Sammlung der Rechtsprechung

SCHLUSSANTRÄGE DES GENERALANWALTS
MANUEL CAMPOS SÁNCHEZ-BORDONA
vom 30. März 2023[1]

Rechtssache C-162/22

A. G.,
unter Beteiligung von:
Lietuvos Respublikos generalinė prokuratūra

(Vorabentscheidungsersuchen des Lietuvos vyriausiasis administracinis teismas [Oberstes Verwaltungsgericht, Litauen])

„Vorlage zur Vorabentscheidung – Telekommunikation – Verarbeitung personenbezogener Daten – Richtlinie2002/58/EG – Anwendungsbereich – Art. 15 Abs. 1 – Zugang zu den von Betreibern elektronischer Kommunikationsdienste gespeicherten und im Rahmen von Ermittlungsverfahren erhobenen Daten – Spätere Nutzung der Daten bei Ermittlungen wegen eines Dienstvergehens“

1. Das vorliegende Vorabentscheidungsersuchen wirft im Wesentlichen die Frage auf, ob bestimmte personenbezogene Daten, die in einem strafrechtlichen Ermittlungsverfahren erlangt wurden, später in einem verwaltungsrechtlichen Disziplinarverfahren gegen einen Amtsträger genutzt werden können.

2. Im Rahmen der Beantwortung dieser Frage hat der Gerichtshof erneut Gelegenheit, sich zu den Anwendungsbereichen zum einen der Richtlinie 2002/58/EG[2] und zum anderen der Richtlinie (EU) 2016/680[3] und der Verordnung (EU) 2016/679[4] zu äußern.

1 Originalsprache: Spanisch.

2 Richtlinie 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).

3 Richtlinie 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, berichtigt in ABl. 2021, L 74, S. 36).

4 Verordnung 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, im Folgenden: DSGVO).

3. In Bezug auf die Richtlinie 2002/58 gibt es bereits eine gefestigte Rechtsprechung des Gerichtshofs zu den Voraussetzungen und Bedingungen, unter denen die Mitgliedstaaten den Anwendungsbereich der Rechte und Pflichten aus dieser Richtlinie begrenzen können [5].

I. Rechtlicher Rahmen

A. Unionsrecht

1. Richtlinie 2002/58

4. Art. 1 („Geltungsbereich und Zielsetzung“) lautet:

„(1) Diese Richtlinie sieht die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG[6] im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des [AEUV] fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union [EUV], und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.“

5. Art. 5 („Vertraulichkeit der Kommunikation“) bestimmt in Abs. 1:

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

[5] Ohne Anspruch auf Vollständigkeit können als wesentliche Bezugspunkte dieser Rechtsprechung u. a. die Urteile vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, im Folgenden: Urteil La Quadrature du Net), vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152), und vom 5. April 2022, Commissioner of An Garda Síochána u. a. (C-140/20, EU:C:2022:258, im Folgenden: Urteil Commissioner of An Garda Síochána), angeführt werden.

[6] Richtlinie 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).

unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen."

6. In Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG") heißt es:

„(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 [EUV] niedergelegten Grundsätzen entsprechen.

…

(2) Die Bestimmungen des Kapitels III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.

…"

2. DSGVO

7. Art. 2 („Sachlicher Anwendungsbereich") bestimmt:

„(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

…

d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

…"

8. In Art. 5 („Grundsätze für die Verarbeitung personenbezogener Daten") heißt es:

„(1) Personenbezogene Daten müssen

…

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken (‚Zweckbindung');

…"

9. Art. 6 („Rechtmäßigkeit der Verarbeitung") bestimmt:

„(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

…

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

…

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

…

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

…“

3. Richtlinie 2016/680

10. Abs. 1 von Art. 1 („Gegenstand und Ziele“) lautet:

„Diese Richtlinie enthält Bestimmungen 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.“

11. Art. 2 („Anwendungsbereich“) sieht in Abs. 1 vor:

„Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zu den in Artikel 1 Absatz 1 genannten Zwecken.“

12. In Art. 4 („Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten“) heißt es:

„(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten

…

b) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,

…

(2) Eine Verarbeitung durch denselben oder einen anderen Verantwortlichen für einen anderen der in Artikel 1 Absatz 1 genannten Zwecke als den, für den die personenbezogenen Daten erhoben werden, ist erlaubt, sofern

a) der Verantwortliche nach dem Unionsrecht oder dem Recht der Mitgliedstaaten befugt ist, solche personenbezogenen Daten für diesen anderen Zweck zu verarbeiten, und

b) die Verarbeitung für diesen anderen Zweck nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich und verhältnismäßig ist.

…“

13. Art. 9 („Besondere Verarbeitungsbedingungen“) bestimmt in Abs. 1:

„Personenbezogene Daten, die von zuständigen Behörden für die in Artikel 1 Absatz 1 genannten Zwecke erhoben werden, dürfen nicht für andere als die in Artikel 1 Absatz 1 genannten Zwecke verarbeitet werden, es sei denn, eine derartige Verarbeitung ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig. Wenn personenbezogene Daten für solche andere Zwecke verarbeitet werden, gilt die [DSGVO], es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.“

B. Nationales Recht

1. Lietuvos Respublikos elektroninių ryšių įstatymas [7]

14. Art. 65 Abs. 2 verpflichtet die Betreiber elektronischer Kommunikationsdienste, die in Anhang 1 dieses Gesetzes aufgeführten Daten zu speichern und gegebenenfalls den zuständigen nationalen Behörden Zugang zu ihnen zu gewähren, damit sie diese Daten zur Bekämpfung schwerer Kriminalität nutzen können [8].

15. Nach Art. 77 Abs. 1 müssen die Betreiber elektronischer Kommunikationsdienste den zuständigen Behörden die Informationen liefern, die sich rechtmäßig in ihrem Besitz befinden und die insbesondere zur Verhütung, Aufdeckung und Verfolgung von Straftaten von Bedeutung sind.

16. Nach Art. 77 Abs. 4 müssen die Betreiber elektronischer Kommunikationsdienste, wenn eine mit Gründen versehene gerichtliche Entscheidung oder eine andere Rechtsgrundlage sie dazu ermächtigt, insbesondere den mit strafrechtlichen Ermittlungen und Untersuchungen betrauten Behörden gemäß den Vorschriften der Strafprozessordnung die Kontrolle des Inhalts durch elektronische Kommunikationsnetze übermittelter Informationen ermöglichen.

2. Lietuvos Respublikos kriminalinės žvalgybos įstatymas [9]

17. Gemäß Art. 6 Abs. 3 Nr. 1 können die mit strafrechtlichen Ermittlungen betrauten Behörden [10] unter den Voraussetzungen des LIC und nach vorheriger staatsanwaltlicher oder gerichtlicher Genehmigung bei den Betreibern elektronischer Kommunikationsdienste Informationen einholen.

18. Nach Art. 8 Abs. 1 und 3 werden die mit strafrechtlichen Ermittlungen betrauten Behörden tätig, sobald ihnen Informationen über die Vorbereitung oder Begehung einer besonders schweren, schweren oder minder schweren Straftat vorliegen, indem sie unverzüglich strafrechtliche Ermittlungen einleiten, wenn die Untersuchung Anhaltspunkte für das Vorliegen einer Straftat ergibt.

19. Nach Art. 19 Abs. 1 Nr. 5 dürfen die bei strafrechtlichen Ermittlungen gewonnenen Informationen in den Fällen genutzt werden, die in den Abs. 3 und 4 dieser Vorschrift aufgeführt oder in anderen Rechtsvorschriften vorgesehen sind.

20. Nach Art. 19 Abs. 3 können Informationen über einen Sachverhalt, der die Merkmale einer mit Korruption im Zusammenhang stehenden Straftat aufweist, mit Einverständnis der Staatsanwaltschaft offengelegt und im Rahmen von Ermittlungen wegen Disziplinar- oder Dienstvergehen genutzt werden.

[7] Gesetz der Republik Litauen über die elektronische Kommunikation in der Fassung des Gesetzes Nr. IX-2135 vom 15. April 2004, geändert durch das Gesetz Nr. XIII-2172 vom 6. Juni 2019, im Folgenden: LCE.

[8] Die im betreffenden Anhang aufgeführten Daten („Kategorien zu schützender Daten“) sind zur Ermittlung von Herkunft und Ziel einer Kommunikation, ihres Datums, ihrer Uhrzeit und ihrer Dauer, der Art der Kommunikation und zur Lokalisierung des Kommunikationsmaterials (auch bei Mobilfunkkommunikation) der Nutzer erforderlich.

[9] Gesetz der Republik Litauen über die kriminalpolizeiliche Erkenntnisgewinnung in der Fassung des Gesetzes Nr. XI-2234 vom 2. Oktober 2012, geändert durch das Gesetz Nr. XIII-1837 vom 20. Dezember 2018, im Folgenden: LIC.

[10] Betrifft nicht die deutsche Fassung.

3. Lietuvos Respublikos baudžiamojo proceso kodeksas [11]

21. Nach Abs. 1 von Art. 154 („Kontrolle, Aufzeichnung und Speicherung durch elektronische Kommunikationsnetze übermittelter Informationen“) kann eine Ermittlungsbehörde auf der Grundlage eines auf Antrag der Staatsanwaltschaft erlassenen gerichtlichen Beschlusses über elektronische Kommunikationsmedien verbreitete Gespräche abhören, aufzeichnen und speichern, wenn Gründe für die Annahme vorliegen, dass Daten über eine geplante, gegenwärtige oder vollendete besonders schwere oder schwere Straftat oder über eine minder schwere oder leichte Straftat erlangt werden können.

22. Nach Abs. 1 von Art. 177 („Geheimhaltung von Daten aus dem Ermittlungsverfahren“) sind Daten aus dem Ermittlungsverfahren vertraulich und dürfen bis zur gerichtlichen Prüfung der Strafsache nur mit Genehmigung der Staatsanwaltschaft und nur im gerechtfertigten Umfang offengelegt werden [12].

II. Sachverhalt, Rechtsstreit und Vorlagefrage

23. Die Lietuvos Respublikos generalinė prokuratūra (Generalstaatsanwaltschaft der Republik Litauen, im Folgenden: Generalstaatsanwaltschaft) führte interne Ermittlungen zu Handlungen von A. G., der zu dieser Zeit das Amt eines Staatsanwalts bei der Apygardos prokuratūra (Bezirksstaatsanwaltschaft) innehatte, durch, weil es Hinweise auf ein dienstliches Fehlverhalten von A. G. gab.

24. Die Kommission der Generalstaatsanwaltschaft kam zu dem Ergebnis, dass A. G. ein dienstliches Fehlverhalten anzulasten sei, und schlug vor, gegen ihn die Disziplinarstrafe der Entlassung aus dem Dienst zu verhängen.

25. Dieses Verhalten soll anhand von Informationen nachgewiesen worden sein, die im Lauf des Verwaltungsverfahrens aufgrund der Tätigkeit der Kriminalpolizei, der Erklärungen anderer Amtsträger und von A. G. sowie der Ergebnisse zweier Ermittlungsverfahren erlangt worden seien.

26. Konkret habe es im Rahmen eines von A. G. geleiteten Ermittlungsverfahrens Telefonate zwischen ihm und dem Rechtsanwalt eines Beschuldigten gegeben; dieses Verfahren habe Fälle betroffen, in denen dieser Rechtsanwalt als Verteidiger aufgetreten sei [13].

27. Die Überwachung und die Speicherung der über elektronische Kommunikationsnetze verbreiteten Informationen waren durch gerichtliche Beschlüsse genehmigt worden.

28. Der Generalstaatsanwalt verhängte gegen A. G. die Sanktion der Entlassung aus dem Dienst, deren Aufhebung A. G. mit einer Klage beim Vilniaus apygardos administracinis teismas (Regionalverwaltungsgericht Vilnius, Litauen) begehrte.

[11] Strafprozessordnung der Republik Litauen vom 14. März 2002 in der im Ausgangsverfahren anwendbaren Fassung, im Folgenden: BPK.

[12] Nach den Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendacijos (Empfehlungen zur Bereitstellung und Nutzung von Daten aus dem Ermittlungsverfahren für nicht strafrechtliche Zwecke und zum Schutz von Daten aus dem Ermittlungsverfahren), genehmigt durch die Anordnung Nr. 1-279 des Generalstaatsanwalts vom 17. August 2017, in der durch die Anordnung Nr. 1-211 vom 25. Juni 2018 geänderten Fassung, insbesondere der Bestimmung 23, entscheidet der Staatsanwalt, wenn er einen Antrag auf Zugang zu Daten aus dem Ermittlungsverfahren erhalten hat, über deren Bereitstellung. Gibt er dem Antrag statt, muss er angeben, auf welche Weise sie bereitgestellt werden können.

[13] Nach den Ausführungen in der mündlichen Verhandlung sind wegen dieses Sachverhalts noch zwei Strafverfahren gegen A. G. und den Rechtsanwalt anhängig.

29. Mit Urteil vom 16. Juli 2021 wurde seine Klage vom erstinstanzlichen Gericht mit der Begründung abgewiesen, dass die Handlungen der Kriminalpolizei sowie die Heranziehung der von ihr erhobenen Daten im Disziplinarverfahren rechtmäßig gewesen seien.

30. A. G. legte gegen dieses erstinstanzliche Urteil Rechtsmittel beim Lietuvos vyriausiasis administracinis teismas (Oberstes Verwaltungsgericht, Litauen) ein, das dem Gerichtshof folgende Frage zur Vorabentscheidung vorlegt:

Ist Art. 15 Abs. 1 der Richtlinie 2002/58 in Verbindung mit den Art. 7, 8, 11 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) dahin auszulegen, dass es den zuständigen Behörden untersagt ist, von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherte Daten, die Informationen über die Daten und die Kommunikationen eines Nutzers eines elektronischen Kommunikationsmittels liefern können, im Rahmen von Ermittlungen wegen dienstlichen Fehlverhaltens im Zusammenhang mit Korruption zu nutzen, unabhängig davon, ob der Zugang zu diesen Daten im konkreten Fall zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit gewährt wurde?

III. Verfahren vor dem Gerichtshof

31. Das Vorabentscheidungsersuchen ist am 3. März 2022 beim Gerichtshof eingegangen.

32. A. G., die tschechische, die estnische, die ungarische, die irische, die italienische und die litauische Regierung sowie die Europäische Kommission haben schriftliche Erklärungen abgegeben.

33. An der mündlichen Verhandlung am 2. Februar 2023 haben A. G., die französische, die ungarische, die irische und die litauische Regierung sowie die Kommission teilgenommen.

IV. Würdigung

A. Zulässigkeit, Beschränkung der Antwort auf die Vorlagefrage

34. Das vorlegende Gericht ist ein Gericht der streitigen Verwaltungsgerichtsbarkeit, das als Rechtsmittelgericht über Entscheidungen der Verwaltung zu befinden hat. Bei der vom Generalstaatsanwalt getroffenen Entscheidung, gegen einen Amtsträger der Bezirksstaatsanwaltschaft wegen Dienstvergehen eine Sanktion in Form der Entlassung aus dem Dienst zu verhängen, handelt es sich um eine solche Entscheidung.

35. Gegenstand des Ausgangsverfahrens sind somit nicht Entscheidungen von Justizbehörden im Bereich des Strafrechts. Auch wenn zwischen diesen Entscheidungen und dem Verwaltungs(disziplinar)verfahren, das zur Entlassung aus dem Dienst führte[14], ein Zusammenhang besteht, ist Gegenstand des Rechtsstreits doch nur die Entlassung selbst.

[14] Siehe oben, Fn. 13.

36. Vor diesem Hintergrund ist festzustellen, dass die Vorlageentscheidung gewisse Ungenauigkeiten hinsichtlich der Tatumstände des Rechtsstreits aufweist, in dessen Kontext das Vorabentscheidungsersuchen steht.

37. Wie die tschechische Regierung und die Kommission ausgeführt haben, lässt sich anhand der Vorlageentscheidung nicht mit Sicherheit bestimmen, ob die zuständigen Behörden a) sich an die Betreiber elektronischer Kommunikationsdienste wandten, um die streitigen Daten zu erhalten, oder b) diese Daten unmittelbar von ihnen erhielten.

38. Diese Frage ist keineswegs unwichtig. Denn von ihr hängt es ab, welche Normen des Unionsrechts für die Antwort auf die Vorlagefrage maßgebend sind. Je nachdem, wie sich der Sachverhalt tatsächlich darstellte, finden folgende Richtlinien Anwendung:

– die Richtlinie 2002/58, wenn die Daten aufgrund einer den Betreibern elektronischer Kommunikationsdienste obliegenden Verpflichtung zu ihrer Verarbeitung erlangt wurden, oder

– die Richtlinie 2016/680, wenn staatliche Stellen die Daten unmittelbar erlangt haben, ohne den Betreibern Verpflichtungen aufzuerlegen.

39. Im letztgenannten Fall muss der Schutz personenbezogener Daten – unbeschadet der Anwendung der Richtlinie 2016/680 – im nationalen Recht geregelt werden[15]. In der Vorlagefrage, in der der Akzent auf die Richtlinie 2002/58 gelegt wird, wäre dann ein unzweckmäßiger Ansatz gewählt worden.

40. Die ungarische Regierung ist davon überzeugt, dass die personenbezogenen Daten dadurch erlangt wurden, dass die Kriminalpolizei Telefongespräche abhörte, und zieht die Zulässigkeit des Vorabentscheidungsersuchens in Zweifel, da die Richtlinie 2002/58 deshalb nicht anwendbar sei.

41. Demgegenüber ist die Kommission der Auffassung, dass

– die Richtlinie 2016/680 zur Anwendung komme, wenn personenbezogene Daten, die unmittelbar von den Behörden im Rahmen früherer strafrechtlicher Ermittlungen erhoben und gespeichert worden seien, bei späteren Ermittlungen genutzt würden;

– die Richtlinie 2002/58 anzuwenden sei, wenn, wie das vorlegende Gericht festgestellt habe[16], zumindest einige Daten aufgrund einer nach ihrem Art. 15 Abs. 1 erlassenen nationalen Rechtsvorschrift erhoben und gespeichert worden seien. In diesem Fall sei die Richtlinie 2002/58 für die Entscheidung des Rechtsstreits relevant.

42. Ich stimme dieser Erwägung der Kommission zu, zumal nur mit ihr die (gerechtfertigten) Vorbehalte gegen die Zulässigkeit der Vorlageentscheidung ausgeräumt werden können.

[15] Urteil La Quadrature du Net, Rn. 103: „Wenn die Mitgliedstaaten unmittelbar Maßnahmen umsetzen, mit denen von der Vertraulichkeit elektronischer Kommunikationen abgewichen wird, ohne den Betreibern elektronischer Kommunikationsdienste Verarbeitungspflichten aufzuerlegen, fällt der Schutz der Daten der Betroffenen hingegen nicht unter die Richtlinie 2002/58, sondern allein unter das nationale Recht, vorbehaltlich der Anwendung der [Richtlinie 2016/680].“

[16] Nr. 37 der Vorlageentscheidung.

43. Versteht man die Vorlagefrage so, ist in Bezug auf die Relevanz der Richtlinie 2002/58 für ihre Beantwortung Folgendes festzustellen:

– Ihre Relevanz folgt aus der jedem Vorabentscheidungsersuchen innewohnenden Vermutung seiner Erforderlichkeit, deren Beurteilung in den Verantwortungsbereich des vorlegenden Gerichts fällt [17].

– Sie kann bejaht werden, da der Gerichtshof nur um die Auslegung der Richtlinie 2002/58 ersucht wird, die das vorlegende Gericht als unerlässlich für die Entscheidung des Rechtsstreits erachtet [18].

44. Das vorlegende Gericht hält in dem von ihm zu entscheidenden Verfahren folgende Gesichtspunkte für relevant:

„i) den Zugang zu *Daten, die von den [Betreibern elektronischer Kommunikationsdienste]* nicht nur zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf Vorrat *gespeichert werden*;

ii) nach der Erlangung des Zugangs die *Nutzung der auf Vorrat gespeicherten Daten* zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit im Rahmen von Ermittlungen wegen dienstlichen Fehlverhaltens im Zusammenhang mit Korruption“ [19].

45. Alles deutet daher darauf hin, dass unabhängig von der Frage, ob es möglicherweise personenbezogene Daten gab, deren Bearbeitung nicht in den Anwendungsbereich der Richtlinie 2002/58 fallen konnte (sondern in den der Richtlinie 2016/680), bei der Untersuchung, die zur Verhängung der Sanktion führte, die von den Betreibern elektronischer Kommunikationsdienste erhobenen personenbezogenen Daten genutzt wurden.

46. Bei seiner Antwort ist der Gerichtshof daran gebunden, wie das Ersuchen des vorlegenden Gerichts gestellt wurde. Deshalb wird er klären müssen, ob die gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 im Rahmen strafrechtlicher Ermittlungen erhobenen und verarbeiteten personenbezogenen Daten später in einem (verwaltungsrechtlichen) Disziplinarverfahren gegen einen Amtsträger genutzt werden können.

47. Vor dem Hintergrund einer solchen inhaltlichen Begrenzung des Vorabentscheidungsersuchens ist festzustellen, dass folgende Fragen nicht von ihm erfasst werden:

– Erstens die Fragen nach der Rechtmäßigkeit der *ursprünglichen Erlangung* der personenbezogenen Daten im Rahmen von Art. 15 Abs. 1 der Richtlinie 2002/58. Das vorlegende Gericht beschränkt sich in seinem Ersuchen auf die *spätere Nutzung* dieser Daten

[17] Vgl. u. a. Urteile vom 4. Dezember 2018, Minister for Justice and Equality und Commissioner of An Garda Síochána (C-378/17, EU:C:2018:979, Rn. 26), und vom 22. Dezember 2022, Airbnb Ireland und Airbnb Payments UK (C-83/21, EU:C:2022:1018, Rn. 82).

[18] Die unmissverständliche Bezugnahme auf die Richtlinie 2002/58 im Tenor der Vorlageentscheidung und die unterbliebene Erwähnung der Richtlinie 2016/680 in ihren Gründen sprechen ebenfalls dafür. Gleichwohl kann der Gerichtshof, ohne die Grenzen der Vorlagefrage zu überschreiten, dem vorlegenden Gericht zweckdienliche Hinweise für dessen Entscheidung geben, gegebenenfalls unter Rückgriff auf weitere unionsrechtliche Vorschriften. Vgl. in diesem Sinne Urteil vom 18. September 2019, VIPA (C-222/18, EU:C:2019:751, Rn. 50 und die dort angeführte Rechtsprechung).

[19] Nr. 35 der Vorlageentscheidung. Hervorhebung nur hier.

im Disziplinarverfahren, ohne die Rechtmäßigkeit ihrer ursprünglichen Erlangung in Zweifel zu ziehen [20].

– Zweitens die Fragen nach der Nutzung der von den Behörden im Rahmen vorangegangener strafrechtlicher Ermittlungen unmittelbar erhobenen und verarbeiteten Daten. Auch in Bezug auf diesen Gesichtspunkt, der in den Anwendungsbereich des nationalen Rechts und der Richtlinie 2016/680 fällt, äußert das vorlegende Gericht keine Zweifel.

48. Im Ergebnis ist festzustellen, dass bei den folgenden Erwägungen zur Beantwortung der Frage die Auslegung der Richtlinie 2016/680 außer Acht zu lassen ist [21]. Was die Richtlinie 2002/58 anbelangt, werde ich meine Ausführungen auf die Nutzung personenbezogener Daten beschränken, die in ihrem Rahmen mittels Verarbeitungen erlangt wurden, von deren ursprünglicher Zulässigkeit auszugehen ist, da sie im Ausgangsverfahren nicht zur Diskussion steht.

B. Zur Beantwortung der Vorlagefrage

1. Zusammenfassung der Rechtsprechung des Gerichtshofs zur Anwendung der Richtlinie 2002/58

49. Gemäß Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 können die Mitgliedstaaten Rechtsvorschriften erlassen, die von dem in Art. 5 Abs. 1 der Richtlinie verankerten Grundsatz der Vertraulichkeit abweichen, sofern sie „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig“ sind und in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen [22].

50. Insbesondere ist die Möglichkeit für die Mitgliedstaaten, eine Beschränkung der in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten zu rechtfertigen, im Licht der Schwere des mit einer solchen Beschränkung verbundenen Eingriffs zu beurteilen und anhand dessen, ob die verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zur Schwere des Eingriffs steht [23].

51. „Um dem Erfordernis der Verhältnismäßigkeit zu genügen, müssen nationale Rechtsvorschriften klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz dieser Daten vor Missbrauchsrisiken ermöglichen. Diese Rechtsvorschriften müssen nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf …“ [24]

[20] Der Gerichtshof braucht sich daher nicht zur Rechtmäßigkeit dieser früheren Vorgänge zu äußern. Würde es dies tun, müsste er bekräftigen, dass der *Zugang* zu Daten, die sich im Besitz der Betreiber elektronischer Kommunikationsdienste befinden, nur gestattet werden kann, wenn ihre *Speicherung* im Einklang mit Art. 15 Abs. 1 der Richtlinie 2002/58 stand. Vgl. in diesem Sinne Urteil La Quadrature du Net, Rn. 167. Diese Vorschrift ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen, dass sie Rechtsvorschriften entgegensteht, die zu den fraglichen Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen (Urteil La Quadrature du Net, Rn. 168).

[21] Ich werde jedoch am Ende der vorliegenden Schlussanträge hilfsweise darauf eingehen.

[22] Urteil La Quadrature du Net, Rn. 129.

[23] Urteil La Quadrature du Net, Rn. 131 und die dort angeführte Rechtsprechung.

[24] Urteil Commissioner of An Garda Síochána, Rn. 54.

52. Was die dem Gemeinwohl dienenden Ziele anbelangt, die eine aufgrund von Art. 15 Abs. 1 der Richtlinie 2002/58 erlassene Vorschrift rechtfertigen können, besteht nach dem Grundsatz der Verhältnismäßigkeit eine Hierarchie zwischen diesen Zielen entsprechend ihrer jeweiligen Bedeutung: Die Bedeutung des mit einer solchen Vorschrift verfolgten Ziels muss in angemessenem Verhältnis zur Schwere des Eingriffs stehen [25].

53. Im Rahmen dieser Hierarchie von Zielen ist die Bedeutung des Ziels des Schutzes der nationalen Sicherheit im Licht von Art. 4 Abs. 2 EUV größer als die der übrigen von Art. 15 Abs. 1 der Richtlinie 2002/58 erfassten Ziele (Landesverteidigung, öffentliche Sicherheit sowie Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen). Das Ziel, die Kriminalität im Allgemeinen, einschließlich schwerer Kriminalität, zu bekämpfen und die öffentliche Sicherheit zu schützen, fällt in diese zweite Kategorie [26].

54. Aus dieser Kategorisierung von Zielen folgt:

– Das Ziel der Verteidigung der nationalen Sicherheit, das in der vom Gerichtshof aufgestellten Hierarchie an oberster Stelle steht, gestattet Eingriffe, deren Schwere der von Rechtsvorschriften entspricht, mit denen den Betreibern elektronischer Kommunikationsdienste aufgegeben wird, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern [27].

– Das Ziel mit der zweitgrößten Bedeutung – Bekämpfung schwerer Kriminalität – kann Eingriffe wie z. B. eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten oder von IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, für einen auf das absolut Notwendige begrenzten Zeitraum rechtfertigen [28].

2. Anwendung dieser Rechtsprechung auf das vorliegende Vorabentscheidungsersuchen

55. Nach den Ausführungen des vorlegenden Gerichts wurden die streitigen Daten mittels schwerwiegender Eingriffe in die durch die Art. 7, 8 und 11 der Charta gewährleisteten Grundrechte erlangt [29].

56. Wie ich bereits ausgeführt habe, geht es im vorliegenden Fall nicht um die Prüfung der Rechtmäßigkeit der ursprünglichen Erlangung dieser Daten, d. h. darum, ob der Eingriff aufgrund der Schwere des Delikts, gegen das vorgegangen werden sollte, hinreichend gerechtfertigt war.

[25] Urteil Commissioner of An Garda Síochána, Rn. 56.

[26] Urteil La Quadrature du Net, Rn. 135 und 136, in dem festgestellt wird, dass die nationale Sicherheit in die alleinige Verantwortung des Staates fällt und dass diese Verantwortung dem zentralen Anliegen entspricht, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft vor Tätigkeiten zu schützen, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten. Derartige Bedrohungen unterscheiden sich aufgrund ihrer Art und ihrer besonderen Schwere von der allgemeinen Gefahr des Auftretens selbst schwerer Spannungen oder Störungen im Bereich der öffentlichen Sicherheit. Das Ziel des Schutzes der nationalen Sicherheit ist daher geeignet, Maßnahmen zu rechtfertigen, die schwerere Grundrechtseingriffe enthalten als solche, die mit den übrigen Zielen gerechtfertigt werden könnten.

[27] Urteil Commissioner of An Garda Síochána, Rn. 58.

[28] Urteil La Quadrature du Net, Rn. 168.

[29] Dies ergibt sich aus Nr. 46 der Vorlageentscheidung. Dort wird auf Daten Bezug genommen, die Informationen über die Kommunikationen des Nutzers eines elektronischen Kommunikationsmittels oder über den Standort der von ihm verwendeten Endgeräte liefern können, aus denen sich genaue Schlüsse auf das Privatleben der betreffenden Personen ziehen lassen.

57. Zu diesen beiden Punkten (Schwere des Eingriffs und Schwere der Straftat) hat das vorlegende Gericht Feststellungen getroffen, die im Ausgangsverfahren nicht zur Debatte stehen und die deshalb für das Vorabentscheidungsersuchen nicht relevant sind.

58. Vorliegend ist, wie das vorlegende Gericht es ausgedrückt hat, zu klären, ob diese Daten a) auch in späteren Ermittlungsverfahren, die der Bekämpfung der Kriminalität im Allgemeinen dienen (unterstellt, das Verhalten, das Gegenstand der streitigen Disziplinarstrafe ist, fällt unter diesen Begriff), oder b) ausschließlich bei Ermittlungen zur Bekämpfung schwerer Kriminalität genutzt werden dürfen.

59. Die tschechische und die irische Regierung haben geprüft, ob das Verhalten, um das es vor dem vorlegenden Gericht geht, als „schwere Straftat" einzustufen ist, und haben dies bejaht.

60. Meines Erachtens ist dieser Gesichtspunkt jedoch vom Gerichtshof nicht zu prüfen, da die Einstufung des Verhaltens Sache des vorlegenden Gerichts ist.

61. Das vorlegende Gericht führt aus, wenn die Nutzung von Daten, die mittels eines schwerwiegenden Eingriffs in die Grundrechte erlangt worden seien, nur zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit gerechtfertigt werden könne, dürften diese Daten bei Ermittlungen wegen Disziplinarvergehen im Zusammenhang mit Korruption nicht herangezogen werden [30]. Mithin bei Ermittlungen wie denen, um die es in dieser Rechtssache geht.

62. Ausgehend von diesen Erwägungen ist zu klären, ob die Disziplinarvergehen, bei deren Verfolgung bestimmte personenbezogene Daten genutzt werden sollen, hinsichtlich ihrer Schwere den Straftaten, bei denen die Erlangung solcher Daten gerechtfertigt ist, qualitativ gleichwertig sein müssen [31].

63. In der mündlichen Verhandlung hat die litauische Regierung anerkannt, dass der zur Rechenschaft gezogene Staatsanwalt wegen eines Dienstvergehens aus dem Amt entfernt wurde. Ob dieses Vergehen (die Weitergabe von Informationen über ein Ermittlungsverfahren) einer schweren Straftat gleichgestellt werden oder mit einer ernsten Gefahr für den Schutz der öffentlichen Sicherheit und Ordnung verbunden sein kann, hängt von einer Reihe von Faktoren ab, die allein vom vorlegenden Gericht geprüft werden können [32].

64. In der mündlichen Verhandlung ist mehrfach auf den Kampf gegen die Korruption hingewiesen worden, bei der es sich um ein Phänomen handele, das zu Verhaltensweisen wie den hier in Rede stehenden führe. Die Debatte über diesen Punkt müsse im Hinblick auf die bei allen Manifestationen der staatlichen Strafbefugnis erforderliche Stringenz sehr nuanciert geführt werden. So müsse z. B. geklärt werden, ob der Begriff „Korruption" generisch gebraucht werde

[30] Vorlageentscheidung, Nr. 46 a. E.

[31] Im Urteil des Europäischen Gerichtshofs für Menschenrechte (EGMR) vom 18. Januar 2022, Adomaitis/Litauen (CE:ECHR:2022:0118JUD001483318, im Folgenden: Urteil Adomaitis des EGMR), in dem es um das Abhören elektronischer Kommunikationen im Fall des fortgesetzten Machtmissbrauchs seitens des Leiters einer Strafanstalt geht, finden sich Leitlinien für die Bewertung dieser Gleichwertigkeit.

[32] Grundsätzlich sind strafbare Handlungen, die in einem Strafverfahren geahndet werden, nicht mit reinen Dienstvergehen gleichzusetzen, die in einem Disziplinarverfahren geahndet werden. Das Strafverfahren und das Disziplinarverfahren unterscheiden sich hinsichtlich ihres Gegenstands, ihres Wesens und der Schwere des zu beurteilenden Verhaltens. Die Verschiedenheit der Verfahren ist insofern ein Indiz für die unterschiedliche Schwere ihres jeweiligen Gegenstands.

oder ob mit ihm eine bestimmte Verhaltensweise gemeint sei, so dass es möglicherweise abstrakt betrachtet zu weit ginge, die bloße Verletzung einer Geheimhaltungspflicht, die nicht mit einem entsprechenden Vorteil für den Amtsträger einhergehe, darunter zu fassen [33].

65. Wäre das vorlegende Gericht der Auffassung, dass das im vorliegenden Fall geahndete Dienstvergehen von geringerer Schwere ist als die Straftat, deren Untersuchung die Anwendung der gemäß Art. 15 der Richtlinie 2002/58 erlassenen Rechtsvorschrift rechtfertigte, ergäbe sich die Antwort auf die Vorlagefrage jedenfalls aus folgenden Ausführungen des Gerichtshofs:

– „[D]er Zugang zu von Betreibern in Anwendung einer gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassenen Rechtsvorschrift auf Vorrat gespeicherten Verkehrs- und Standortdaten, der unter vollständiger Beachtung der sich aus der Rechtsprechung zur Auslegung der Richtlinie 2002/58 ergebenden Voraussetzungen zu erfolgen hat, [kann] grundsätzlich nur mit dem dem Gemeinwohl dienenden Ziel gerechtfertigt werden, zu dem die Speicherung den Betreibern auferlegt wurde. Etwas anderes gilt nur, wenn die Bedeutung des mit dem Zugang verfolgten Ziels die Bedeutung des Ziels, das die Speicherung gerechtfertigt hat, übersteigt …“ [34]

– „[I]nsbesondere [kann] keinesfalls ein Zugang zu solchen Daten zwecks Verfolgung und Ahndung einer gewöhnlichen Straftat gewährt werden …, wenn ihre Speicherung mit dem Ziel der Bekämpfung schwerer Kriminalität oder gar dem Schutz der nationalen Sicherheit gerechtfertigt wurde.“ [35]

66. Insoweit ist also gewissermaßen von einem Grundsatz der Gleichwertigkeit zwischen den dem Gemeinwohl dienenden Zielen, die die *Erlangung* personenbezogener Daten rechtfertigen, und jenen Zielen auszugehen, die ihre spätere *Nutzung* rechtfertigen. Wie bereits dargelegt, besteht die einzige Ausnahme von diesem Grundsatz darin, dass die Bedeutung des mit dem Zugang verfolgten Ziels höher zu bewerten ist als das Ziel, das die Speicherung rechtfertigte.

67. Eine andere Betrachtungsweise würde das System der mit der Richtlinie 2002/58 gewährten Garantien verfälschen: Die von ihr geschützten Rechte könnten Gegenstand schwerwiegender Eingriffe sein, die nicht zu den in ihrem Art. 15 genannten Fallgruppen gehören und nicht den in der Rechtsprechung des Gerichtshofs festgelegten Bedingungen entsprechen.

68. Insbesondere ist ein Verzicht auf die Unversehrtheit des Rechts auf Vertraulichkeit der Kommunikation nur nach Maßgabe des damit verfolgten konkreten Gemeinwohlziels zulässig. Deshalb ist die Rechtmäßigkeit des Zugangs zu den gespeicherten Daten von Fall zu Fall zu prüfen, wobei die jeweilige Schwere des Eingriffs und die Bedeutung seines dem Gemeinwohl dienenden Ziels gegeneinander abzuwägen sind.

[33] In dem Übereinkommen aufgrund von Artikel K.3 Absatz 2 Buchstabe c) des Vertrags über die Europäische Union über die Bekämpfung der Bestechung, an der Beamte der Europäischen Gemeinschaften oder der Mitgliedstaaten der Europäischen Union beteiligt sind (ABl. 1997, C 195, S. 2) werden Fälle der Bestechlichkeit („[D]er Tatbestand der Bestechlichkeit [ist] dann gegeben, wenn ein Beamter vorsätzlich unmittelbar oder über eine Mittelsperson für sich oder einen Dritten Vorteile jedweder Art als Gegenleistung dafür fordert, annimmt oder sich versprechen lässt, dass er unter Verletzung seiner Dienstpflichten eine Diensthandlung oder eine Handlung bei der Ausübung seines Dienstes vornimmt oder unterlässt.“) und der Bestechung („[D]er Tatbestand der Bestechung [ist] dann gegeben, wenn eine Person vorsätzlich einem Beamten unmittelbar oder über eine Mittelsperson einen Vorteil jedweder Art für ihn selbst oder für einen Dritten als Gegenleistung dafür verspricht oder gewährt, dass der Beamte unter Verletzung seiner Dienstpflichten eine Diensthandlung oder eine Handlung bei der Ausübung seines Dienstes vornimmt oder unterlässt.“) behandelt, die als Straftaten einzustufen sind.

[34] Urteil Commissioner of An Garda Síochána, Rn. 98.

[35] Urteil La Quadrature du Net, Rn. 166.

69. Die Richtlinie 2002/58 kann aber nicht dahin ausgelegt werden, dass nach der Gewährung des Zugangs in einem ersten Fall, in dem es eine Rechtfertigung dafür gab, der Weg frei wäre für einen späteren Zugang (*de facto* eine erneute Nutzung der erlangten Daten), der auf ein in der Hierarchie niedriger angesiedeltes Ziel gestützt wird als der ursprüngliche Fall.

70. Insoweit sind die für den ursprünglichen Zugang bestehenden Anforderungen (einschließlich der vom Gerichtshof aufgestellten) [36] auf die spätere Nutzung der gleichen Daten durch andere Behörden übertragbar.

C. Hilfsweise: Auswirkung der Richtlinie 2016/680

71. Bislang habe ich mich mit der meines Erachtens angemessensten, am Wortlaut der Vorlageentscheidung orientierten Antwort auf das Ersuchen befasst, die darin besteht, dem vorlegenden Gericht, wie von ihm erbeten, die Auslegung der Richtlinie 2002/58 zu erleichtern.

72. Sollten die Daten, um die es in dieser Rechtssache geht, nicht im Rahmen von Art. 15 Abs. 1 der Richtlinie 2002/58 erlangt worden sein, sondern unmittelbar von der Kriminalpolizei des Mitgliedstaats in einem Strafverfahren, hätten wir es mit einem anderen Szenario zu tun.

73. In diesem Fall kämen – unbeschadet der Anwendung der Richtlinie 2016/680 in Bezug auf die Verarbeitung personenbezogener Daten, die bei strafrechtlichen Ermittlungen erlangt wurden – die nationalen Rechtsvorschriften ins Spiel. Ich gehe davon aus, dass das Tätigwerden der Kriminalpolizei in solchen Fällen in den Anwendungsbereich der Richtlinie 2016/680 fällt. Dies ist in der mündlichen Verhandlung bestätigt worden.

74. Wie ich in meinen Schlussanträgen in der Rechtssache Inspektor v Inspektorata kam Visshia sadeben savet (Zwecke der Verarbeitung personenbezogener Daten – Strafrechtliche Ermittlungen) ausgeführt habe [37], stellen die DSGVO und die Richtlinie 2016/680 „ein in sich kohärentes System dar, in dem

– die DSGVO die *allgemeinen Vorschriften* zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten festlegt,

– die Richtlinie 2016/680 *Spezialvorschriften* für die Verarbeitung dieser Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit enthält.“ [38]

75. Ich habe hinzugefügt [39]:

– „Der durch diese beiden Rechtsakte gewährte Schutz beruht auf den Grundsätzen der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben, der Transparenz und, was hier besonders von Interesse ist, dem Grundsatz der strengen Beschränkung der Erhebung und Verarbeitung von Daten auf die gesetzlich festgelegten Zwecke.“

– „Insbesondere sieht Art. 5 Abs. 1 Buchst. b der DSGVO vor, dass die Daten ‚für festgelegte, eindeutige und legitime Zwecke erhoben werden und … *nicht in einer mit diesen Zwecken*

[36] Urteil Commissioner of An Garda Síochána, Rn. 106 und das dort angeführte Urteil Prokuratuur, Rn. 51.

[37] C-180/21 (EU:C:2022:406), im Folgenden: Schlussanträge Inspektor v Inspektorata.

[38] Schlussanträge Inspektor v Inspektorata, Nr. 35.

[39] Schlussanträge Inspektor v Inspektorata, Nrn. 36 bis 39.

nicht zu vereinbarenden Weise weiterverarbeitet werden [dürfen]'; eine entsprechende Formulierung findet sich in der *lex specialis*, Art. 4 Abs. 1 Buchst. b der Richtlinie 2016/680."

– „Somit dürfen personenbezogene Daten nicht generell erhoben und verarbeitet werden, sondern nur zu bestimmten Zwecken und unter den vom Unionsgesetzgeber festgelegten Bedingungen der Rechtmäßigkeit." [40]

– „Der Grundsatz einer engen Verknüpfung zwischen der Erhebung und Verarbeitung der Daten einerseits und den Zwecken, denen beide Vorgänge dienen sollen, andererseits ist aber nicht absolut, da sowohl die DSGVO als auch die Richtlinie 2016/680 … eine gewisse Flexibilität ermöglichen."

76. Demnach kann es unter Zugrundelegung der Auslegung von Art. 4 Abs. 2 der Richtlinie2016/680 durch den Gerichtshof[41] wohl kaum als zulässig erachtet werden, dass die in einem Strafverfahren gesammelten personenbezogenen Daten *zu demselben Zweck* im Kontext eines späteren Disziplinarverfahrens gegen einen Amtsträger genutzt werden.

77. Nach Art. 4 Abs. 2 der Richtlinie 2016/680 ist allerdings „[e]ine Verarbeitung durch denselben oder einen anderen Verantwortlichen für einen anderen der in Artikel 1 Absatz 1 genannten Zwecke als den, für den die personenbezogenen Daten erhoben werden, … erlaubt, sofern

– der Verantwortliche nach dem Unionsrecht oder dem Recht der Mitgliedstaaten befugt ist, solche personenbezogenen Daten für diesen anderen Zweck zu verarbeiten, und

– die Verarbeitung für diesen anderen Zweck nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich und verhältnismäßig ist."

78. Ausgehend von dieser Prämisse wird das vorlegende Gericht zu prüfen haben, ob der (*andere*) Zweck der späteren Verarbeitung zu den in Art. 1 Abs. 1 der Richtlinie 2016/680 genannten Zwecken gehört oder nicht:

– Im erstgenannten Fall (Umwidmung *ad intra*) wird zu prüfen sein, ob die beiden Voraussetzungen von Art. 4 Abs. 2 der Richtlinie 2016/680 erfüllt sind.

– Im letztgenannten Fall (Umwidmung *ad extra*) kommt Art. 9 Abs. 1 der Richtlinie 2016/680 ins Spiel.

[40] Das Erfordernis der „Rechtmäßigkeit" wird in Art. 5 Abs. 1 Buchst. a der DSGVO (Art. 4 Abs. 1 Buchst. a der Richtlinie 2016/680) aufgestellt, und in Art. 6 der DSGVO werden die Bedingungen dafür erläutert. Insoweit ist zu beachten, dass nach Art. 6 Abs. 1 Buchst. e der DSGVO die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich sein muss, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem (für die Verarbeitung) Verantwortlichen übertragen wurde.

[41] Urteil vom 8. Dezember 2022, Inspektor v Inspektorata kam Visshia sadeben savet (Zwecke der Verarbeitung personenbezogener Daten – Strafrechtliche Ermittlungen) (C-180/21, EU:C:2022:967, im Folgenden: Urteil Inspektor v Inspektorata).

1. Nutzung der Daten gemäß Art. 4 Art. 2 der Richtlinie 2016/680

79. Nach der *ersten* der beiden in dieser Vorschrift vorgesehenen Voraussetzungen kommt es nur darauf an, ob das Recht des Mitgliedstaats ein Gesetz enthält [42], das regelt, unter welchen Voraussetzungen der Verantwortliche zur Verarbeitung der personenbezogenen Daten befugt ist. Es muss darüber hinaus bindende, klare und präzise Regeln enthalten [43].

80. Dieser Gesichtspunkt ist jedoch naturgemäß vom vorlegenden Gericht auf der Grundlage von Art. 177 BPK, Art. 19 Abs. 3 LIC und der Empfehlungen der Generalstaatsanwaltschaft zu beurteilen [44]. Anhand dieser Elemente ist zu prüfen, inwieweit das nationale Recht es zulässt, dass im Rahmen eines Strafverfahrens erhobene Informationen unter bestimmten Bedingungen im Kontext der Ermittlungen wegen Disziplinarvergehen genutzt werden können. Bei dieser Prüfung können sich die Erwägungen im Urteil Adomaitis des EGMR [45] als nützlich erweisen.

81. Hinsichtlich der *zweiten* Voraussetzung wird das vorlegende Gericht prüfen müssen, ob bei der im vorliegenden Rechtsstreit in Rede stehenden Verarbeitung von Daten ein Eingriff erforderlich war und ob dieser verhältnismäßig war [46].

82. Bei dieser Prüfung können die Ausführungen im Urteil Adomaitis des EGMR erneut hilfreich sein:

– Was die Erforderlichkeit anbelangt, ist zu untersuchen, inwieweit der Ausgang des laufenden Ermittlungsverfahrens es angesichts der unzureichenden Beweiskraft anderer im Disziplinarverfahren verfügbarer Daten tatsächlich erforderlich machte, die streitigen Daten heranzuziehen [47].

– Bei der Frage der Verhältnismäßigkeit ist die Schwere des Verstoßes, der zu dem Disziplinarverfahren führte, zu beurteilen; dabei ist zu berücksichtigen, dass nach dem Vorbringen der litauischen Regierung und den Ausführungen im Urteil Adomaitis des EGMR [48] die Nutzung personenbezogener Daten auf Fälle von Verstößen beschränkt ist, für die die schwerste Disziplinarstrafe – die Entlassung – vorgesehen ist.

2. Nutzung der Daten gemäß Art. 9 der Richtlinie 2016/680

83. Gemäß Art. 9 Abs. 1 der Richtlinie 2016/680 können personenbezogene Daten, die von zuständigen Behörden für die in ihrem Art. 1 Abs. 1 genannten Zwecke erhoben werden, für andere als die in Art. 1 Abs. 1 genannten Zwecke verarbeitet werden, wenn eine derartige

[42] Ich stimme der Kommission zu, dass die spätere Nutzung der in einem strafrechtlichen Ermittlungsverfahren erlangten personenbezogenen Daten einen Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte darstellt, so dass eine solche Nutzung nach Art. 52 Abs. 1 der Charta nur zulässig ist, wenn sie gesetzlich vorgesehen ist.

[43] Siehe oben, Nr. 51.

[44] Siehe oben, Fn. 12.

[45] In § 83 dieses Urteils wird es als ausreichend angesehen, dass die Rechtmäßigkeit des Eingriffs durch nationale Rechtsvorschriften und die Rechtsprechung des litauischen Verfassungsgerichts gewährleistet wird.

[46] Wie die Kommission ausführt, unterscheidet sich diese Rechtssache nicht wesentlich von der Rechtssache, zu der das Urteil des EGMR vom 16. Juni 2016, Versini-Campinchi und Crasnianski/Frankreich (CE:ECHR:2016:0616JUD004917611), ergangen ist. Nach § 57 dieses Urteils dient die Nutzung der in einem Strafverfahren überwachten Kommunikationen im Rahmen eines die Verletzung des Berufsgeheimnisses betreffenden Disziplinarverfahrens einem legitimen Ziel im Sinne von Art. 8 der EMRK. Die enge inhaltliche Verflechtung der Gegenstände von Strafverfahren und Disziplinarverfahren führt dazu, dass es auch bei der Rechtmäßigkeit der Zwecke dieser beiden Verfahren Gemeinsamkeiten gibt.

[47] Urteil Adomaitis des EGMR, § 85.

[48] Urteil Adomaitis des EGMR, § 87.

Verarbeitung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist. In diesem Fall gilt die DSGVO, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt [49].

84. Sollte das vorlegende Gericht Art. 4 Abs. 2 der Richtlinie 2016/680 für unanwendbar halten, ist die DSGVO heranzuziehen. In ihrem Rahmen wird zu klären sein, ob neben der gesetzlichen Regelung zumindest eine der in ihrem Art. 6 Abs. 1 abschließend aufgeführten Voraussetzungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten vorliegt.

V. Ergebnis

85. Nach alledem schlage ich dem Gerichtshof vor, dem Lietuvos vyriausiasis administracinis teismas (Oberstes Verwaltungsgericht, Litauen) wie folgt zu antworten:

1. Art. 15 Abs. 1 der 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) in Verbindung mit den Art. 7, 8, 11 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union

   ist dahin auszulegen, dass

   es den zuständigen Behörden nicht gestattet ist, von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherte Daten, die detaillierte Informationen über einen Nutzer liefern können, zu erheben und diese Daten in Ermittlungsverfahren wegen Verhaltensweisen zu nutzen, die Verstöße von geringerer Schwere darstellen als diejenigen, deren Untersuchung den Zugang zu den Daten seinerzeit rechtfertigen konnte.

2. Hilfsweise:

   Art. 9 Abs. 1 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 in Verbindung mit den Art. 6 und 10 der 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 und im Licht der Art. 7 und 8 der Charta der Grundrechte der Europäischen Union

   ist dahin auszulegen, dass

   er der Nutzung personenbezogener Daten, die von staatlichen Stellen im Rahmen strafrechtlicher Ermittlungen rechtmäßig und unmittelbar erlangt wurden, in einem verwaltungsrechtlichen Disziplinarverfahren nicht entgegensteht, falls das betreffende Verfahren und die Ermittlungen anhand klarer, präziser und bindender Vorschriften des

[49] Diese Ausnahme wurde im Urteil vom 22. Juni 2021, Latvijas Republikas Saeima (Strafpunkte) (C-439/19, EU:C:2021:504, Rn. 66), restriktiv ausgelegt.

nationalen Rechts miteinander verknüpft sind und soweit die Nutzung der Daten einem legitimen Zweck dient sowie erforderlich und verhältnismäßig ist; dies zu klären ist Sache der Justizbehörde.