinbarkeit des abgeleiteten Unionsrechts mit dem Recht auf Schutz personenbezogener Daten“) gibt der Gerichtshof im Anschluss an die Feststellung der Gültigkeit der PNR-Richtlinie Erläuterungen zur Auslegung einiger ihrer Bestimmungen[73].

Erstens führt er aus, dass in der Richtlinie die mit der Verarbeitung von PNR-Daten verfolgten Ziele abschließend aufgezählt werden. Daher steht sie nationalen Rechtsvorschriften entgegen, nach denen die Verarbeitung der PNR-Daten zu anderen Zwecken als zur Bekämpfung terroristischer Straftaten und schwerer Kriminalität zulässig ist. Somit sind nationale Rechtsvorschriften, die als Zweck der Verarbeitung der PNR-Daten überdies die Beaufsichtigung der erwähnten Aktivitäten durch die Nachrichten- und Sicherheitsdienste zulassen, geeignet, den abschließenden Charakter dieser Aufzählung zu missachten. Desgleichen darf das durch die PNR-Richtlinie geschaffene System nicht zum Zweck der Verbesserung der Grenzkontrollen und der Bekämpfung illegaler Einwanderung herangezogen werden. Daraus folgt ferner, dass die PNR-Daten nicht in einer einheitlichen Datenbank gespeichert werden dürfen, die zur Verfolgung sowohl der Ziele der PNR-Richtlinie als auch anderer Ziele konsultiert werden kann.

Zweitens erläutert der Gerichtshof den Begriff der unabhängigen nationalen Behörde, die für die Prüfung, ob die Bedingungen für die Offenlegung der PNR-Daten zum Zweck ihrer nachträglichen Überprüfung erfüllt sind, und für die Genehmigung ihrer Offenlegung zuständig ist. Insbesondere darf die als PNR-Zentralstelle errichtete Behörde diese Aufgabe nicht wahrnehmen, da sie gegenüber der den Zugriff auf die Daten begehrenden Behörde nicht die Eigenschaft eines Dritten hat. Das Personal der PNR-Zentralstelle kann nämlich aus Mitarbeitern bestehen, die von Behörden abgeordnet wurden, die befugt sind, einen solchen Zugriff zu beantragen, so dass die

[73] Insbesondere von Art. 2 („Anwendung [der] Richtlinie auf EU-Flüge“), Art. 6 („Verarbeitung der PNR-Daten“) und Art. 12 („Speicherfrist und Depersonalisierung“) der PNR-Richtlinie.

PNR-Zentralstelle zwangsläufig mit diesen Behörden verbunden ist. Daher steht die PNR-Richtlinie nationalen Rechtsvorschriften entgegen, nach denen die als PNR-Zentralstelle errichtete Behörde zugleich die für die Genehmigung der Offenlegung der PNR-Daten nach Ablauf der Frist von sechs Monaten ab ihrer Übermittlung an die PNR-Zentralstelle zuständige nationale Behörde ist.

Drittens entscheidet der Gerichtshof in Bezug auf die Speicherfrist der PNR-Daten, dass Art. 12 der PNR-Richtlinie im Licht der Art. 7 und 8 sowie von Art. 52 Abs. 1 der Charta nationalen Rechtsvorschriften entgegensteht, die eine allgemeine, unterschiedslos für alle Fluggäste geltende Speicherfrist dieser Daten von fünf Jahren vorsehen.

Dazu führt der Gerichtshof aus, dass sich nach Ablauf der ursprünglichen sechsmonatigen Speicherfrist die Speicherung von PNR-Daten nicht auf das absolut Notwendige beschränkt, wenn sie sich auf Fluggäste bezieht, bei denen weder die Vorabüberprüfung noch etwaige Überprüfungen während der ursprünglichen sechsmonatigen Speicherfrist oder irgendein anderer Umstand objektive Anhaltspunkte – wie die Tatsache, dass die PNR-Daten der betreffenden Fluggäste im Rahmen der Vorabüberprüfung zu einem überprüften Treffer führten – geliefert haben, die eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit ihrer Flugreise belegen können. Während des ursprünglichen Zeitraums von sechs Monaten überschreitet die Speicherung der PNR-Daten aller Fluggäste, für die das durch die PNR-Richtlinie geschaffene System gilt, dagegen grundsätzlich nicht die Grenzen des absolut Notwendigen.

Viertens befasst sich der Gerichtshof damit, ob die Anwendung der PNR-Richtlinie zur Bekämpfung terroristischer Straftaten und schwerer Kriminalität auf andere Arten der Personenbeförderung innerhalb der Union erstreckt werden kann. Er kommt zu dem Ergebnis, dass die Richtlinie, im Licht von Art. 3 Abs. 2 EUV, Art. 67 Abs. 2 AEUV und Art. 45 der Charta, einem System entgegensteht, wonach die PNR-Daten aller Beförderungen mit anderen Mitteln innerhalb der Union übermittelt und verarbeitet werden, ohne dass der betreffende Mitgliedstaat mit einer realen und aktuellen oder vorhersehbaren terroristischen Bedrohung konfrontiert ist. In einer solchen Situation muss die Anwendung des durch die PNR-Richtlinie geschaffenen Systems – wie bei den EU-Flügen – auf die PNR-Daten von Beförderungen beschränkt werden, die insbesondere bestimmte Verbindungen, bestimmte Reisemuster oder bestimmte Bahnhöfe oder Seehäfen betreffen, für die es Anhaltspunkte gibt, die seine Anwendung rechtfertigen können. Es ist Sache des betreffenden Mitgliedstaats, die Beförderungen, für die es solche Anhaltspunkte gibt, auszuwählen und sie nach Maßgabe der Entwicklung der Bedingungen, die ihre Auswahl gerechtfertigt haben, regelmäßig zu überprüfen.

IV. Übermittlung personenbezogener Daten in Drittländer des données à caractère personnel vers des pays tiers

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

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.

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.

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

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 [74] festgestellt habe, dass die Vereinigten Staaten im Rahmen der Safe-Harbor-Regelung[75] hinsichtlich der übermittelten personenbezogenen Daten ein angemessenes Schutzniveau gewährleisteten.

Vor diesem Hintergrund wurde der Gerichtshof vom High Court (Hoher Gerichtshof, Irland) mit einem Vorabentscheidungsersuchen zur Auslegung von Art. 25 Abs. 6 der Richtlinie 95/46, 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.

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. Der Gerichtshof hat festgestellt, dass die Ungültigkeit der Art. 1 und 3 der Entscheidung 2000/520 die Gültigkeit der gesamten Entscheidung berührt.

---

[74] 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).

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

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.

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. 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. 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.

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.

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).

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.

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.

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 Verwendung der Fluggastdatensätze zur Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität 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 Fluggastdatensätze 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.

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

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[76]. 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[77]. 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[78].

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 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[79] festgestellt, dass die Vereinigten Staaten ein angemessenes Schutzniveau gewährleisteten. Mit Urteil

[76] Art. 45 DSGVO.
[77] Art. 46 Abs. 1 und 2 Buchst. c DSGVO.
[78] Art. 49 DSGVO.
[79] 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).

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)[80].

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[81] 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[82].

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.

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

---

80 Urteil des Gerichtshofs vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650.

81 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).

82 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).

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.

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.

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.

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.

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.

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.

V. Der Schutz personenbezogener Daten im Internet protection des données à caractère personnel sur Internet

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

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

In diesem Urteil (vgl. auch die Abschnitte II.1 „Anwendungsbereich der allgemeinen Regelung“ und 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.

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. 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. 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.

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.

2. Verarbeitung personenbezogener Daten und Rechte des geistigen Eigentums

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

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“)[83], 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft[84], 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums[85] und 2002/58 es den Mitgliedstaaten nicht gebieten, in einer Situation wie der des Ausgangsverfahrens im Hinblick auf einen effektiven Schutz des Urheberrechts die Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen. Die Mitgliedstaaten sind gemäß dem Unionsrecht jedoch dazu verpflichtet, sich bei der Umsetzung dieser Richtlinien auf eine Auslegung derselben zu stützen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Unionsrechtsordnung geschützten Grundrechten sicherzustellen. Bei der Durchführung der Maßnahmen zur Umsetzung dieser Richtlinien haben die Behörden und Gerichte der Mitgliedstaaten nicht nur ihr nationales Recht im Einklang mit diesen Richtlinien auszulegen, sondern auch darauf zu achten, dass sie sich nicht auf eine Auslegung dieser Richtlinien stützen, die mit diesen Grundrechten oder den anderen allgemeinen Grundsätzen des Unionsrechts, wie etwa dem Grundsatz der Verhältnismäßigkeit, kollidiert.

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

[83] 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).

[84] 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).

[85] 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).

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.

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.

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.

3. Auslistung personenbezogener Daten

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

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 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[86]. 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[87].

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

---

86 Art. 8 Abs. 1 der Richtlinie 95/46 und Art. 9 Abs. 1 DSGVO.
87 Art. 8 Abs. 5 der Richtlinie 95/46 und Art. 10 DSGVO.

einen besonders schweren Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen können.

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.

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[88], 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[89].

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 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.

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

[88] Art. 8 Abs. 2 Buchst. e der Richtlinie 95/46 und Art. 9 Abs. 2 Buchst. e DSGVO.
[89] Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 und Art. 21 Abs. 1 DSGVO.

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.

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

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 befinden, die sich auf dieses Recht beruft, in die Ergebnisliste) in oder außerhalb der Union stattfindet[90].

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

[90] Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 und Art. 3 Abs. DSGVO.

werden, doch ergibt sich aus dem Unionsrecht[91] 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.

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.

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.

Urteil vom 8. Dezember 2022 (Große Kammer), Google (Auslistung eines angeblich unrichtigen Inhalts) (C-460/20, EU:C:2022:962)

Die Kläger des Ausgangsverfahrens, zum einen TU, der mehrere leitende Posten bekleidet und Anteile an mehreren Gesellschaften hält, und zum anderen RE, die seine Lebensgefährtin und bis Mai 2015 Prokuristin einer dieser Gesellschaften war, waren

[91] Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 und Art. 17 Abs. 1 DSGVO.

Gegenstand dreier Artikel, die im Jahr 2015 auf einer Website von der G- LLC, dem Betreiber dieser Website, veröffentlicht wurden. Diese Artikel, von denen einer mit vier Fotos bebildert war, die die Kläger darstellten und nahelegten, dass sie einen luxuriösen Lebensstil führten, stellten das Anlagemodell mehrerer ihrer Gesellschaften kritisch dar. Der Zugang zu diesen Artikeln war dadurch möglich, dass in der von der Google LLC (im Folgenden: Google) betriebenen Suchmaschine die Namen und Vornamen der Kläger sowohl einzeln als auch in Verbindung mit bestimmten Firmennamen eingegeben wurden. In der Ergebnisübersicht wurde mittels eines Links auf diese Artikel sowie auf die in Gestalt von Vorschaubildern angezeigten Fotos („thumbnails“) verwiesen.

Die Kläger des Ausgangsverfahrens forderten Google als die für die mit ihrer Suchmaschine vorgenommene Verarbeitung personenbezogener Daten verantwortliche Stelle auf, zum einen aus der Übersicht der Suchergebnisse die Links zu den im Ausgangsverfahren in Rede stehenden Artikeln auszulisten, weil sie unrichtige Behauptungen und verleumderische Ansichten enthielten, und zum anderen die Vorschaubilder aus der Übersicht der Suchergebnisse zu entfernen. Google lehnte es ab, dieser Aufforderung Folge zu leisten.

Da die Kläger des Ausgangsverfahrens sowohl im ersten Rechtszug als auch in der Berufungsinstanz keinen Erfolg hatten, legten sie beim Bundesgerichtshof (Deutschland) Revision ein, in deren Rahmen der Bundesgerichtshof den Gerichtshof um Vorabentscheidung über die Auslegung der DSGVO und der Richtlinie 95/46[92] ersucht hat.

Mit seinem von der Großen Kammer erlassenen Urteil entwickelt der Gerichtshof seine Rechtsprechung zu den Voraussetzungen weiter, die für Anträge auf Auslistung gelten, die auf der Grundlage der Regeln über den Schutz personenbezogener Daten an den Betreiber einer Suchmaschine gestellt werden. Im Einzelnen untersucht er zum einen den Umfang der Verpflichtungen und des Verantwortungsbereichs des Betreibers einer Suchmaschine bei der Bearbeitung eines Auslistungsbegehrens, das auf die angebliche Unrichtigkeit der im aufgelisteten Inhalt stehenden Informationen gestützt wird, und zum anderen die Beweislast der betroffenen Person in Bezug auf diese Unrichtigkeit. Ferner äußert er sich zu dem Erfordernis, bei der Prüfung eines Antrags auf Löschung von Fotos, die in der Übersicht der Ergebnisse einer Bildersuche in Gestalt von Vorschaubildern angezeigt werden, den ursprünglichen Kontext der Veröffentlichung dieser Fotos im Internet zu berücksichtigen.

Der Gerichtshof erkennt erstens für Recht, dass im Rahmen der Abwägung zwischen den Rechten auf Achtung des Privatlebens und auf Schutz personenbezogener Daten einerseits und dem Recht auf freie Meinungsäußerung und Information andererseits[93], die bei der Prüfung eines an den Betreiber einer Suchmaschine gestellten

[92] Art. 17 Abs. 3 Buchst. a DSGVO bzw. Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46.
[93] Durch die Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union verbürgte Grundrechte.

Auslistungsantrags vorzunehmen ist, der darauf abzielt, dass in der Übersicht der Ergebnisse einer Suche der Link zu einem Inhalt, der angeblich unrichtige Informationen enthält, gelöscht wird, diese Auslistung nicht davon abhängt, dass die Frage der Richtigkeit des aufgelisteten Inhalts im Rahmen eines von dem Antragsteller gegen den Inhalteanbieter eingelegten Rechtsbehelfs einer zumindest vorläufigen Klärung zugeführt worden ist.

Vorab hat der Gerichtshof hinsichtlich der Prüfung der Frage, unter welchen Voraussetzungen der Betreiber einer Suchmaschine verpflichtet ist, einem Auslistungsantrag stattzugeben und folglich aus der im Anschluss an eine Suche anhand des Namens der betroffenen Person angezeigten Ergebnisliste den Link zu einer Website zu löschen, auf der sich Behauptungen befinden, die von dieser Person für unrichtig gehalten werden, auf Folgendes hingewiesen:

• Durch die Tätigkeit einer Suchmaschine können die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten erheblich beeinträchtigt werden, und zwar zusätzlich zur Tätigkeit der Herausgeber von Websites. Der Betreiber dieser Suchmaschine hat als derjenige, der über die Zwecke und Mittel dieser Tätigkeit entscheidet, daher in seinem Verantwortungsbereich im Rahmen seiner Befugnisse und Möglichkeiten dafür zu sorgen, dass die in der Richtlinie 95/46 und der DSGVO vorgesehenen Garantien ihre volle Wirksamkeit entfalten können und ein wirksamer und umfassender Schutz der betroffenen Personen tatsächlich verwirklicht werden kann.

• Der mit einem Auslistungsantrag befasste Betreiber einer Suchmaschine muss prüfen, ob die Aufnahme des Links zu der fraglichen Website in die Ergebnisübersicht für die Ausübung des Rechts auf freie Information der Internetnutzer, die potenziell Interesse an einem Zugang zu dieser Website mittels einer solchen Suche haben, erforderlich ist; dieses Recht wird durch das Recht auf freie Meinungsäußerung und Informationsfreiheit geschützt.

• Die DSGVO verlangt ausdrücklich eine Abwägung zwischen den Grundrechten auf Achtung des Privatlebens und auf Schutz personenbezogener Daten einerseits und dem Grundrecht auf freie Information andererseits.

Der Gerichtshof stellt zunächst fest, dass die Rechte der betroffenen Person auf Achtung des Privatlebens und auf Schutz personenbezogener Daten zwar im Allgemeinen gegenüber dem berechtigten Interesse der Internetnutzer überwiegen, die potenziell Interesse an einem Zugang zu der fraglichen Information haben. Dieser Ausgleich kann aber von den relevanten Umständen des Einzelfalls abhängen, insbesondere von der Art dieser Information, von deren Sensibilität für das Privatleben der betroffenen Person und vom Interesse der Öffentlichkeit am Zugang zu der Information, das u. a. je nach der Rolle, die die Person im öffentlichen Leben spielt, variieren kann.

Bei dieser Beurteilung ist auch die Frage der Richtigkeit des aufgelisteten Inhalts ein relevanter Gesichtspunkt. So können das Recht der Internetnutzer auf Information und

die Meinungsäußerungsfreiheit des Inhalteanbieters unter bestimmten Umständen Vorrang vor den Rechten auf Schutz der Privatsphäre und auf Schutz personenbezogener Daten haben, insbesondere wenn die betroffene Person im öffentlichen Leben eine Rolle spielt. Dieses Verhältnis kehrt sich jedoch dann um, wenn zumindest ein für den gesamten Inhalt nicht unbedeutender Teil der Informationen, um die es in dem Auslistungsantrag geht, unrichtig ist. Denn in einem solchen Fall können das Recht, Informationen weiterzugeben, und das Recht, Informationen zu erhalten, nicht berücksichtigt werden, da sie nicht das Recht einschließen können, derartige Informationen zu verbreiten und Zugang zu ihnen zu erhalten.

Was sodann zum einen die Verpflichtungen hinsichtlich der Feststellung betrifft, ob die in dem aufgelisteten Inhalt enthaltenen Informationen richtig sind, stellt der Gerichtshof klar, dass der Person, die wegen der Unrichtigkeit dieser Informationen die Auslistung begehrt, der Nachweis obliegt, dass diese Informationen offensichtlich unrichtig sind oder zumindest ein für diesen gesamten Inhalt nicht unbedeutender Teil dieser Informationen offensichtlich unrichtig ist. Damit dieser Person jedoch keine übermäßige Belastung auferlegt wird, die die praktische Wirksamkeit des Rechts auf Auslistung beeinträchtigen könnte, hat sie lediglich die Nachweise beizubringen, die unter Berücksichtigung der Umstände des Einzelfalls von ihr vernünftigerweise verlangt werden können. Diese Person kann grundsätzlich nicht dazu verpflichtet werden, bereits im vorgerichtlichen Stadium zur Stützung ihres Auslistungsantrags eine gegen den Herausgeber der Website erwirkte gerichtliche Entscheidung – selbst in Form einer im Verfahren des vorläufigen Rechtsschutzes ergangenen Entscheidung – vorzulegen.

Zum anderen hebt der Gerichtshof hinsichtlich der Verpflichtungen und des Verantwortungsbereichs des Suchmaschinenbetreibers hervor, dass sich dieser Betreiber bei der infolge eines Auslistungsantrags vorzunehmenden Prüfung, ob ein Inhalt in der Ergebnisübersicht der über seine Suchmaschine durchgeführten Suche verbleiben kann, auf alle betroffenen Rechte und Interessen sowie auf alle Umstände des Einzelfalls zu stützen hat. Dieser Betreiber ist allerdings nicht verpflichtet, den Sachverhalt zu ermitteln und hierfür mit dem Inhalteanbieter einen kontradiktorischen Schriftwechsel zu führen, der darauf gerichtet ist, fehlende Angaben zur Richtigkeit des aufgelisteten Inhalts zu erlangen. Eine Verpflichtung, zur Feststellung der Richtigkeit des aufgelisteten Inhalts beizutragen, würde zu einer Belastung dieses Betreibers führen, die über das hinausginge, was von ihm im Hinblick auf seinen Verantwortungsbereich, seine Befugnisse und seine Möglichkeiten vernünftigerweise erwartet werden kann. Diese Lösung brächte die ernste Gefahr mit sich, dass Inhalte, die einem schutzwürdigen und überwiegenden Informationsbedürfnis der Öffentlichkeit dienen, ausgelistet würden und es somit schwierig würde, sie im Internet zu finden. Somit bestünde die reale Gefahr einer abschreckenden Wirkung für die Ausübung der Freiheit der Meinungsäußerung und der Informationsfreiheit, wenn ein solcher Betreiber eine Auslistung nahezu systematisch vornähme, um zu vermeiden, dass er die Last der Ermittlung der Tatsachen zu tragen hat, die für die Feststellung der Richtigkeit oder Unrichtigkeit des aufgelisteten Inhalts relevant sind.

Folglich ist der Betreiber der Suchmaschine, wenn die eine Auslistung begehrende Person Nachweise vorlegt, die belegen, dass die in dem aufgelisteten Inhalt enthaltenen Informationen offensichtlich unrichtig sind oder zumindest ein für diesen gesamten Inhalt nicht unbedeutender Teil dieser Informationen offensichtlich unrichtig ist, verpflichtet, diesem Auslistungsantrag stattzugeben. Das Gleiche gilt, wenn dieser Antragsteller eine gegenüber dem Herausgeber der Website ergangene gerichtliche Entscheidung vorlegt, die auf der Feststellung beruht, dass in dem aufgelisteten Inhalt enthaltene Informationen, die im Hinblick auf den gesamten Inhalt nicht unbedeutend sind, zumindest auf den ersten Blick unrichtig sind. Dagegen ist bei Nichtvorliegen einer solchen gerichtlichen Entscheidung der Betreiber der Suchmaschine, wenn sich aus den vom Antragsteller vorgelegten Nachweisen nicht offensichtlich ergibt, dass solche Informationen unrichtig sind, nicht verpflichtet, dem Auslistungsantrag stattzugeben. Wenn die fraglichen Informationen zu einer Debatte von allgemeinem Interesse beitragen können, ist unter Berücksichtigung aller Umstände des Einzelfalls dem Recht auf freie Meinungsäußerung und Information besondere Bedeutung beizumessen.

Schließlich fügt der Gerichtshof hinzu, dass sich die betroffene Person, wenn der Betreiber einer Suchmaschine einem Auslistungsantrag nicht stattgibt, an die Kontrollstelle oder das Gericht wenden können muss, damit diese die erforderlichen Überprüfungen vornehmen und den Verantwortlichen anweisen, die gebotenen Maßnahmen zu ergreifen. Insoweit ist es insbesondere Sache der Justizbehörden, die Abwägung der widerstreitenden Interessen zu gewährleisten, da sie am besten in der Lage sind, eine komplexe und eingehende Abwägung vorzunehmen, die alle in der einschlägigen Rechtsprechung aufgestellten Kriterien und Gesichtspunkte berücksichtigt.

Zweitens erkennt der Gerichtshof für Recht, dass im Rahmen der Abwägung, die zwischen den oben genannten Grundrechten vorzunehmen ist, um einen Auslistungsantrag zu prüfen, der darauf abzielt, dass in den Ergebnissen einer anhand des Namens einer natürlichen Person durchgeführten Bildersuche Fotos, die in Gestalt von Vorschaubildern angezeigt werden und diese Person darstellen, gelöscht werden, dem Informationswert dieser Fotos unabhängig vom ursprünglichen Kontext ihrer Veröffentlichung auf der Internetseite, von der sie stammen, Rechnung zu tragen ist. Allerdings ist jedes Textelement zu berücksichtigen, das mit der Anzeige dieser Fotos in den Suchergebnissen unmittelbar einhergeht und Aufschluss über den Informationswert dieser Fotos geben kann.

Zur Begründung dieses Ergebnisses hebt der Gerichtshof hervor, dass für die Bildersuche, die über eine Suchmaschine im Internet anhand des Namens einer Person durchgeführt wird, dieselben Grundsätze gelten wie für die Suche nach Internetseiten und den darin enthaltenen Informationen. Er weist darauf hin, dass die nach einer namensbezogenen Suche erfolgende Anzeige von Fotos der betroffenen Person in Gestalt von Vorschaubildern einen besonders starken Eingriff in die Rechte dieser

Person auf Schutz des Privatlebens und ihrer personenbezogenen Daten darstellen kann.

Daher muss der Betreiber einer Suchmaschine, wenn er mit einem Auslistungsantrag befasst wird, der darauf abzielt, dass aus den Ergebnissen einer anhand des Namens einer Person durchgeführten Bildersuche Fotos gelöscht werden, die in Gestalt von diese Person darstellenden Vorschaubildern angezeigt werden, prüfen, ob die Anzeige der fraglichen Fotos erforderlich ist, um das Recht auf freie Information auszuüben, das den Internetnutzern zusteht, die potenziell Interesse an einem Zugang zu diesen Fotos mittels einer solchen Suche haben.

Soweit die Suchmaschine Fotos der betroffenen Person aber außerhalb desjenigen Kontexts anzeigt, in dem die Fotos auf der aufgelisteten Internetseite – zumeist zur Veranschaulichung der auf dieser Seite enthaltenen Textelemente – veröffentlicht sind, ist zu prüfen, ob dieser Kontext bei der vorzunehmenden Abwägung der widerstreitenden Rechte und Interessen gleichwohl zu berücksichtigen ist. In diesem Rahmen hängt die Frage, ob in die genannte Beurteilung auch der Inhalt der Internetseite miteinzubeziehen ist, auf der sich das Foto befindet, in Bezug auf dessen Anzeige in Gestalt eines Vorschaubildes die Löschung begehrt wird, von dem Gegenstand und der Art der in Rede stehenden Verarbeitung ab.

Was zunächst den Gegenstand der in Rede stehenden Verarbeitung anbelangt, stellt der Gerichtshof fest, dass die Veröffentlichung von Fotos als nicht mündliches Kommunikationsmittel eine stärkere Wirkung als veröffentlichte Texte auf die Internetnutzer ausüben kann. Denn Fotos sind als solche ein wichtiges Mittel, um die Aufmerksamkeit der Internetnutzer auf sich zu ziehen, und können ein Interesse wecken, auf die Artikel zuzugreifen, die sie bebildern. Doch insbesondere aufgrund des Umstands, dass Fotos häufig mehreren Interpretationen zugänglich sind, kann ihre Anzeige als Vorschaubilder in der Übersicht der Suchergebnisse zu einem besonders schwerwiegenden Eingriff in das Recht der betroffenen Person auf Schutz am eigenen Bild führen, was bei der Abwägung der widerstreitenden Rechte und Interessen zu berücksichtigen ist. Es ist eine unterschiedliche Abwägung je nachdem erforderlich, ob es sich einerseits um Artikel handelt, die mit Fotos versehen sind, die der Herausgeber der Internetseite veröffentlicht hat und die in ihrem ursprünglichen Kontext die in diesen Artikeln enthaltenen Informationen und die dort zum Ausdruck gebrachten Meinungen veranschaulichen, und andererseits um Fotos, die in Gestalt von Vorschaubildern in der Ergebnisübersicht vom Betreiber einer Suchmaschine außerhalb des Kontexts angezeigt werden, in dem sie auf der ursprünglichen Internetseite veröffentlicht worden sind.

Insoweit weist der Gerichtshof darauf hin, dass der Grund für die Zulässigkeit der Veröffentlichung personenbezogener Daten auf einer Website nicht unbedingt derselbe ist wie der für die Tätigkeit der Suchmaschinen. Doch selbst wenn dies der Fall ist, kann die vorzunehmende Abwägung der betroffenen Rechte und Interessen verschieden ausfallen, je nachdem, ob es sich um die vom Betreiber einer Suchmaschine oder die

vom Herausgeber der Internetseite ausgeführte Verarbeitung handelt. Zum einen können die berechtigten Interessen, die die Verarbeitungen rechtfertigen, verschieden sein, und zum anderen sind die Folgen, die diese Verarbeitungen für die betroffene Person, insbesondere für ihr Privatleben, haben, nicht zwangsläufig dieselben.

Was sodann die Art der vom Suchmaschinenbetreiber vorgenommenen Verarbeitung anbelangt, stellt der Gerichtshof fest, dass der Betreiber einer Suchmaschine dadurch, dass er die im Internet veröffentlichten Fotos natürlicher Personen sammelt und sie in den Ergebnissen einer Bildersuche in Gestalt von Vorschaubildern getrennt anzeigt, einen Dienst anbietet, mit dem er eine eigenständige Verarbeitung personenbezogener Daten vornimmt, die sowohl von der des Herausgebers der Internetseite, von der die Fotos entnommen sind, als auch von derjenigen der Listung der Internetseite verschieden ist, für die dieser Betreiber ebenfalls verantwortlich ist.

Daher ist die Tätigkeit des Suchmaschinenbetreibers, die darin besteht, Ergebnisse einer Bildersuche in Gestalt von Vorschaubildern anzuzeigen, eigenständig zu beurteilen, da die zusätzliche Beeinträchtigung der Grundrechte, die sich aus einer solchen Tätigkeit ergibt, besonders stark sein kann, weil bei einer namensbezogenen Suche alle im Internet befindlichen Informationen über die betroffene Person zusammengestellt werden. Im Rahmen dieser eigenständigen Beurteilung ist zu berücksichtigen, dass diese Anzeige als solche das vom Internetnutzer gesuchte Ergebnis darstellt, unabhängig davon, ob er sich später dazu entschließt, auf die ursprüngliche Internetseite zuzugreifen.

Der Gerichtshof weist jedoch darauf hin, dass eine solche spezifische Abwägung, die den eigenständigen Charakter der vom Suchmaschinenbetreiber vorgenommenen Verarbeitung berücksichtigt, die etwaige Relevanz von Textelementen, die mit der Anzeige eines Fotos in der Übersicht der Ergebnisse einer Suche unmittelbar einhergehen können, unberührt lässt, da solche Textelemente Aufschluss über den Informationswert dieses Fotos für die Öffentlichkeit geben und damit die Abwägung der betroffenen Rechte und Interessen beeinflussen können.

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)

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[94] in Verbindung mit der Richtlinie 95/46[95] und der DSGVO[96].

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[97] nunmehr 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.

Der Gerichtshof ist deshalb zu dem Schluss gelangt, dass keine wirksame Einwilligung vorliegt, wenn die Speicherung von Informationen oder der Zugriff auf Informationen,

---

94 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.

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

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

97 Ebd.

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.

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.

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.

5. Verarbeitung personenbezogener Daten in sozialen Online-Netzwerken

Urteil vom 4. Juli 2023 (Große Kammer), Meta Platforms u. a. (Allgemeine Nutzungsbedingungen eines sozialen Netzwerks) (C-252/21, EU:C:2023:537)

Die Gesellschaft Meta Platforms ist Eigentümerin des sozialen Online-Netzwerks „Facebook“, das für private Nutzer kostenlos ist. Das Geschäftsmodell dieses sozialen Netzwerks basiert auf der Finanzierung durch Online-Werbung, die auf den individuellen Nutzer zugeschnitten ist. Technische Grundlage dieser Art von Werbung ist die automatisierte Erstellung von detaillierten Profilen der Nutzer des Netzwerks und der auf Ebene des Meta-Konzerns angebotenen Online-Dienste. Um das soziale Netzwerk nutzen zu können, müssen die Nutzer daher bei ihrer Registrierung den von Meta Platforms festgelegten Allgemeinen Nutzungsbedingungen zustimmen, die auf die von diesem Unternehmen festgelegten Richtlinien für die Verwendung von Daten und Cookies verweisen. Danach erfasst Meta Platforms neben den Daten, die diese Nutzer bei ihrer Registrierung direkt angeben, auch Daten über Nutzeraktivitäten innerhalb und außerhalb des sozialen Netzwerks und ordnet sie den Facebook-Konten der betroffenen Nutzer zu. Bei den Daten, die Aktivitäten außerhalb des sozialen Netzwerks betreffen

(auch „Off-Facebook-Daten“ genannt), handelt es sich zum einen um Daten über den Aufruf dritter Websites und Apps und zum anderen um Daten über die Nutzung anderer zum Meta-Konzern gehörender Online-Dienste (darunter Instagram und WhatsApp). In ihrer Gesamtheit lassen die auf diese Weise erhobenen Daten detaillierte Rückschlüsse auf die Präferenzen und Interessen der Nutzer zu.

Mit Beschluss vom 6. Februar 2019 untersagte das Bundeskartellamt (Deutschland) Meta Platforms zum einen, in den damals geltenden Allgemeinen Nutzungsbedingungen die Nutzung des sozialen Netzwerks Facebook durch in Deutschland wohnhafte private Nutzer von der Verarbeitung ihrer Off-Facebook-Daten abhängig zu machen, und zum anderen, diese Daten ohne ihre Einwilligung zu verarbeiten. Außerdem verpflichtete das Bundeskartellamt dieses Unternehmen, die Allgemeinen Nutzungsbedingungen so anzupassen, dass aus ihnen eindeutig hervorgeht, dass die fraglichen Daten nicht ohne Einwilligung der betreffenden Nutzer erfasst, mit den Facebook-Nutzerkonten verknüpft und verwendet werden. Schließlich hob das Bundeskartellamt hervor, dass eine solche Einwilligung ungültig sei, wenn sie eine Bedingung für die Nutzung des sozialen Netzwerks darstelle. Es begründete seinen Beschluss damit, dass die Verarbeitung der fraglichen Daten, die nicht im Einklang mit der DSGVO stehe, eine missbräuchliche Ausnutzung der beherrschenden Stellung von Meta Platforms auf dem Markt für soziale Online-Netzwerke darstelle.

Gegen diesen Beschluss legte Meta Platforms beim Oberlandesgericht Düsseldorf (Deutschland) Beschwerde ein. Da dieses Gericht sowohl hinsichtlich der Befugnis von Wettbewerbsbehörden, zu prüfen, ob eine Verarbeitung personenbezogener Daten den Anforderungen der DSGVO entspricht, als auch hinsichtlich der Auslegung und Anwendung bestimmter Vorschriften dieser Verordnung Zweifel hegt, hat es den Gerichtshof um Vorabentscheidung ersucht.

Mit seinem Urteil erteilt der Gerichtshof (Große Kammer) klarstellende Hinweise zu der Möglichkeit, dass der Betreiber eines sozialen Netzwerks „sensible“ personenbezogene Daten seiner Nutzer verarbeitet, zu den Voraussetzungen für die Rechtmäßigkeit der Datenverarbeitung durch einen solchen Betreiber sowie zur Gültigkeit der Einwilligung, die diese Nutzer einem Unternehmen, das auf dem nationalen Markt für soziale Online-Netzwerke eine beherrschende Stellung einnimmt, im Hinblick auf eine solche Verarbeitung erteilen.

Was die Verarbeitung besonderer Kategorien personenbezogener Daten[98] betrifft, befindet der Gerichtshof, dass in dem Fall, dass ein Nutzer eines sozialen Online-Netzwerks Websites oder Apps mit Bezug zu einer oder mehreren dieser Kategorien aufruft und dort gegebenenfalls Daten eingibt, indem er sich registriert oder Online-

[98] Gemäß Art. 9 Abs. 1 DSGVO. Diese Vorschrift bestimmt: „Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.“

Bestellungen aufgibt, die Verarbeitung personenbezogener Daten durch den Betreiber dieses sozialen Online-Netzwerks[99] als eine „Verarbeitung besonderer Kategorien personenbezogener Daten“ im Sinne von Art. 9 Abs. 1 DSGVO anzusehen ist, wenn sie die Offenlegung von Informationen ermöglicht, die in eine dieser besonderen Kategorien fallen, unabhängig davon, ob diese Informationen einen Nutzer dieses Netzwerks oder eine andere natürliche Person betreffen. Eine solche Datenverarbeitung ist vorbehaltlich bestimmter Ausnahmen[100] grundsätzlich untersagt.

In letzterer Hinsicht stellt der Gerichtshof klar, dass ein Nutzer eines sozialen Online-Netzwerks, wenn er Websites oder Apps mit Bezug zu einer oder mehreren der fraglichen besonderen Kategorien von Daten aufruft, die diesen Aufruf betreffenden Daten, die der Betreiber dieses sozialen Online-Netzwerks über Cookies oder ähnliche Speichertechnologien erhebt, nicht offensichtlich öffentlich macht[101]. Im Übrigen macht ein solcher Nutzer, wenn er Daten auf solchen Websites oder in solchen Apps eingibt oder darin eingebundene Schaltflächen betätigt – wie etwa „Gefällt mir“ oder „Teilen“ oder Schaltflächen, die es dem Nutzer ermöglichen, sich auf diesen Websites oder in diesen Apps unter Verwendung der Anmeldedaten, die mit seinem Konto als Nutzer des sozialen Netzwerks, seiner Telefonnummer oder seiner E- Mail-Adresse verknüpft sind, zu identifizieren –, die eingegebenen oder sich aus der Betätigung dieser Schaltflächen ergebenden Daten nur dann offensichtlich öffentlich, wenn er zuvor, gegebenenfalls durch in voller Kenntnis der Sachlage vorgenommene individuelle Einstellungen, explizit seine Entscheidung zum Ausdruck gebracht hat, die ihn betreffenden Daten einer unbegrenzten Zahl von Personen öffentlich zugänglich zu machen.

Was, allgemeiner betrachtet, die Voraussetzungen für die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten betrifft, weist der Gerichtshof darauf hin, dass nach der DSGVO die Verarbeitung von Daten rechtmäßig ist, wenn und soweit die betroffene Person ihre Einwilligung dazu für einen oder mehrere bestimmte Zwecke gegeben hat[102]. Liegt keine solche Einwilligung vor oder wurde die Einwilligung nicht freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich erteilt, ist eine solche Verarbeitung gleichwohl gerechtfertigt, wenn sie eine der Voraussetzungen in Bezug auf die Erforderlichkeit[103] erfüllt, die eng auszulegen sind. Die

---

99 Diese Verarbeitung besteht darin, dass dieser Betreiber die aus dem Aufruf dieser Websites und Apps stammenden Daten sowie die vom Nutzer eingegebenen Daten über integrierte Schnittstellen, Cookies oder ähnliche Speichertechnologien erhebt, die Gesamtheit dieser Daten mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und diese Daten verwendet.

100 Vorgesehen in Art. 9 Abs. 2 DSGVO. In dieser Vorschrift heißt es: „Absatz 1 gilt nicht in folgenden Fällen:
a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden, …
e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,
f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich, …“.

101 Im Sinne von Art. 9 Abs. 2 Buchst. e DSGVO.

102 Gemäß Art. 6 Abs. 1 Unterabs. 1 Buchst. a DSGVO.

103 Genannt in Art. 6 Abs. 1 Unterabs. 1 Buchst. b bis f DSGVO. Nach diesen Vorschriften ist die Verarbeitung nur rechtmäßig, wenn sie erforderlich ist, und zwar u. a. für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist (Art. 6 Abs. 1 Unterabs. 1 Buchst. b DSGVO), zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt (Art. 6 Abs. 1 Unterabs. 1 Buchst. c

vom Betreiber eines sozialen Online-Netzwerks vorgenommene Verarbeitung personenbezogener Daten seiner Nutzer kann indessen nur dann als für die Erfüllung eines Vertrags, dessen Vertragsparteien diese Nutzer sind, erforderlich angesehen werden, wenn diese Verarbeitung objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für diese Nutzer bestimmten Vertragsleistung ist, so dass der Hauptgegenstand des Vertrags ohne diese Verarbeitung nicht erfüllt werden könnte.

Ferner entscheidet der Gerichtshof, dass die in Rede stehende Datenverarbeitung nur dann als zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich angesehen werden kann, wenn der fragliche Betreiber den Nutzern, bei denen die Daten erhoben wurden, ein mit der Datenverarbeitung verfolgtes berechtigtes Interesse mitgeteilt hat, wenn diese Verarbeitung innerhalb der Grenzen dessen erfolgt, was zur Verwirklichung dieses berechtigten Interesses absolut notwendig ist und wenn sich aus einer Abwägung der einander gegenüberstehenden Interessen unter Würdigung aller relevanten Umstände ergibt, dass die Interessen oder Grundrechte und Grundfreiheiten dieser Nutzer gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen. Insoweit ist der Gerichtshof der Auffassung, dass bei fehlender Einwilligung der Nutzer ihre Interessen und Grundrechte gegenüber dem Interesse des Betreibers eines sozialen Online-Netzwerks an der Personalisierung der Werbung, mit der er seine Tätigkeit finanziert, überwiegen.

Schließlich stellt der Gerichtshof klar, dass die in Rede stehende Datenverarbeitung gerechtfertigt ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche gemäß einer Vorschrift des Unionsrechts oder des Rechts des betreffenden Mitgliedstaats unterliegt, tatsächlich erforderlich ist, diese Rechtsgrundlage ein im öffentlichen Interesse liegendes Ziel verfolgt und in einem angemessenen Verhältnis zu dem verfolgten legitimen Ziel steht und diese Verarbeitung in den Grenzen des absolut Notwendigen erfolgt.

Hinsichtlich der Frage, ob nach der DSGVO die Einwilligung der betroffenen Nutzer in die Verarbeitung ihrer Daten gültig ist, befindet der Gerichtshof, dass der Umstand, dass der Betreiber eines sozialen Online-Netzwerks eine beherrschende Stellung auf dem Markt für soziale Online-Netzwerke einnimmt, für sich genommen nicht ausschließt, dass die Nutzer eines solchen Netzwerks wirksam in die Verarbeitung ihrer personenbezogenen Daten durch diesen Betreiber einwilligen können. Da eine solche Stellung geeignet ist, die Wahlfreiheit der Nutzer zu beeinträchtigen und ein klares Ungleichgewicht zwischen ihnen und dem Betreiber zu schaffen, ist sie jedoch ein wichtiger Aspekt für die Prüfung,

DSGVO), oder zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO).

ob die Einwilligung tatsächlich wfarrirksam, insbesondere freiwillig, erteilt wurde, wofür der Betreiber die Beweislast trägt[104].

Insbesondere müssen die Nutzer des fraglichen sozialen Netzwerks die Freiheit haben, im Zuge des Vertragsabschlusses die Einwilligung in bestimmte Datenverarbeitungsvorgänge, die für die Erfüllung des Vertrags nicht erforderlich sind, einzeln zu verweigern, ohne dazu gezwungen zu sein, auf die Nutzung dieses sozialen Online-Netzwerks vollständig zu verzichten, was bedingt, dass ihnen, gegebenenfalls gegen ein angemessenes Entgelt, eine gleichwertige Alternative angeboten wird, die nicht mit solchen Datenverarbeitungsvorgängen einhergeht. Darüber hinaus muss es möglich sein, eine gesonderte Einwilligung für die Verarbeitung der Off-Facebook-Daten zu erteilen.

VI. Nationale Kontrollstellen nationales de contrôle

1. Tragweite des Unabhängigkeitserfordernisses

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

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.

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

[104] Gemäß Art. 7 Abs. 1 DSGVO.

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.

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.

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 der Regierungschef über ein unbedingtes Recht verfügt, sich über alle Gegenstände der Geschäftsführung der Behörde zu unterrichten, nicht das Erfordernis der Unabhängigkeit der Kontrollstelle erfüllt.

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.

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.

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

n 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.

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

auf Privatsphäre und dem freien Verkehr personenbezogener Daten ein ausgewogenes Verhältnis herzustellen.

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.

2. Bestimmung des anwendbaren Rechts und der zuständigen Kontrollstelle

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

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 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

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. 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.

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.

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.

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.

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.

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.

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[105] 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[106] 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

[105] Z. B. die Buttons „Gefällt mir“ oder „Teilen“.

[106] „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.“

nämlich nur der irische Datenschutzbeauftragte befugt, unter der Kontrolle der irischen Gerichte eine Unterlassungsklage zu erheben.

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[107] die Einleitung eines gerichtlichen Verfahrens zu betreiben, obgleich sie für diese Verarbeitung nicht die federführende Behörde ist.

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 vorgesehenen Verfahren der Zusammenarbeit und Kohärenz ausgeübt werden[108].

Für grenzüberschreitende Verarbeitungen sieht die DSGVO nämlich ein Verfahren der Zusammenarbeit und Kohärenz[109] 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[110], wohingegen die Zuständigkeit der anderen nationalen Aufsichtsbehörden für den Erlass eines solchen, wenn auch nur vorläufigen, Beschlusses die Ausnahme darstellt[111]. Indessen muss die federführende Aufsichtsbehörde bei der Wahrnehmung ihrer Zuständigkeiten insbesondere den gebotenen Dialog führen und loyal und wirksam mit den anderen betroffenen

[107] Im Sinne von Art. 4 Nr. 23 DSGVO.
[108] In den Art. 56 und 60 DSGVO vorgesehen.
[109] Art. 56 Abs. 1 DSGVO.
[110] Art. 60 Abs. 7 DSGVO.
[111] Art. 56 Abs. 2 und Art. 66 DSGVO betreffen die Ausnahmen vom Grundsatz der Entscheidungsbefugnis der federführenden Aufsichtsbehörde.

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.

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[112] Gebrauch machen kann.

Zweitens hat der Gerichtshof entschieden, dass im Fall einer grenzüberschreitenden Datenverarbeitung die Ausübung der Befugnis zur Klageerhebung[113] 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 Anwendungsbereich der DSGVO[114] fallen, was voraussetzt, dass der für die grenzüberschreitende Verarbeitung Verantwortliche oder der Auftragsverarbeiter über eine Niederlassung im Gebiet der Union verfügt.

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.

---

[112] Vgl. Art. 55 und 56 DSGVO in Verbindung mit Art. 60 DSGVO.
[113] Nach Art. 58 Abs. 5 DSGVO.
[114] 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".

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.

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.

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 Vorschrift in der Rechtsordnung des betreffenden Mitgliedstaats nicht speziell umgesetzt worden ist.

Urteil vom 16. Januar 2024 (Große Kammer), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

In dieser Rechtssache (vgl. auch Abschnitt II.1 „Anwendungsbereich der allgemeinen Regelung“) stellt der Gerichtshof fest, dass für die Bestimmungen der DSGVO über die Zuständigkeit der nationalen Aufsichtsbehörden und das Beschwerderecht[115] keine nationalen Durchführungsmaßnahmen erforderlich sind und sie hinreichend klar, genau und unbedingt sind, um unmittelbar anwendbar zu sein. Daraus folgt, dass die DSGVO

[115] Art. 55 Abs. 1 bzw. Art. 77 Abs. 1 DSGVO.

den Mitgliedstaaten bei der Anzahl der einzurichtenden Aufsichtsbehörden einen Ermessensspielraum einräumt[116], im Gegenzug aber den Umfang ihrer Zuständigkeiten für die Überwachung der Anwendung der DSGVO festlegt. In Fällen, in denen sich ein Mitgliedstaat für die Einrichtung einer einzigen nationalen Aufsichtsbehörde entscheidet, ist diese zwangsläufig mit allen in der DSGVO vorgesehenen Zuständigkeiten ausgestattet. Jede andere Auslegung würde die praktische Wirksamkeit dieser Bestimmungen in Frage stellen und könnte die praktische Wirksamkeit aller anderen Bestimmungen der DSGVO, die für eine Beschwerde von Bedeutung sein könnten, schwächen.

Was den Umstand betrifft, dass eine Aufsichtsbehörde, die der Exekutive zuzurechnen ist, aufgrund nationaler Bestimmungen im Verfassungsrang nicht die Anwendung der DSGVO durch ein Organ der Legislative überwachen kann, weist der Gerichtshof darauf hin, dass sich die DSGVO gerade mit Blick auf die Achtung der verfassungsrechtlichen Struktur der Mitgliedstaaten darauf beschränkt, ihnen die Einrichtung mindestens einer Aufsichtsbehörde aufzuerlegen, und es ihnen freistellt, mehrere einzurichten. Die DSGVO räumt also jedem Mitgliedstaat einen Ermessensspielraum ein, der es ihm ermöglicht, so viele Aufsichtsbehörden einzurichten, wie insbesondere aufgrund seiner verfassungsmäßigen Struktur erforderlich sind.

Außerdem können die Einheit und die Wirksamkeit des Unionsrechts nicht dadurch beeinträchtigt werden, dass sich ein Mitgliedstaat auf Bestimmungen des nationalen Rechts beruft. Die Wirkungen des Grundsatzes des Vorrangs des Unionsrechts sind nämlich für alle Stellen eines Mitgliedstaats verbindlich, ohne dass dem insbesondere die innerstaatlichen Bestimmungen, auch wenn sie Verfassungsrang haben, entgegenstehen könnten.

Sofern sich ein Mitgliedstaat also für die Einrichtung einer einzigen Aufsichtsbehörde entschieden hat, kann er sich nicht auf Bestimmungen des nationalen Rechts berufen – auch wenn sie Verfassungsrang haben –, um Verarbeitungen personenbezogener Daten, die in den Anwendungsbereich der DSGVO fallen, der Überwachung durch diese Behörde zu entziehen.

[116] Gemäß Art. 51 Abs. 1 DSGVO.

4. Voraussetzungen für die Verhängung von Geldbußen

Urteil vom 5. Dezember 2023 (Große Kammer), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In dieser Rechtssache (vgl. auch die Abschnitte II.3 „Begriff ‚Verarbeitung personenbezogener Daten'", II.5 „Begriff ‚für die Verarbeitung [personenbezogener Daten] Verantwortlicher'" und II.6. „Begriff ‚gemeinsam Verantwortlicher'") stellt der Gerichtshof fest, dass nach Art. 83 DSGVO eine Geldbuße gegen einen Verantwortlichen nur dann verhängt werden kann, wenn feststeht, dass er vorsätzlich oder fahrlässig gegen Bestimmungen der DSGVO verstoßen hat[117].

In diesem Zusammenhang erläutert der Gerichtshof, dass der Unionsgesetzgeber den Mitgliedstaaten kein Ermessen hinsichtlich der materiellen Voraussetzungen eingeräumt hat, die von einer Aufsichtsbehörde einzuhalten sind, wenn sie beschließt, gemäß dieser Bestimmung eine Geldbuße gegen einen Verantwortlichen zu verhängen. Dass die DSGVO den Mitgliedstaaten die Möglichkeit gibt, Ausnahmen für Behörden und öffentliche Stellen, die in den Mitgliedstaaten niedergelassen sind[118], und Verfahrensanforderungen, die die Aufsichtsbehörden beachten müssen, wenn sie eine Geldbuße verhängen[119], vorzusehen, bedeutet nicht, dass sie auch solche materielle Voraussetzungen vorsehen dürften.

Zu diesen Voraussetzungen führt der Gerichtshof aus, dass zu den in der DSGVO aufgezählten Gesichtspunkten, die die Aufsichtsbehörde bei der Verhängung einer Geldbuße gegen den Verantwortlichen berücksichtigt, die „Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes"[120] gehört. Dagegen lässt sich keinem dieser Gesichtspunkte eine Möglichkeit entnehmen, den Verantwortlichen haftbar zu machen, wenn kein schuldhaftes Verhalten seinerseits vorliegt. Daher kann nur bei Verstößen gegen die Bestimmungen der DSGVO, die der Verantwortliche vorsätzlich oder fahrlässig begangen hat, eine Geldbuße gemäß Art. 83 DSGVO verhängt werden.

Diese Auslegung wird durch die allgemeine Systematik und den Zweck der DSGVO gestützt. Durch ein Sanktionssystem, das es ermöglicht, in Fällen, in denen die besonderen Umstände des Einzelfalls dies rechtfertigen, eine Geldbuße nach der DSGVO zu verhängen, werden die Verantwortlichen und Auftragsverarbeiter dazu angehalten, diese Verordnung einzuhalten. Geldbußen tragen durch ihre abschreckende Wirkung dazu bei, dass der Schutz der betroffenen Personen verbessert wird. Der Unionsgesetzgeber hat es jedoch nicht für erforderlich gehalten, die Verhängung von

---

117 Verstoß im Sinne von Art. 83 Abs. 4 bis 6.

118 In Art. 83 Abs. 7 DSGVO, wonach „jeder Mitgliedstaat Vorschriften dafür festlegen [kann], ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können".

119 Nach Art. 83 Abs. 8 DSGVO in Verbindung mit dem 129. Erwägungsgrund der DSGVO.

120 Art. 83 Abs. 2 Buchst. b DSGVO.

Geldbußen auch bei fehlendem Verschulden vorzusehen. Da die DSGVO auf ein gleichwertiges und homogenes Schutzniveau abzielt und deshalb in der gesamten Union einheitlich angewandt werden muss, liefe es diesem Zweck zuwider, den Mitgliedstaaten zu gestatten, eine solche Regelung für die Verhängung einer Geldbuße vorzusehen.

Der Gerichtshof stellt abschließend fest, dass eine solche Geldbuße gegen einen Verantwortlichen für personenbezogene Daten betreffende Verarbeitungsvorgänge, die von einem Auftragsverarbeiter in seinem Namen durchgeführt wurden, verhängt werden kann, es sei denn, der Auftragsverarbeiter hat im Rahmen dieser Verarbeitungsvorgänge Verarbeitungen für eigene Zwecke vorgenommen oder diese Daten auf eine Weise verarbeitet, die nicht mit dem Rahmen oder den Modalitäten der Verarbeitung, wie sie vom Verantwortlichen festgelegt wurden, vereinbar ist, oder auf eine Weise, bei der vernünftigerweise nicht davon ausgegangen werden kann, dass der Verantwortliche ihr zugestimmt hätte. In diesem Fall gilt der Auftragsverarbeiter nämlich in Bezug auf eine solche Verarbeitung als Verantwortlicher.

Urteil vom 5. Dezember 2023 (Große Kammer), Deutsche Wohnen (C-807/21, EU:C:2023:950)

Die Deutsche Wohnen SE (im Folgenden: DW) ist eine Immobiliengesellschaft, die über Beteiligungen an verschiedenen Gesellschaften mittelbar zahlreiche Wohn- und Gewerbeeinheiten hält. Sie verarbeitet im Rahmen ihrer Geschäftstätigkeit personenbezogene Daten der Mieter dieser Einheiten.

Im Anschluss an zwei in den Jahren 2017 und 2019 durchgeführte Kontrollen stellte die Berliner Beauftragte für den Datenschutz (Deutschland) fest, dass DW eine Reihe von Verstößen gegen die DSGVO begangen habe. Deswegen setzte sie mit Bescheid vom 30. Oktober 2019 Geldbußen gegen DW fest.

DW legte gegen diesen Bescheid Einspruch beim Landgericht Berlin (Deutschland) ein, das das Verfahren einstellte. Das Landgericht war der Auffassung, dass nach deutschem Recht[121] eine Ordnungswidrigkeit nur von einer natürlichen Person und nicht von einer juristischen Person begangen werden könne. Außerdem hafte eine juristische Person nur dann, wenn ihr die Handlungen ihrer Organmitglieder oder Repräsentanten zugerechnet werden könnten. Die Staatsanwaltschaft Berlin (Deutschland) focht diesen Beschluss beim Kammergericht Berlin (Deutschland) mit einer sofortigen Beschwerde an. In diesem Kontext ersuchte das Kammergericht den Gerichtshof im Rahmen der Vorabentscheidung um eine Auslegung der DSGVO.

In seinem Urteil äußert sich der Gerichtshof (Große Kammer) zu den Voraussetzungen für die Verhängung von Geldbußen nach der DSGVO. Erstens prüft der Gerichtshof die Frage, ob die Mitgliedstaaten die Verhängung einer Geldbuße gegen eine juristische

[121] Gesetz über Ordnungswidrigkeiten vom 24. Mai 1968 (BGBl. I S. 481) in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), geändert durch Gesetz vom 19. Juni 2020 (BGBl. I S. 1350).

Person davon abhängig machen dürfen, dass der Verstoß gegen die DSGVO zuvor einer identifizierten natürlichen Person zugerechnet wurde. Zweitens befasst er sich, wie im Urteil Nacionalinis visuomenės sveikatos centras (siehe oben), auch mit der Frage, ob der geahndete Verstoß gegen die DSGVO vorsätzlich oder fahrlässig begangen werden muss.

Was die Verhängung einer Geldbuße nach der DSGVO gegen eine juristische Person angeht, stellt der Gerichtshof zunächst fest, dass sich die in der DSGVO vorgesehenen Grundsätze, Verbote und Pflichten insbesondere an „Verantwortliche“ richten. Deren Verantwortung und Haftung erstreckt sich auf jedwede Verarbeitung personenbezogener Daten, die durch sie oder in ihrem Namen erfolgt. Diese Haftung ist es, die bei einem Verstoß gegen die DSGVO die Grundlage dafür bildet, nach Art. 83 DSGVO eine Geldbuße gegen den Verantwortlichen zu verhängen. Jedoch hat der Unionsgesetzgeber bei der Bestimmung dieser Haftung nicht zwischen natürlichen und juristischen Personen unterschieden, da die einzige Voraussetzung für diese Haftung darin besteht, dass diese Personen allein oder zusammen mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden[122]. Folglich haftet grundsätzlich jede Person, die diese Voraussetzung erfüllt, u. a. für jeden Verstoß gegen die DSGVO, der von ihr selbst oder in ihrem Namen begangen wurde. Dies bedeutet zum einen, dass juristische Personen nicht nur für Verstöße haften, die von ihren Vertretern, Leitern oder Geschäftsführern begangen wurden, sondern auch für Verstöße, die von jeder anderen Person begangen wurden, die im Rahmen der unternehmerischen Tätigkeit und im Namen dieser juristischen Personen handelt. Zum anderen muss es möglich sein, die in der DSGVO für solche Verstöße vorgesehenen Geldbußen unmittelbar gegen juristische Personen zu verhängen, wenn diese als für die Verarbeitung Verantwortliche eingestuft werden können.

Sodann stellt der Gerichtshof fest, dass es in der DSGVO keine Bestimmung gibt, die die Verhängung einer Geldbuße gegen eine juristische Person als Verantwortliche davon abhängig macht, dass zuvor festgestellt wird, dass dieser Verstoß von einer identifizierten natürlichen Person begangen wurde. Außerdem hat der Unionsgesetzgeber den Mitgliedstaaten insoweit keinen Gestaltungsspielraum gelassen. Die Tatsache, dass die DSGVO ihnen die Möglichkeit einräumt, Anforderungen an das von den Aufsichtsbehörden anzuwendende Verfahren bei der Verhängung einer Geldbuße vorzusehen[123], bedeutet keineswegs, dass sie auch befugt wären, über die in der DSGVO geregelten Anforderungen hinaus zusätzliche materielle Voraussetzungen vorzusehen.

In diesem Kontext stellt der Gerichtshof klar, dass es dem Zweck der DSGVO zuwiderliefe, den Mitgliedstaaten zu gestatten, einseitig und als erforderliche

[122] Gemäß Art. 4 Nr. 7 DSGVO.
[123] Wie sich aus Art. 58 Abs. 4 und Art. 83 Abs. 8 in Verbindung mit dem 129. Erwägungsgrund der DSGVO ergibt.

Voraussetzung für die Verhängung einer Geldbuße gemäß Art. 83 DSGVO gegen einen Verantwortlichen, der eine juristische Person ist, zu verlangen, dass der betreffende Verstoß zuvor einer identifizierten natürlichen Person zugerechnet wurde oder ihr zuzurechnen ist. Außerdem könnte eine solche zusätzliche Anforderung letztlich die Wirksamkeit und die abschreckende Wirkung von Geldbußen schwächen, die gegen juristische Personen als Verantwortliche verhängt werden.

Schließlich weist der Gerichtshof darauf hin, dass der Begriff „Unternehmen“ im Sinne der Art. 101 und 102 AEUV[124] ohne Bedeutung für die Frage ist, ob und unter welchen Voraussetzungen eine Geldbuße gegen einen Verantwortlichen verhängt werden kann, der eine juristische Person ist, und nur von Bedeutung ist, um die Höhe einer solchen Geldbuße zu bestimmen.

Somit kommt der Gerichtshof zu dem Ergebnis, dass die DSGVO[125] einer nationalen Regelung entgegensteht, wonach eine Geldbuße wegen eines Verstoßes gegen die DSGVO[126] gegen eine juristische Person in ihrer Eigenschaft als Verantwortliche nur dann verhängt werden kann, wenn dieser Verstoß zuvor einer identifizierten natürlichen Person zugerechnet wurde.

Zu der Frage, ob die Mitgliedstaaten die Verhängung einer Geldbuße selbst dann vorsehen dürfen, wenn der geahndete Verstoß weder vorsätzlich noch fahrlässig begangen wurde, stellt der Gerichtshof zunächst fest, dass für die materiellen Voraussetzungen, die eine Aufsichtsbehörde bei der Verhängung einer Geldbuße gegen einen Verantwortlichen zu beachten hat, ausschließlich das Unionsrecht gilt und dass die Mitgliedstaaten insoweit über keinen Gestaltungsspielraum verfügen. Derselben Argumentation wie im vorgenannten Urteil Nacionalinis visuomenės sveikatos centras folgend stellt der Gerichtshof fest, dass gemäß Art. 83 DSGVO eine Geldbuße nur dann verhängt werden darf, wenn nachgewiesen ist, dass der Verantwortliche, der eine juristische Person und zugleich ein Unternehmen ist, einen Verstoß gegen die Bestimmungen dieser Verordnung vorsätzlich oder fahrlässig begangen hat.

---

[124] Auf den im 150. Erwägungsgrund der DSGVO verwiesen wird.
[125] Art. 58 Abs. 2 Buchst. i und Art. 83 Abs. 1 bis 6 DSGVO.
[126] Gemäß Art. 83 Abs. 4 bis 6 DSGVO.

5. Verhältnis der Zuständigkeiten nationaler Aufsichtsbehörden zu den Zuständigkeiten anderer nationaler Behörden

Urteil vom 4. Juli 2023 (Große Kammer), Meta Platforms u. a. (Allgemeine Nutzungsbedingungen eines sozialen Netzwerks) (C-252/21, EU:C:2023:537)

In dieser Rechtssache (vgl. auch Abschnitt V.5 „Verarbeitung personenbezogener Daten in sozialen Online-Netzwerken“) weist der Gerichtshof hinsichtlich der Frage, ob eine Wettbewerbsbehörde dafür zuständig ist, festzustellen, dass eine Verarbeitung personenbezogener Daten mit der DSGVO unvereinbar ist, darauf hin, dass eine solche Behörde im Rahmen der Prüfung, ob ein Missbrauch einer beherrschenden Stellung durch ein Unternehmen[127] vorliegt, vorbehaltlich der Erfüllung ihrer Pflicht zur loyalen Zusammenarbeit[128] mit den Datenschutzaufsichtsbehörden feststellen kann, dass die von diesem Unternehmen festgelegten Allgemeinen Nutzungsbedingungen, soweit sie sich auf die Verarbeitung personenbezogener Daten beziehen, und die Durchführung dieser Nutzungsbedingungen nicht mit dieser Verordnung vereinbar sind, wenn diese Feststellung erforderlich ist, um das Vorliegen eines solchen Missbrauchs zu belegen. Stellt eine Wettbewerbsbehörde im Rahmen der Feststellung des Missbrauchs einer beherrschenden Stellung einen Verstoß gegen die DSGVO fest, tritt sie jedoch nicht an die Stelle der Aufsichtsbehörden.

Unter Berücksichtigung des Grundsatzes der loyalen Zusammenarbeit sind die Wettbewerbsbehörden, wenn sie in Ausübung ihrer Zuständigkeiten zu prüfen haben, ob ein Verhalten eines Unternehmens mit den Bestimmungen der DSGVO vereinbar ist, somit verpflichtet, sich abzustimmen und loyal mit den betreffenden nationalen Aufsichtsbehörden bzw. der federführenden Aufsichtsbehörde zusammenzuarbeiten. In diesem Fall müssen alle diese Behörden ihre jeweiligen Befugnisse und Zuständigkeiten dergestalt einhalten, dass die Verpflichtungen aus der DSGVO und die Ziele dieser Verordnung beachtet werden und ihre praktische Wirksamkeit gewahrt wird. Hält es eine Wettbewerbsbehörde im Rahmen der Prüfung, ob ein Unternehmen eine beherrschende Stellung missbraucht, für erforderlich, die Vereinbarkeit eines Verhaltens dieses Unternehmens mit den Bestimmungen der DSGVO zu prüfen, so muss sie daher ermitteln, ob dieses oder ein ähnliches Verhalten bereits Gegenstand einer Entscheidung durch die zuständige nationale Aufsichtsbehörde oder die federführende Aufsichtsbehörde oder auch durch den Gerichtshof war. Ist dies der Fall, darf die Wettbewerbsbehörde davon nicht abweichen, wobei es ihr aber freisteht, daraus eigene Schlussfolgerungen unter dem Gesichtspunkt der Anwendung des Wettbewerbsrechts zu ziehen.

---

[127] Im Sinne von Art. 102 AEUV.
[128] Niedergelegt in Art. 4 Abs. 3 EUV.

Wenn sie Zweifel hinsichtlich der Tragweite der von der zuständigen nationalen Aufsichtsbehörde bzw. der federführenden Aufsichtsbehörde vorgenommenen Beurteilung hat, wenn das in Rede stehende Verhalten oder ein ähnliches Verhalten gleichzeitig Gegenstand einer Prüfung durch diese Behörden ist oder wenn sie bei Nichtvorliegen einer Untersuchung dieser Behörden der Auffassung ist, dass das Verhalten eines Unternehmens nicht mit den Bestimmungen der DSGVO vereinbar ist, muss die Wettbewerbsbehörde diese Behörden konsultieren und um deren Mitarbeit bitten, um ihre Zweifel auszuräumen oder zu klären, ob sie eine Entscheidung der betreffenden Aufsichtsbehörde abwarten muss, bevor sie mit ihrer eigenen Beurteilung beginnt. Wenn diese Behörden innerhalb einer angemessenen Frist keine Einwände erheben oder keine Antwort erteilen, kann die Wettbewerbsbehörde ihre eigene Untersuchung fortsetzen.

GERICHTSHOF
DER EUROPÄISCHEN UNION

Direktion Wissenschaftlicher Dienst und Dokumentation

Juli 2024