Rechtssache C-817/19

Zusammenfassung des Vorabentscheidungsersuchens gemäß Art. 98 Abs. 1 der Verfahrensordnung des Gerichtshofs

Eingangsdatum:

31. Oktober 2019

Vorlegendes Gericht:

Cour constitutionnelle (Verfassungsgerichtshof, Belgien)

Datum der Vorlageentscheidung:

17. Oktober 2019

Klägerin:

ASBL „Ligue des droits humains“

I. Streitgegenstand und Vorbringen der Parteien

1 Der belgische Gesetzgeber hat das Gesetz vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten (Moniteur belge vom 25. Januar 2017, im Folgenden auch: PNR-Gesetz) erlassen, um im Wesentlichen folgende Richtlinien umzusetzen:

– die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 „über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität“ (im Folgenden auch: PNR-Richtlinie),

– die Richtlinie 2004/82/EG des Rates vom 29. April 2004 „über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln“ (im Folgenden auch: API-Richtlinie).

2 Das PNR-Gesetz verpflichtet verschiedene Sektoren der internationalen Beförderung von Personen (auf dem Luft-, Eisenbahn-, internationalen Straßen- und Seeweg) sowie Reiseunternehmen, die Daten ihrer Passagiere an eine vom Föderalen Öffentlichen Dienst Inneres verwaltete Datenbank zu übermitteln.

3 Zu diesem Zweck errichtet das Gesetz innerhalb des Föderalen Öffentlichen Dienstes Inneres eine „PNR-Zentralstelle“ (Art. 12 bis 14), die sich u. a. aus

entsandten Mitgliedern der Polizeidienste, der Staatssicherheit, der Nachrichten- und Sicherheitsdienste und des Zolls zusammensetzt und insbesondere für die Erhebung, Aufbewahrung und Verarbeitung der Passagierdaten, die von den Beförderungsunternehmen und Reiseunternehmen übermittelt werden, verantwortlich ist.

4 Die „Passagierdatenbank“ enthält zum einen die Buchungsdaten und zum anderen die Daten des Eincheckstatus und des Anbordgehens (sogenannte „API-Daten“ [Advance Passenger Information] und sogenannte „PNR-Daten“ [Passenger Name Record]) (Art. 9).

5 Diese Daten werden u. a. zu Zwecken der Ermittlung, Verfolgung und Vollstreckung von Strafen in Bezug auf im Gesetz erwähnte Straftaten sowie der Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung, der Beaufsichtigung der Aktivitäten durch Nachrichten- und Sicherheitsdienste und zur Verbesserung der Personenkontrollen an den Außengrenzen und zur Bekämpfung der illegalen Einwanderung verarbeitet (Art. 8).

6 Die Daten können im Rahmen der Vorabüberprüfung der Passagiere (vor ihrer Abreise oder ihrer Ankunft) (Art. 24 bis 26) oder im Rahmen gezielter Recherchen (Art. 27) verarbeitet werden.

7 Das Gesetz sieht vor, dass die Passagierdaten höchstens fünf Jahre ab ihrer Speicherung in der Passagierdatenbank aufbewahrt werden (Art. 18 bis 23).

8 Die ASBL „Ligue des droits humains“ beanstandet das Gesetz in den folgenden sieben Einzelpunkten:

– den Durchführungsmodalitäten des Gesetzes vom 25. Dezember 2016 (Art. 3 § 2 und Art. 7 § 3),

– den Begriffen „Identität[sdokumente]“ und „Reisedokumente“ (Art. 7 §§ 1 und 2),

– den genannten Daten (Art. 4 Nr. 9 und Art. 9),

– dem Begriff „Passagier“ (Art. 4 Nr. 10),

– den Zwecken der Verarbeitung der „PNR-Daten“ (Art. 8),

– der Verwaltung der Passagierdatenbank und der Verarbeitung der Daten im Rahmen der Vorabüberprüfung der Passagiere und gezielter Recherchen (Art. 12 bis 16, 24 bis 27, 50 und 51),

– der Aufbewahrungsdauer der PNR-Daten (Art. 18).

9 Sie macht insoweit Unregelmäßigkeiten geltend und hat beim Verfassungsgerichtshof Nichtigkeitsklage erhoben, die auf zwei Klagegründe gestützt wird.

10 Der *erste Klagegrund* stützt sich im Wesentlichen auf Art. 23 der Verordnung (EU) 2016/679[1], auf Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) und auf Art. 8 der Europäischen Menschenrechtskonvention (im Folgenden: EMRK).

11 Sie macht im Wesentlichen geltend, dass der Eingriff in das Recht auf Achtung des Privatlebens und in das Recht auf den Schutz personenbezogener Daten rechtswidrig sei, weil er die Kriterien der *Gesetzmäßigkeit*, der *Notwendigkeit* und der *Verhältnismäßigkeit* nicht erfülle.

12 Zunächst räume das PNR-Gesetz der Exekutive einen weiten Wertungsspielraum ein, indem es ihr aufgebe, bestimmte wesentliche Bestandteile durch Königlichen Erlass zu definieren, was gegen den Grundsatz der Gesetzmäßigkeit verstoße, der verlange, dass der Eingriff gesetzlich vorgesehen sei oder im Fall der Delegation an den König die wesentlichen Bestandteile hinreichend genau und detailliert durch das Gesetz bestimmt seien.

Zudem verfolge das angefochtene Gesetz kein legitimes Ziel. Es sehe nämlich eine Vorabüberprüfung vor, ein sogenanntes *pre-screening*, das darin bestehe, das Risiko zu bewerten, das die Passagiere vor ihrer Ankunft im nationalen Hoheitsgebiet, ihrer Durchreise durch dieses Gebiet oder ihrer Abreise aus diesem Gebiet darstellten.

13 Ferner bestreitet die Klägerin, dass die angefochtenen Maßnahmen notwendig seien, um das angestrebte Ziel zu erreichen.

Sie macht geltend, das angestrebte Ziel könne auch mit einem Datenabgleich erreicht werden, der weit weniger in das Privatleben eindringe als die Schaffung einer Datenbank.

14 Schließlich macht sie geltend, das angefochtene Gesetz verstoße gegen den Grundsatz der Verhältnismäßigkeit, weil die Daten von den Betreibern undifferenziert und generell erhoben und an die zuständigen Behörden zur Speicherung für fünf Jahre ohne Unterscheidung, Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel übermittelt würden.

[1] 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 (im Folgenden auch: DSGVO).

15 Im Einzelnen missachte das Gesetz den Grundsatz der Verhältnismäßigkeit in Bezug auf (a) seinen Anwendungsbereich und die Kategorien der in ihm genannten Daten, (b) die von ihm vorgesehene Verarbeitung der Daten, (c) seine Ziele und (d) die Dauer der Aufbewahrung der Daten.

16 Als Erstes definiere das angefochtene Gesetz die erhobenen Daten, die offensichtlich über das hinausgingen, was unbedingt erforderlich sei, sehr weit.

17 Die Klägerin stellt fest, dass das *pre-screening* offenbar – insoweit sei das Gesetz nicht klar – in der zentralen Datenbank der PNR-Zentralstelle durchgeführt werden solle, und zwar anhand im Voraus festgelegter Kriterien, die als Indikatoren für die Bedrohung dienten. Das PNR-Gesetz definiere aber weder die präzise Art der für den Abgleich verwendeten Datenbanken noch die Modalitäten dieses Abgleichs. Das PNR-Gesetz sehe auch nicht vor, dass dieser Abgleich auf die Datenbanken beschränkt sei, die im Zusammenhang mit der Bekämpfung des Terrorismus und der schweren Kriminalität betrieben würden.

18 Die Klägerin beanstandet auch die gezielten Recherchen, die das Gesetz vorsehe, ohne die tatsächlich zugänglichen Daten zu präzisieren.

19 Sie rügt auch die Ziele der Datenverarbeitung, die deutlich über das hinausgingen, was die PNR-Richtlinie vorsehe, wie die Bekämpfung der illegalen Einwanderung, von Aktivitäten, die eine Gefahr für die grundlegenden Interessen des Staates darstellten, oder auch die Bekämpfung der „gewalttätigen Radikalisierung“, die lediglich in einem Rundschreiben definiert werde.

20 Schließlich beanstandet die Klägerin die Aufbewahrungsdauer der Daten von fünf Jahren. Der Gesetzgeber habe seine Entscheidung für die nach der PNR-Richtlinie gestattete Höchstdauer in keiner Weise gerechtfertigt, was die Unverhältnismäßigkeit der Maßnahme aufzeige.

21 Der Ministerrat (der das Gesetz verteidigt) macht in erster Linie geltend, dass der erste Klagegrund unzulässig sei, weil er sich auf einen Verstoß gegen Art. 23 der DSGVO stütze, obwohl sowohl aus dem 19. Erwägungsgrund der DSGVO als auch aus Art. 1 der PNR-Richtlinie eindeutig hervorgehe, dass die Verarbeitung von „PNR-Daten“ nicht unter die DSGVO falle, sondern unter die justizielle und polizeiliche Zusammenarbeit zwischen den Mitgliedstaaten und unter die Richtlinie (EU) 2016/680 [2].

22 Außerdem macht der Ministerrat geltend, dass der Grundsatz der Gesetzmäßigkeit nicht verletzt sei, weil das Gesetz die wesentlichen Bestandteile der Maßnahmen

[2] 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) (im Folgenden: Richtlinie 2016/680).

enthalte, die es vorsehe, und die dem König erteilte Ermächtigung hinreichend präzise sei. Im Übrigen sei das Erfordernis der Gesetzmäßigkeit dem Europäischen Gerichtshof für Menschenrechte zufolge im materiellen Sinn zu verstehen, so dass Rechtsakte mit Verordnungscharakter den Begriff „Gesetz“ im Sinne der EMRK erfüllten.

Das PNR-Gesetz ziele darauf ab, die öffentliche Sicherheit zu gewährleisten, indem es nicht nur die Verfolgung terroristischer Straftaten oder bestimmter Formen schwerer Kriminalität erlaube, sondern auch die Verhütung dieser Straftaten mit Hilfe einer Vorabanalyse erhobener Daten. Der Gerichtshof habe diese Ziele sowohl in seinem Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), als auch in seinem Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017, EU:C:2017:592, als legitim im Sinne von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union anerkannt.

23 Der Ministerrat hält die angefochtenen Maßnahmen für verhältnismäßig.

24 Was die Schaffung einer „Passagierdatenbank“ betrifft, weist der Ministerrat darauf hin, dass die Klägerin sich auf die Behauptung beschränke – ohne sie zu beweisen –, dass ein Datenabgleich genügt hätte, um die verfolgten Ziele zu erreichen, und das Recht auf Achtung des Privatlebens weniger beeinträchtigt hätte. Er fügt hinzu, dass ein schlichter Datenabgleich nicht ausreichen würde, um die Vorabüberprüfungen zur Erkennung der Sicherheitsrisiken durchzuführen. Die Schaffung einer Datenbank erlaube es zudem, dem 25. Erwägungsgrund der PNR-Richtlinie nachzukommen, der dazu auffordere, die Daten für die Dauer zu speichern, die im Hinblick auf die verfolgten Ziele erforderlich sei.

25 Was die Korrelation zwischen den verschiedenen Datenbanken betrifft, weist der Ministerrat darauf hin, dass die Art. 24 und 25 des PNR-Gesetzes Art. 6 der PNR-Richtlinie umsetzten. Außerdem gehe aus den Materialien hervor, dass der Gesetzgeber nicht beabsichtige, eine Korrelation der „Passagierdatenbank“ mit sämtlichen Datenbanken herbeizuführen, zu denen die zuständigen Behörden Zugang hätten, sondern nur zwischen der „Passagierdatenbank“ und den Datenbanken, die den vom angefochtenen Gesetz verfolgten Zielen entsprächen. Diese Maßnahmen seien mit den Lehren aus dem Gutachten 1/15 des Gerichtshofs vereinbar, weil auch Art. 6 Abs. 3 der PNR-Richtlinie nicht präzisiere, welche Datenbanken miteinander abgeglichen werden dürften. Ein Wertungsspielraum sei ebenfalls mit dem Grundsatz der Gesetzmäßigkeit in seiner Auslegung durch den Europäischen Gerichtshof für Menschenrechte vereinbar.

Zudem könne der Zweck des Gesetzes nicht erreicht werden, wenn die Reisenden vorab wüssten, welche Kriterien zu einer positiven Übereinstimmung führen würden, weil sie dann ihr Verhalten danach ausrichten könnten. Zudem bestimme Art. 16 des angefochtenen Gesetzes ganz klar, dass das *pre-screening* innerhalb der „Passagierdatenbank“ durchgeführt werde, was somit mit dem Grundsatz der Gesetzmäßigkeit im Einklang stehe.

26 Was die Aufbewahrungsdauer der Daten betrifft, hält der Ministerrat es nicht für unangemessen, eine Aufbewahrungsfrist von fünf Jahren vorzusehen, was im Übrigen der Mindestdauer der Verjährungsfrist für die Strafverfolgung in Bezug auf Vergehen und zu Vergehen umgestuften Verbrechen entspreche.

Die Aufbewahrungsdauer der Daten, die mit der von der PNR-Richtlinie vorgesehenen Dauer im Einklang stehe, sei daher keinesfalls unverhältnismäßig.

27 Der *zweite*, hilfsweise geltend gemachte *Klagegrund* stützt sich im Wesentlichen auf einen Verstoß gegen Art. 3 Abs. 2 AEUV in Verbindung mit Art. 45 der Charta.

28 Die Klägerin macht geltend, Art. 3 § 1, Art. 8 § 2 und Kapitel 11 des PNR-Gesetzes, das dessen Art. 28 bis 31 enthalte, verstießen gegen die Freizügigkeit, weil sie nicht nur die EU-Außengrenzen überschreitende Beförderungen, sondern auch Beförderungen innerhalb der EU (einschließlich Zwischenaufenthalten) beträfen. Die Klägerin ist mit anderen Worten der Auffassung, dass die angefochtenen Vorschriften durch die Ausweitung des „PNR-Systems“ auf Flüge innerhalb der EU indirekt wieder Grenzkontrollen einführten, die gegen die Freizügigkeit verstießen.

29 Der Ministerrat ist der Ansicht, das angefochtene Gesetz führe keineswegs Grenzkontrollen wieder ein und verstoße in keiner Weise gegen die Freizügigkeit. Die PNR-Richtlinie sei auf die illegale Einwanderung nicht anwendbar und das angefochtene Gesetz setze nicht nur die PNR-Richtlinie, sondern auch die API-Richtlinie um.

So, wie der Klagegrund formuliert sei, betreffe er nur Art. 3 § 1, Art. 8 § 2 und Kapitel 11 des angefochtenen Gesetzes. Aus der Definition des Begriffs „Außengrenzen“ gehe jedoch hervor, dass das PNR-Gesetz nur Kontrollen von Reisen aus und in Drittstaaten betreffe. Außerdem setze das PNR-Gesetz die Richtlinie 2004/82/EG um, so dass es nicht so angesehen werden könne, als führe es Grenzkontrollen innerhalb des Schengen-Raums wieder ein.

Äußerst hilfsweise weist der Ministerrat darauf hin, dass der zehnte Erwägungsgrund der PNR-Richtlinie ausdrücklich die Möglichkeit vorsehe, die Verwendung der „PNR-Daten“ auf Flüge innerhalb der EU auszudehnen, was zeige, dass diese Maßnahme für sich genommen weder gegen die Freizügigkeit noch gegen die Verordnung (EG) Nr. 562/2006 verstoße.

II. Rechtsrahmen

Europäische Menschenrechtskonvention

30 Art. 8 bestimmt:

„1. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer."

Unionsrecht

Charta der Grundrechte der Europäischen Union

31 Art. 7 („Achtung des Privat- und Familienlebens") der Charta bestimmt:

„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation."

32 Art. 8 („Schutz personenbezogener Daten") der Charta bestimmt:

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

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

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

33 Art. 52 Abs. 1 der Charta bestimmt:

„Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen."

Datenschutz-Grundverordnung (DSGVO)

34 Art. 2 Abs. 2 Buchst. d bestimmt:

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

…

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.“

35 Art. 23 bestimmt:

„(1) Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

a) | die nationale Sicherheit;

b) | die Landesverteidigung;

c) | die öffentliche Sicherheit;

d) | die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) | den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;

f) | den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

g) | die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h) | Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind;

i) | den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

j) | die Durchsetzung zivilrechtlicher Ansprüche.

(2) Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf

a) | die Zwecke der Verarbeitung oder die Verarbeitungskategorien,

b) | die Kategorien personenbezogener Daten,

c) | den Umfang der vorgenommenen Beschränkungen,

d) | die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung,

e) | die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,

f) | die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,

g) | die Risiken für die Rechte und Freiheiten der betroffenen Personen und

h) | das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.“

PNR-Richtlinie

36 Art. 3 lautet:

„Im Sinne dieser Richtlinie bezeichnet der Ausdruck

…

4. | ‚Fluggast‘ jede Person, einschließlich Transfer- oder Transitfluggästen, mit Ausnahme der Besatzungsmitglieder, die mit Zustimmung der Fluggesellschaft in einem Luftfahrzeug befördert wird oder befördert werden soll, wobei diese Zustimmung durch die Eintragung der Person in die Fluggastliste belegt wird“.

37 Art. 4 bestimmt:

„PNR-Zentralstelle

(1) Jeder Mitgliedstaat errichtet oder benennt eine für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten und schwerer Kriminalität zuständige Behörde oder eine Abteilung einer solchen Behörde, die als seine PNR-Zentralstelle handelt.

(2) Die PNR-Zentralstelle ist verantwortlich für

a) | die Erhebung der PNR-Daten bei Fluggesellschaften, für die Speicherung und Verarbeitung dieser Daten sowie die Übermittlung dieser Daten oder der Ergebnisse ihrer Verarbeitung an die zuständigen Behörden nach Artikel 7;

b) | den Austausch sowohl von PNR-Daten als auch der Ergebnisse der Verarbeitung dieser Daten mit den PNR-Zentralstellen anderer Mitgliedstaaten und mit Europol gemäß den Artikeln 9 und 10.

…“

38 Art. 6 bestimmt:

„(1) Die von den Fluggesellschaften übermittelten PNR-Daten werden von der PNR-Zentralstelle des betreffenden Mitgliedstaats gemäß Artikel 8 erhoben. Wenn die von Fluggesellschaften übermittelten PNR-Daten andere als die in Anhang I genannten Daten beinhalten, werden diese Daten von der PNR-Zentralstelle unmittelbar nach ihrem Eingang dauerhaft gelöscht.

(2) Die PNR-Zentralstelle verarbeitet PNR-Daten ausschließlich zu folgenden Zwecken:

a) | Überprüfung von Fluggästen vor ihrer planmäßigen Ankunft in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat, um diejenigen Personen zu ermitteln, die von den zuständigen Behörden gemäß Artikel 7 und gegebenenfalls – im Einklang mit Artikel 10 – von Europol genauer überprüft werden müssen, da sie möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind;

b) | im Einzelfall Beantwortung von auf einer hinreichenden Grundlage gebührend begründeten Anfragen zuständiger Behörden hinsichtlich der Zurverfügungstellung und Verarbeitung von PNR-Daten in besonderen Fällen zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität, und der Zurverfügungstellung der Ergebnisse dieser Verarbeitung an die zuständigen Behörden oder gegebenenfalls an Europol, und

c) | Analyse von PNR-Daten zwecks Aktualisierung der Kriterien oder Aufstellung neuer Kriterien zur Verwendung in gemäß Absatz 3 Buchstabe b durchgeführten Überprüfungen, die der Ermittlung von Personen gelten, die möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind.

…“

39 Art. 12 bestimmt:

„(1) Die Mitgliedstaaten stellen sicher, dass die von den Fluggesellschaften an die PNR-Zentralstelle übermittelten PNR-Daten für einen Zeitraum von fünf Jahren

ab ihrer Übermittlung an die PNR-Zentralstelle des Mitgliedstaats, in dessen Hoheitsgebiet der Flug angekommen beziehungsweise von dem er abgegangen ist, in einer bei dieser PNR-Zentralstelle angesiedelten Datenbank vorgehalten werden.

(2) Nach Ablauf einer Frist von sechs Monaten ab Übermittlung der PNR-Daten gemäß Absatz 1 werden alle PNR-Daten durch Unkenntlichmachung der folgenden Datenelemente, mit denen die Identität des Fluggasts, auf den sich die PNR-Daten beziehen, unmittelbar festgestellt werden könnte, depersonalisiert:

a) | Name(n), auch die Namen und die Zahl der im PNR-Datensatz verzeichneten mitreisenden Personen;

b) | Anschrift und Kontaktdaten;

c) | alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift, die zur unmittelbaren Feststellung der Identität des Fluggasts, zu dem die PNR-Daten erstellt wurden, oder anderer Personen beitragen könnten;

d) | Vielflieger-Eintrag;

e) | allgemeine Hinweise, die zur unmittelbaren Feststellung der Identität des Fluggastes beitragen könnten, zu dem die PNR-Daten erstellt wurden, und

f) | jedwede erhobenen API-Daten.

(3) Nach Ablauf der in Absatz 2 genannten Frist von sechs Monaten ist die Offenlegung der vollständigen PNR-Daten nur zulässig, wenn

a) | berechtigter Grund zu der Annahme besteht, dass dies für die Zwecke des Artikels 6 Absatz 2 Buchstabe b erforderlich ist und

b) | dies genehmigt wird durch

i) | eine Justizbehörde oder

ii) | eine andere nationale Behörde, die nach nationalem Recht dafür zuständig ist zu überprüfen, ob die Bedingungen für die Offenlegung erfüllt sind, vorbehaltlich der Unterrichtung des Datenschutzbeauftragten der PNR-Zentralstelle und einer Ex-Post-Überprüfung durch diesen Datenschutzbeauftragten.

(4) Die Mitgliedstaaten stellen sicher, dass die PNR-Daten nach Ablauf der Frist nach Absatz 1 dauerhaft gelöscht werden. Diese Verpflichtung lässt Fälle unberührt, in denen bestimmte PNR-Daten an eine zuständige Behörde übermittelt wurden und im Zusammenhang mit einem konkreten Fall zum Zwecke der Verhütung, Aufdeckung, Ermittlung oder Verfolgung terroristischer Straftaten oder schwerer Kriminalität verwendet werden; in diesem Fall richtet sich die Frist

für die Speicherung dieser Daten durch die zuständige Behörde nach nationalem Recht.

(5) Die Ergebnisse der Verarbeitung nach Artikel 6 Absatz 2 Buchstabe a werden von der PNR-Zentralstelle nur so lange vorgehalten, wie dies erforderlich ist, um die zuständigen Behörden und die PNR-Zentralstellen anderer Mitgliedstaaten gemäß Artikel 9 Absatz 1 über einen Treffer zu informieren. Fällt die in Artikel 6 Absatz 5 genannte anschließende individuelle nicht-automatisierte Überprüfung eines Treffers bei der automatisierten Verarbeitung negativ aus, so kann dieses Ergebnis dennoch gespeichert werden, um künftige ‚falsche' Treffer zu vermeiden, solange die dazugehörigen Daten nicht gemäß Absatz 4 dieses Artikels gelöscht sind."

40 Anhang I („Von Fluggesellschaften erhobene PNR-Daten") der PNR-Richtlinie erwähnt u. a.:

„ …

12. | Allgemeine Hinweise (einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Flughafenmitarbeiter bei Abflug und Ankunft)

…

18. | Etwaige erhobene erweiterte Fluggastdaten (API-Daten) (einschließlich Art, Nummer, Ausstellungsland und Ablaufdatum von Identitätsdokumenten, Staatsangehörigkeit, Familienname, Vorname, Geschlecht, Geburtsdatum, Fluggesellschaft, Flugnummer, Tag des Abflugs, Tag der Ankunft, Flughafen des Abflugs, Flughafen der Ankunft, Uhrzeit des Abflugs und Uhrzeit der Ankunft)

…"

API -Richtlinie

41 Art. 1 bestimmt:

„Zweck dieser Richtlinie ist es, die Grenzkontrollen zu verbessern und die illegale Einwanderung zu bekämpfen, indem die Beförderungsunternehmen Angaben über die beförderten Personen vorab an die zuständigen nationalen Behörden übermitteln."

Belgisches Recht

42 Die maßgeblichen Vorschriften des *PNR-Gesetzes* (in der durch die Gesetze vom 15. und 30. Juli 2018 und durch das Gesetz vom 2. Mai 2019 geänderten Fassung) lauten wie folgt:

„KAPITEL 2 – Anwendungsbereich

Art. 3 – § 1 – Vorliegendes Gesetz bestimmt die Verpflichtungen der Beförderungsunternehmen und Reiseunternehmen in Bezug auf die Übermittlung von Daten zu Passagieren, die in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet befördert werden.

§ 2 – Der König bestimmt durch einen im Ministerrat beratenen Erlass für jeden Beförderungssektor und für die Reiseunternehmen die zu übermittelnden Passagierdaten sowie die Übermittlungsmodalitäten nach Stellungnahme der für die Kontrolle der Verarbeitung personenbezogener Daten zuständigen Behörde.
…

KAPITEL 3 – Begriffsbestimmungen

Art. 4 – Für die Anwendung des vorliegenden Gesetzes und seiner Ausführungserlasse versteht man unter:

…

9. ‚PNR‘: den Datensatz mit den zu jedem einzelnen Passagier notwendigen Reisedaten, der die in Artikel 9 erwähnten Informationen enthält, die die Bearbeitung und Überprüfung der von einer Person oder in ihrem Namen getätigten Reservierungen für jede Reise durch die buchenden und beteiligten Beförderungsunternehmen und Reiseunternehmen ermöglichen, unabhängig davon, ob dieser Datensatz in Buchungssystemen, Abfertigungssystemen (zur Überprüfung der Passagiere beim Anbordgehen) oder gleichwertigen Systemen, die die gleichen Funktionen bieten, enthalten ist,

10. ‚Passagier‘: jede Person, einschließlich der Personen im Transfer- oder Transitverkehr, mit Ausnahme der Besatzungsmitglieder, die mit Zustimmung des Beförderungsunternehmens von ihm befördert wird oder befördert werden soll, wobei diese Zustimmung durch die Eintragung dieser Person in die Passagierliste belegt wird,

…

KAPITEL 5 – Zwecke der Datenverarbeitung

Art. 8 – § 1 – Die Passagierdaten werden zu folgenden Zwecken verarbeitet:

1. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die [im Strafprozessgesetzbuch] erwähnten Straftaten,

2. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die [im Strafgesetzbuch] erwähnten Straftaten,

3. Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung durch Beobachtung der Phänomene und Gruppierungen gemäß Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 über das Polizeiamt,

4. Beaufsichtigung der in den Artikeln 7 Nr. 1 und 3/1 und 11 § 1 Nr. 1 bis 3 und 5 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Aktivitäten,

5. Ermittlung und Verfolgung der Straftaten, erwähnt in [verschiedenen Gesetzen].

§ 2 – Die Passagierdaten werden unter den in Kapitel 11 erwähnten Bedingungen ebenfalls verarbeitet, um die Personenkontrolle an den Außengrenzen zu verbessern und die illegale Einwanderung zu bekämpfen.

KAPITEL 6 – Passagierdaten

Art. 9 – § 1 In Bezug auf die Buchungsdaten enthalten die Passagierdaten höchstens:

1. PNR-Buchungscode (Record Locator),

2. Datum der Buchung und der Fahr- beziehungsweise Flugscheinausstellung,

3. planmäßige Reisedaten,

4. Namen, Vornamen und Geburtsdatum,

5. Anschrift und Kontaktangaben (Telefonnummer, E-Mail-Adresse),

6. Zahlungsinformationen einschließlich Rechnungsanschrift,

7. den gesamten Reiseverlauf für den betreffenden Passagier,

8. Informationen zu den „registrierten Reisenden“, d. h. zu den „Vielreisenden“,

9. Reisebüro oder Sachbearbeiter,

10. Reisestatus des Reisenden mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Reisen (No show) oder Passagier mit Fahr- beziehungsweise Flugschein, aber ohne Reservierung (Go show),

11. Angaben über gesplittete oder geteilte PNR-Daten,

12. allgemeine Hinweise, einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktangaben der Begleitperson bei der Abreise und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktangaben der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Mitarbeiter bei der Abreise und der Ankunft,

13. Fahr- beziehungsweise Flugscheindaten einschließlich Fahr- beziehungsweise Flugscheinnummer, Ausstellungsdatum, einfache Fahrten beziehungsweise Flüge, informatisierte tarifbezogene Felder der Fahr- beziehungsweise Flugscheine,

14. Sitzplatznummer und sonstige Sitzplatzinformationen,

15. Code-Sharing,

16. vollständige Gepäckangaben,

17. Zahl und Namen von Mitreisenden im Rahmen der PNR-Daten,

18. etwaige erhobene erweiterte Passagierdaten (API-Daten), die in § 2 aufgezählt sind,

19. alle vormaligen Änderungen der unter den Nummern 1 bis 18 aufgeführten Daten.

§ 2 – In Bezug auf die Daten des Eincheckstatus und des Anbordgehens umfassen die in § 1 Nr. 18 erwähnten erweiterten Daten Folgendes:

1. Art des Reisedokuments,

2. Nummer des Reisedokuments,

3. Staatsangehörigkeit,

4. Land, das das Dokument ausgestellt hat,

5. Ablaufdatum des Dokuments,

6. Familienname, Vorname, Geschlecht, Geburtsdatum,

7. Beförderungsunternehmen/Reiseunternehmen,

8. Beförderungsnummer,

9. Abreisedatum, Ankunftsdatum,

10. Abreiseort, Ankunftsort,

11. Abreisezeit, Ankunftszeit,

12. Gesamtzahl der mit der betreffenden Beförderung beförderten Personen,

13. Sitzplatznummer,

14. PNR-Buchungscode (Record Locator),

15. Anzahl, Gewicht und Identifizierung der Gepäckstücke,

16. Grenzübergangsstelle für die Einreise in das nationale Hoheitsgebiet.

…

KAPITEL 7 – PNR-Zentralstelle

Art. 12 – Innerhalb des Föderalen Öffentlichen Dienstes Inneres wird eine PNR-Zentralstelle geschaffen.

Art. 13 – § 1 – Die PNR-Zentralstelle ist verantwortlich für:

1. die Erhebung, Aufbewahrung und Verarbeitung der Passagierdaten, die von den Beförderungsunternehmen und Reiseunternehmen übermittelt werden, sowie die Verwaltung der Passagierdatenbank,

2. den Austausch sowohl der Passagierdaten als auch der Ergebnisse der Verarbeitung dieser Daten mit den PNR-Zentralstellen anderer Mitgliedstaaten der Europäischen Union, mit Europol und mit Drittstaaten gemäß Kapitel 12.

§ 2 – Unbeschadet anderer gesetzlicher Bestimmungen darf die PNR-Zentralstelle die aufgrund von Kapitel 9 aufbewahrten Daten nicht zu anderen als den in Artikel 8 erwähnten Zwecken benutzen.

Art. 14 – § 1 – Die PNR-Zentralstelle setzt sich zusammen aus:

1. einem … Beamten, … der verantwortlich ist für:

a) Organisation und Arbeitsweise der PNR-Zentralstelle,

b) Überprüfung der Einhaltung der in Kapitel 4 vorgesehenen Verpflichtungen durch die Beförderungsunternehmen und Reiseunternehmen,

c) Verwaltung und Betrieb der Passagierdatenbank,

d) Verarbeitung der Passagierdaten,

e) Einhaltung der Recht- und Ordnungsmäßigkeit der in Kapitel 10 erwähnten Verarbeitungen,

…

2. entsandten Mitgliedern, die aus folgenden … Diensten stammen:

a) den … Polizeidiensten,

b) der … Staatssicherheit,

c) dem … Allgemeinen Nachrichten- und Sicherheitsdienst,

d) der … Generalverwaltung Zoll und Akzisen.

…

KAPITEL 8 – Passagierdatenbank

Art. 15 – § 1 – Eine vom Föderalen Öffentlichen Dienst Inneres verwaltete Passagierdatenbank wird geschaffen, in der die Passagierdaten gespeichert werden.

…

§ 4 – Die aufgrund des vorliegenden Gesetzes vorgenommenen Verarbeitungen der Passagierdaten unterliegen dem Gesetz über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten. Die für die Kontrolle der Verarbeitung personenbezogener Daten zuständige Behörde übt die im Gesetz über den Schutz des Privatlebens vorgesehenen Befugnisse aus. …

…

KAPITEL 9 – Aufbewahrungsfristen

Art. 18 – Passagierdaten werden höchstens fünf Jahre ab ihrer Speicherung in der Passagierdatenbank aufbewahrt. Am Ende dieser Frist werden sie vernichtet.

…

KAPITEL 10 – Datenverarbeitung

Abschnitt 1 – Verarbeitung von Passagierdaten im Rahmen der Vorabüberprüfung der Passagiere

Art. 24 – § 1 – Die Passagierdaten werden im Hinblick auf die Durchführung einer Vorabüberprüfung der Passagiere vor ihrer Ankunft im nationalen Hoheitsgebiet, ihrer Abreise aus dem nationalen Hoheitsgebiet oder ihrer

Durchreise durch das nationale Hoheitsgebiet verarbeitet, um diejenigen Personen zu ermitteln, die genauer überprüft werden müssen.

[Methoden der Vorabüberprüfung]

Art. 25 – …

§ 2 – Die Überprüfung der Passagiere vor ihrer Ankunft, ihrer Durchreise oder ihrer Abreise anhand im Voraus festgelegter Kriterien erfolgt in nichtdiskrimierender Weise. Diese Kriterien dürfen nicht darauf abzielen, eine Person zu identifizieren, und müssen zielgerichtet, verhältnismäßig und bestimmt sein.

§ 3 – Die rassische oder ethnische Herkunft, die politischen Meinungen, die religiösen oder weltanschaulichen Überzeugungen, die Mitgliedschaft in einer Gewerkschaftsorganisation, der Gesundheitszustand, das Sexualleben oder die sexuelle Orientierung einer Person dürfen nicht als Grundlage für diese Kriterien dienen.

…

Abschnitt 2 – Datenverarbeitung im Rahmen gezielter Recherchen

Art. 27 – Die Passagierdaten werden benutzt, um gezielte Recherchen zu den in Artikel 8 § 1 Nr. 1, 2, 4 und 5 erwähnten Zwecken und unter den in Artikel 46*septies* des Strafprozessgesetzbuches, in Artikel 16/3 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste oder in Artikel 281 § 4 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen vorgesehenen Bedingungen durchzuführen.

KAPITEL 11 – Verarbeitung der Passagierdaten im Hinblick auf eine Verbesserung der Grenzkontrolle und die Bekämpfung der illegalen Einwanderung

Art. 28 – § 1 – Vorliegendes Kapitel findet Anwendung auf die Verarbeitung der Passagierdaten durch die Polizeidienste, die mit der Grenzkontrolle beauftragt sind, und durch das Ausländeramt im Hinblick auf eine Verbesserung der Personenkontrolle an den Außengrenzen und die Bekämpfung der illegalen Einwanderung.

…

Art. 29 – § 1 – …

§ 2 – Nur die [API-Daten] in Bezug auf folgende Kategorien von Passagieren werden übermittelt:

1. Passagiere, die beabsichtigen, über die Außengrenzen Belgiens ins Hoheitsgebiet zu kommen, oder bereits über die Außengrenzen Belgiens ins Hoheitsgebiet gekommen sind,

2. Passagiere, die beabsichtigen, das Hoheitsgebiet über die Außengrenzen Belgiens zu verlassen, oder die das Hoheitsgebiet bereits über die Außengrenzen Belgiens verlassen haben,

3. Passagiere, die beabsichtigen, sich in einer in Belgien gelegenen internationalen Transitzone aufzuhalten, sich dort aufhalten oder sich dort aufgehalten haben.

§ 3 – Die in § 2 erwähnten Passagierdaten werden den in Art. 14 § 1 Nr. 2 a) genannten Polizeidiensten unmittelbar nach ihrer Speicherung in der Passagierdatenbank übermittelt. Diese Polizeidienste bewahren diese Daten in einer temporären Datei auf und vernichten sie innerhalb von vierundzwanzig Stunden nach ihrer Übermittlung.

§ 4 – … die in § 2 erwähnten Passagierdaten … werden [dem Ausländeramt] unmittelbar nach ihrer Speicherung in der Passagierdatenbank übermittelt. Das Ausländeramt bewahrt diese Daten in einer temporären Datei auf und vernichtet sie innerhalb von vierundzwanzig Stunden nach ihrer Übermittlung.

…

Art. 31 – Binnen vierundzwanzig Stunden nach dem Ende der in Artikel 4 Nr. 3 bis 6 erwähnten Beförderung löschen die Beförderungsunternehmen und Reiseunternehmen alle in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten …

…

KAPITEL 15 – Abänderungsbestimmungen

Abschnitt 1 – Abänderung des Strafprozessgesetzbuches

Art. 50 – In das Strafprozessgesetzbuch wird ein Artikel 46*septies* mit folgendem Wortlaut eingefügt:

‚Art. 46*septies* – Bei der Ermittlung von Verbrechen und Vergehen, die in Artikel 8 § 1 Nr. 1, 2 und 5 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten erwähnt sind, kann der Prokurator des Königs durch einen mit Gründen versehenen schriftlichen Beschluss den Gerichtspolizeioffizier damit beauftragen, die PNR-Zentralstelle aufzufordern, die Passagierdaten gemäß Artikel 27 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten mitzuteilen.‘

…

Abschnitt 2 – Abänderung des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste

Art. 51 – In Kapitel III Abschnitt 1 Unterabschnitt 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste wird ein Artikel 16/3 mit folgendem Wortlaut eingefügt:

‚Art. 16/3 – § 1 – Die Nachrichten- und Sicherheitsdienste können im Interesse der Ausübung ihrer Aufträge und ordnungsgemäß begründet beschließen, auf die in Artikel 27 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten erwähnten Passagierdaten zuzugreifen …‘“

III. Würdigung durch den Verfassungsgerichtshof

43 Der Verfassungsgerichtshof präzisiert zunächst, dass sie die Klage unter Berücksichtigung der Änderungen des Gesetzes vom 25. Dezember 2016 durch die Gesetze vom 15. und 30. Juli 2018 und das Gesetz vom 2. Mai 2019 prüft.

44 Außerdem grenzt der Verfassungsgerichtshof den Umfang der Nichtigkeitsklage ein, indem er feststellt, dass sich der erste Klagegrund allein gegen Art. 3 § 2, Art. 4 Nr. 9 und 10, Art. 7 bis 9, Art. 12 bis 16, Art. 18, Art. 24 bis 27 und Art. 50 und 51 des Gesetzes und der zweite Klagegrund allein gegen Art. 3 § 1, Art. 8 § 2 und Art. 28 bis 31 des Gesetzes richtet.

1. Zulässigkeit des ersten Klagegrundes: Ist Art. 23 der DSGVO auf das PNR-Gesetz anwendbar?

45 Das vorlegende Gericht weist darauf hin, dass der Schutz, den die DSGVO bietet, auf Art. 16 Abs. 2 AEUV beruht und dass die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung nicht unter die DSGVO, sondern unter die Richtlinie 2016/680 fällt. Diese Richtlinie legt spezifische Regeln 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 fest, wobei den Besonderheiten dieser Tätigkeiten Rechnung getragen wird.

46 Das PNR-Gesetz regelt die Erhebung und Übermittlung der PNR-Daten, die Schaffung einer von der PNR-Zentralstelle verwalteten Passagierdatenbank, die Zwecke der Verarbeitung der darin enthaltenen Daten und den Zugang zu dieser Datenbank. Es setzt im Wesentlichen die PNR-Richtlinie um, geht inhaltlich aber über die Umsetzung dieser Richtlinie hinaus.

47 Unter Bezugnahme auf das Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017 (EU:C:2017:592) stellt das vorlegende Gericht fest, dass die Vorschriften über die Erhebung, Übermittlung und Verarbeitung von „PNR-Daten“ sowohl unter den Datenschutz (Art. 16 AEUV) als auch unter die polizeiliche Zusammenarbeit (Art. 87 AEUV) fallen können.

Es weist ferner darauf hin, dass der fünfte Erwägungsgrund der PNR-Richtlinie besagt, dass die Ziele dieser Richtlinie „*unter anderem darin [bestehen], für Sicherheit zu sorgen, das Leben und die Sicherheit von Personen zu schützen und einen Rechtsrahmen für den Schutz von PNR-Daten in Bezug auf deren Verarbeitung durch die zuständigen Behörden zu schaffen*“. Der 38. Erwägungsgrund derselben Richtlinie führt jedoch als deren Ziele „*die Übermittlung von PNR-Daten durch Fluggesellschaften und deren Verarbeitung zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität*“ an, was diesen Zielen größeres Gewicht verleihen könnte als dem Ziel des Datenschutzes.

Das vorlegende Gericht stellt ferner fest, dass das nationale Recht nicht das gesamte PNR-Gesetz vom Anwendungsbereich des Art. 23 der DSGVO ausnimmt.

48 Der Verfassungsgerichtshof kommt daher zu dem Schluss, dass dem Gerichtshof eine erste Frage zur Vorabentscheidung vorzulegen ist, um festzustellen, ob die Anforderungen des Art. 23 der DSGVO auf das PNR-Gesetz anzuwenden sind, das u. a. und hauptsächlich die PNR-Richtlinie umsetzt.

2. Zur Begründetheit des ersten Klagegrundes

Im Anschluss daran prüft der Verfassungsgerichtshof die Begründetheit des Klagegrundes im Hinblick auf die sieben in Rn. 8 der vorliegenden Zusammenfassung erwähnten Einzelpunkte. Er befindet, dass die ersten beiden gegen die „Durchführungsmodalitäten“ und die Begriffe „Identitätsdokumente“ und „Reisedokumente“ erhobenen Rügen unbegründet sind. Er fährt mit der Prüfung der fünf weiteren Rügen fort und äußert Zweifel im Zusammenhang mit der Auslegung bestimmter Vorschriften der PNR-Richtlinie und ihrer Vereinbarkeit mit der Charta.

Zu den im PNR-Gesetz (Art. 4 Nr. 9 und Art. 9) genannten Daten

49 Nach Auffassung der Klägerin steht der sehr weite Anwendungsbereich hinsichtlich der in Art. 4 Nr. 9 und Art. 9 des PNR-Gesetzes genannten Passagierdaten offensichtlich außer Verhältnis zu dem verfolgten Zweck. Nach ihrer Ansicht könnten die betreffenden Daten sensible Daten wie die Mitgliedschaft in einer Gewerkschaftsorganisation, persönliche Affinitäten und persönliche oder berufliche Beziehungen preisgeben.

50 Das vorlegende Gericht weist darauf hin, dass ein Eingriff öffentlicher Stellen in die Ausübung des Rechts auf Achtung der Privatsphäre nicht nur auf einer hinreichend präzisen Rechtsvorschrift beruhen, sondern auch einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entsprechen und in einem angemessenen Verhältnis zu dem verfolgten berechtigten Zweck stehen muss. Der Gesetzgeber verfügt in diesem Bereich über einen Ermessensspielraum, der jedoch nicht unbegrenzt ist: Damit eine Norm mit dem

Recht auf Achtung der Privatsphäre vereinbar ist, muss der Gesetzgeber einen angemessenen Ausgleich zwischen allen betroffenen Rechten und Interessen hergestellt haben.

In seinem Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017 (EU:C:2017:592) hat der Gerichtshof darauf hingewiesen, dass ein Eingriff in das Recht auf Schutz personenbezogener Daten auf das „absolut Notwendige“ beschränkt sein muss (vgl. Rn. 140 und 141).

51 Der Verfassungsgerichtshof weist darauf hin, dass das PNR-Gesetz den Zweck verfolgt, die öffentliche Sicherheit zu gewährleisten, indem es eine Übermittlung und Verwendung von Passagierdaten im Rahmen der Bekämpfung terroristischer Straftaten und der grenzüberschreitenden schweren Kriminalität vorsieht. Diese Zwecke stellen eine dem Gemeinwohl dienende Zielsetzung dar, die Eingriffe in das Recht auf Achtung der Privatsphäre und in das Recht auf Schutz personenbezogener Daten rechtfertigen kann (Urteil vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 42). Der Gerichtshof hat ferner bestätigt, dass diese dem Gemeinwohl dienenden Ziele die Übermittlung und Verarbeitung von Passagierdatensätzen rechtfertigen konnten (Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 148 und 149).

52 Anschließend prüft das vorlegende Gericht unter Berücksichtigung des Umfangs der im PNR-Gesetz genannten Daten, ob diese Eingriffe hinreichend präzise, verhältnismäßig und auf das „absolut Notwendige“ beschränkt sind.

Die Erfassung der im PNR-Gesetz aufgeführten Passagierdaten ist mit Garantien hinsichtlich des Inhalts dieser Daten versehen. Diese Daten sind in der Tat in Art. 9 des PNR-Gesetzes abschließend bestimmt. Es handelt sich um Informationen, die in unmittelbarem Zusammenhang mit der Reise stehen, die zu der in den Anwendungsbereich des PNR-Gesetzes fallenden Beförderung führt, und die den Beförderungs- und Reiseunternehmen grundsätzlich bereits vorliegen. Außerdem entsprechen diese Daten dem Anhang I der Richtlinien der Internationalen Zivilluftfahrt-Organisation (ICAO). Sie sind daher für die vom PNR-Gesetz verfolgten Zwecke relevant.

Außerdem sehen die nicht angefochtenen Artikel 10 und 11 des PNR-Gesetzes vor, dass die Passagierdaten nicht die rassische oder ethnische Herkunft einer Person, ihre religiösen oder weltanschaulichen Überzeugungen, ihre politischen Meinungen, ihre Mitgliedschaft in einer Gewerkschaftsorganisation, ihren Gesundheitszustand, ihr Sexualleben oder ihre sexuelle Orientierung betreffen dürfen. Wenn die von den Beförderungs- und Reiseunternehmen übermittelten Passagierdaten andere als die in Art. 9 aufgeführten Daten oder in Art. 10 aufgeführte Daten beinhalten, werden diese zusätzlichen Daten von der PNR-Zentralstelle unmittelbar nach ihrem Eingang dauerhaft gelöscht. Diese Bestimmungen gewährleisten, dass sensible Daten grundsätzlich nicht als „Passagierdaten“ erfasst oder aufbewahrt werden können.

53 In seinem vorgenannten Gutachten 1/15 vom 26. Juli 2017 hat der Gerichtshof in Bezug auf sensible Daten ferner ausgeführt, dass „Art. 7, *Art. 8, Art. 21 und Art. 52 Abs. 1 der Charta sowohl der Übermittlung sensibler Daten an Kanada als auch der von der Union mit diesem Drittstaat ausgehandelten Regelung der Bedingungen für die Verwendung und Speicherung solcher Daten durch die Behörden dieses Drittstaats entgegenstehen*“ (Rn. 167).

Diese Feststellung lässt sich auf den vorliegenden Fall übertragen. Auch wenn die im PNR-Gesetz vorgesehen Passagierdaten mit Garantien versehen sind, ist gleichwohl zu fragen, ob diese Garantien angesichts des Umfangs der genannten Daten ausreichen. Die in Art. 9 § 1 des PNR-Gesetzes bezeichneten Daten, die den im Anhang I der PNR-Richtlinie bezeichneten Daten entsprechen, umfassen nämlich sehr umfangreiche, über die Daten des Eincheckstatus und des Anbordgehens hinausgehende Angaben, insbesondere: den gesamten Reiseverlauf für den Passagier, das Reisebüro, die Sitzplatznummer, vollständige Gepäckangaben, die Zahlungsinformationen einschließlich der Rechnungsanschrift und allgemeine Hinweise „einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren“.

In seinem vorgenannten Gutachten 1/15 vom 26. Juli 2017 hat der Gerichtshof ferner ausgeführt, dass „*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 [können]*“ (Rn. 128).

In seiner Stellungnahme vom 19. August 2016 zu den datenschutzrechtlichen Auswirkungen der Verarbeitung von Fluggastdatensätzen (im Folgenden: Stellungnahme vom 19. August 2016) hat der Beratende Ausschuss für das Übereinkommen Nr. 108 des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (im Folgenden: Beratender Ausschuss für das Übereinkommen Nr. 108) ebenfalls festgestellt, dass „*[d]ie PNR … Informationen [enthalten], die zur Erleichterung der Reise eines Passagiers dienen und eine Reihe von sensiblen Daten (Angaben, die als Hinweis auf die rassische Herkunft, die politischen Meinungen, die religiösen oder sonstigen Überzeugungen, den Gesundheitszustand oder die sexuelle Orientierung eines Menschen dienen können) enthalten können, und zwar nicht nur in bestimmten ‚kodierten‘ Daten, sondern auch in der freien Rubrik mit allgemeinen Hinweisen (wie Ernährungsbedürfnisse und medizinische Bedürfnisse oder der Umstand, dass eine politische oder religiöse Vereinigung ermäßigte Tarife für die Reise ihrer Mitglieder in Anspruch genommen hat), was zu einer unmittelbaren Diskriminierung führen könnte*“ (Europarat, Stellungnahme vom 19. August 2016, T-PD(2016)18 rev, S. 7).

Die Agentur der Europäischen Union für Grundrechte hat ebenfalls darauf hingewiesen, dass PNR-Daten „*[s]ensible oder besondere Daten … in dem Posten ‚allgemeine Hinweise' enthalten [können]*" (Gutachten 1/2011 der Agentur der Europäischen Union für Grundrechte betreffend den Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (KOM(2011) 32 endgültig), 14. Juni 2011, S. 8; vgl. auch ebd., S. 14 f.).

54 Angesichts ihres sehr weiten Anwendungsbereichs könnten die in Art. 9 des PNR-Gesetzes genannten Daten auch dann, wenn sie nicht direkt sensible Daten enthalten, indirekt sensible Angaben offenbaren, die unter den Schutz personenbezogener Daten und unter die Wahrung der Privatsphäre fallen. In Anbetracht des Gutachtens 1/15 des Gerichtshofs fragt sich der Verfassungsgerichtshof, ob diese Daten, die die in Anhang I der PNR-Richtlinie aufgeführten Daten umfassen, nicht über das hinausgehen, was zur Erreichung der Zwecke dieser Richtlinie „absolut notwendig" ist. Er beschließt daher, dem Gerichtshof eine zweite Frage zur Vorabentscheidung vorzulegen.

55 In seinem vorgenannten Gutachten 1/15 vom 26. Juli 2017 hat der Gerichtshof außerdem zum Erfordernis einer klaren und präzisen Definition der im Entwurf eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen genannten Daten Folgendes ausgeführt:

„*156 | Die 19 Rubriken von PNR-Daten im Anhang des geplanten Abkommens entsprechen zwar nach der Stellungnahme der Kommission dem Anhang I der Leitlinien der International Civil Aviation Organization (ICAO) über PNR-Daten. Wie der Generalanwalt in Nr. 217 seiner Schlussanträge ausgeführt hat, werden die zu übermittelnden PNR-Daten in den Rubriken 5 (‚Verfügbare Vielflieger- und Bonus-Daten [Gratisflugscheine, Upgrades usw.]') und 7 (‚Sämtliche verfügbaren Kontaktangaben, einschließlich Informationen zur Identifizierung des Dateneingebers') aber nicht hinreichend klar und präzise definiert.*

157 | Bei Rubrik 5 ist der Umfang der zu übermittelnden Daten wegen der Verwendung des Ausdrucks ‚usw.' nicht hinreichend bestimmt. Außerdem ist aus dem Wortlaut dieser Rubrik nicht ersichtlich, ob mit ihr Informationen allein über die Teilnahme der Fluggäste an Bonusprogrammen gemeint sind oder sämtliche Informationen über die Flüge und Buchungen, die im Rahmen solcher Programme durchgeführt werden.

158 | Der Umfang der zu übermittelnden Daten ist auch in Rubrik 7 nicht hinreichend bestimmt, in der der Ausdruck ‚[s]ämtliche verfügbaren Kontaktangaben' verwendet wird. Insbesondere wird nicht präzisiert, welche Art von Kontaktangaben gemeint sind und ob diese auch, wie sich aus der schriftlichen Antwort der Kommission auf die Fragen des Gerichtshofs ableiten lässt, Informationen über Dritte umfassen, die die Buchung des Fluges für den

Fluggast vorgenommen haben, über die ein Fluggast erreicht werden kann oder die im Notfall zu verständigen sind.

159 | Rubrik 8 betrifft ‚[s]ämtliche verfügbaren Zahlungs-/Abrechnungsinformationen (ohne weitere Transaktionsdetails für eine Kreditkarte oder ein Konto, die nicht mit der die Reise betreffenden Transaktion verknüpft sind)'. Sie könnte zwar wegen der Verwendung des Ausdrucks ‚[s]ämtliche verfügbaren ... [I]nformationen' besonders weit erscheinen. Wie sich aus der Antwort der Kommission auf die Fragen des Gerichtshofs ergibt, ist aber davon auszugehen, dass sie lediglich Informationen über die Modalitäten der Zahlung und die Abrechnung des Flugtickets betrifft, nicht aber andere Informationen, die keinen direkten Bezug zum Flug aufweisen. Bei dieser Auslegung genügt die Rubrik den Anforderungen an Klarheit und Präzision.

160 | Rubrik 17 betrifft ‚[a]llgemeine Eintragungen einschließlich OSI- (Other Supplementary Information), SSI- (Special Service Information) und SSR-Informationen (Special Service Request)'. Nach den Erläuterungen, die insbesondere die Kommission gegeben hat, handelt es sich bei dieser Rubrik um eine sogenannte ‚free text'-Rubrik, mit der über die im Anhang des geplanten Abkommens angeführten Informationen hinaus ‚weitere Informationen' einbezogen werden sollen. Eine solche Rubrik enthält keine Angaben über Art und Umfang der zu übermittelnden Informationen und könnte selbst Informationen umfassen, die keinerlei Bezug zum Zweck der Übermittlung der PNR-Daten haben. Da die in dieser Rubrik genannten Informationen lediglich beispielhaft genannt werden, wie aus der Verwendung des Wortes ‚einschließlich' hervorgeht, begrenzt sie Art und Umfang der Informationen, die von ihr erfasst werden können, nicht. Rubrik 17 ist mithin nicht hinreichend klar und präzise abgegrenzt.

161 | Schließlich betrifft Rubrik 18 ‚[e]twaige für Buchungszwecke erhobene Daten zur Advance Passenger Information (API)'. Nach den Erläuterungen, die der Rat und die Kommission gegeben haben, entsprechen diese Informationen den Angaben gemäß Art. 3 Abs. 2 der Richtlinie 2004/82, d. h. Nummer und Art des mitgeführten Reisedokuments, Staatsangehörigkeit, vollständiger Name, Geburtsdatum, Grenzübergangsstelle für die Einreise in das Hoheitsgebiet der Mitgliedstaaten, Beförderungs-Codenummer, Abreise- und Ankunftszeit, Gesamtzahl der beförderten Personen und ursprünglicher Abreiseort. Soweit die Rubrik dahin ausgelegt wird, dass sie sich lediglich auf die ausdrücklich in Art. 3 Abs. 2 der Richtlinie 2004/82 genannten Angaben erstreckt, kann davon ausgegangen werden, dass sie die Anforderungen an Klarheit und Präzision erfüllt.

162 | Die Vorschriften von Art. 4 Abs. 3 des geplanten Abkommens, die die Verpflichtung Kanadas vorsehen, alle von den Fluggesellschaften übermittelten PNR-Daten, die nicht in der Liste im Anhang des Abkommens aufgeführt sind, zu löschen, kann die mangelnde Bestimmtheit der Rubriken 5, 7 und 17 des Anhangs nicht ausgleichen. Da die Liste als solche die zu übermittelnden PNR-Daten nicht hinreichend klar und präzise bestimmt, sind diese Bestimmungen nämlich nicht

geeignet, die Unsicherheiten hinsichtlich der zu übermittelnden PNR-Daten zu beseitigen.

163 | Somit ist hinsichtlich der an Kanada zu übermittelnden PNR-Daten festzustellen, dass die Rubriken 5, 7 und 17 des Anhangs des geplanten Abkommens den Umfang des Eingriffs in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte nicht hinreichend klar und präzise regeln.“

56 Da sich einige dieser Ausführungen wegen des exemplarischen und nicht abschließenden Charakters bestimmter Daten, die in Anhang I der insoweit durch Art. 9 des PNR-Gesetzes umgesetzten PNR-Richtlinie aufgeführt sind, auf den vorliegenden Fall übertragen lassen könnten, beschließt das vorlegende Gericht, eine dritte Frage zur Vorabentscheidung vorzulegen.

Zum Begriff „Passagier“ (Art. 4 Nr. 10° des PNR-Gesetzes)

57 Die Klägerin beanstandet die Weite des Begriffs „Passagier“, die zu einer systematischen und nicht zielgerichteten automatisierten Verarbeitung der Daten aller Reisenden führe.

58 Die Definition des Begriffs „Passagier“ (Art. 4 Nr. 10 des PNR-Gesetzes) habe zur Folge, dass die Erfassung, Übermittlung und Verarbeitung der PNR-Daten der „Passagiere“ Gegenstand allgemeiner und undifferenzierter Verpflichtungen sei, die für jede beförderte oder zu befördernde und in der Passagierliste eingetragene Person gälten. Die Verpflichtungen, die das PNR-Gesetz auferlege, gälten somit unabhängig davon, ob ein begründeter Verdacht vorliege, dass die betroffenen Personen eine Straftat begangen hätten oder in naher Zukunft begehen würden oder verurteilte Straftäter seien.

59 In seiner Stellungnahme vom 19. August 2016 hat der Beratende Ausschuss für das Übereinkommen Nr. 108 hierzu ausgeführt: „*Die Verarbeitung von PNR-Daten – die den einzigartigen Vorteil bietet, Personen von Interesse identifizieren zu können –, stellt eine allgemeine und unterschiedslose Überprüfung sämtlicher Passagiere einschließlich derjenigen, die nicht verdächtigt werden, irgendeine Straftat begangen zu haben, durch verschiedene zuständige Behörden dar und betrifft Daten, die ursprünglich von privaten Unternehmen zu kommerziellen Zwecken erfasst wurden. Angesichts des Ausmaßes des Eingriffs in die Rechte auf Privatsphäre und Datenschutz, zu dem die Verarbeitung der PNR-Daten führen würde, muss eindeutig nachgewiesen werden, dass diese Verarbeitung eine in einer demokratischen Gesellschaft notwendige und einem legitimen Zweck dienende Maßnahme ist; außerdem müssen angemessene Garantien geschaffen werden. Es ist unerlässlich, die Notwendigkeit der Erfassung und späteren Auswertung der PNR-Daten ausdrücklich nachzuweisen*“ (Stellungnahme vom 19. August 2016, T-PD(2016)18 rev, S. 5).

60 Im Bereich der elektronischen Kommunikation hat sich der Gerichtshof zu einer nationalen Regelung geäußert, die eine allgemeine und unterschiedslose

Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsah und die Betreiber elektronischer Kommunikationsdienste verpflichtete, diese Daten systematisch und kontinuierlich auf Vorrat zu speichern, und zwar ausnahmslos (Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970).

Er war der Auffassung, dass „*die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, [zwar] in hohem Maß von der Nutzung moderner Ermittlungstechniken abhäng[e], eine solche dem Gemeinwohl dienende Zielsetzung … jedoch, so grundlegend sie auch sein [möge], für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vors[ehe], für die Kriminalitätsbekämpfung nicht rechtfertigen [könne]*“ (Rn. 103).

Der Gerichtshof hat entschieden, dass zum einen eine solche Regelung zur Folge hat, dass die Vorratsspeicherung der Verkehrs- und Standortdaten die Regel ist, obwohl nach dem mit der Richtlinie 2002/58 geschaffenen System die Vorratsspeicherung von Daten die Ausnahme zu sein hat, und dass zum anderen „*eine nationale Regelung …, die sich allgemein auf alle Teilnehmer und registrierten Nutzer erstreckt und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erfasst, keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vor[sieht]. Sie betrifft pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keine Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 57 und 58).*

106 | Eine solche Regelung verlangt keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit. Insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 59).

107 | Eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es

Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta verlangt.

108 | Hingegen untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einem Mitgliedstaat nicht, eine Regelung zu erlassen, 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.

109 | Um den in der vorstehenden Randnummer des vorliegenden Urteils genannten Erfordernissen zu genügen, muss die betreffende nationale Regelung erstens klare und präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken 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 (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 54 und die dort angeführte Rechtsprechung).

110 | Zweitens können sich die materiellen Voraussetzungen, die eine nationale Regelung, die im Rahmen der Bekämpfung von Straftaten vorbeugend die Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterscheiden, doch muss die Vorratsspeicherung der Daten 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.

111 | Bei der Begrenzung einer solchen Maßnahme im Hinblick auf die potenziell betroffenen Personenkreise und Situationen 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. Eine solche Begrenzung lässt sich durch ein geografisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem

oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden.

112 | In Anbetracht all dessen ist auf die erste Frage in der Rechtssache C-203/15 zu antworten, 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 dahin auszulegen ist, dass er einer nationalen Regelung 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.“

Auf die zweite Frage zur Vorabentscheidung in der Rechtssache C-203/15 und auf die erste Frage zur Vorabentscheidung in der Rechtssache C-698/15 antwortet der Gerichtshof, 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 „*dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind*“ (Rn. 125).

61 Der EGMR hat inzwischen in seinem Urteil *Centrum för Rättvisa/Schweden vom 19. Juni 2018* seinerseits entschieden, dass die schwedischen Rechtsvorschriften über die massenhafte Überwachung der elektronischen Kommunikation im Einklang mit Art. 8 der Europäischen Menschenrechtskonvention stehen. Er hat insbesondere Folgendes ausgeführt:

„*Der [EGMR] hat ausdrücklich den weiten Ermessensspielraum anerkannt, über den die nationalen Behörden bei Wahl der Mittel zum Schutz der nationalen Sicherheit verfügen. In den Rechtssachen Weber und Saravia sowie Liberty u. a. hat der [EGMR] anerkannt, dass Systeme zur Massenüberwachung nicht schon als solche außerhalb dieses Spielraums liegen. Angesichts der Begründung dieser Urteile und der derzeitigen Bedrohungen, mit denen viele Konventionsstaaten konfrontiert sind (einschließlich der Geißel des internationalen Terrorismus und anderer schwerer Straftaten wie Drogenhandel, Menschenhandel, sexuelle Ausbeutung von Kindern und Computerkriminalität), der technologischen Fortschritte, die es Terroristen und Kriminellen erleichtern, ihrer Entdeckung im Internet zu entgehen, und der Unvorhersehbarkeit der Übermittlungswege elektronischer Kommunikation ist der [EGMR] der Auffassung, dass die Entscheidung, zur Entdeckung bislang unbekannter Bedrohungen der nationalen Sicherheit auf ein System massenhafter Überwachung zurückzugreifen, in den Ermessensspielraum der Staaten fällt.*“ (EGMR, 19 Juni 2018, *Centrum för Rättvisa/Schweden* , § 112).

Hingegen hat derselbe Gerichtshof entschieden, dass das englische Gesetz über die Überwachung der Kommunikation gegen Art. 8 EMRK verstieß, weil es die in seiner Rechtsprechung aufgestellten Kriterien nicht erfüllte. Er war ferner der Auffassung, dass „*das Funktionieren der Systeme zur massenhaften Überwachung grundsätzlich in den Ermessensspielraum des Staates fällt. Die massenhafte Überwachung ist definitionsgemäß nicht zielgerichtet, und sie vom Vorliegen eines ‚begründeten Verdachts' abhängig zu machen würde ihre Durchführung unmöglich machen*“ (EMRK, 13. September 2018, *Big Brother Watch u. a./Vereinigtes Königreich*, § 317).

62 Die Frage ist, inwieweit die vorerwähnte Rechtsprechung, die die allgemeine und unterschiedslose Vorratsspeicherung von Daten im Bereich der elektronischen Kommunikation betrifft, auf die allgemeine und unterschiedslose Erfassung, Übermittlung und Verarbeitung von Passagierdaten, wie sie im Gesetz vom 25. Dezember 2016 geregelt sind, übertragen werden kann.

63 In seinem vorgenannten Gutachten 1/15 vom 26. Juli 2017 hat sich der Gerichtshof zu einem vergleichbaren PNR-System mit allerdings begrenzterem Anwendungsbereich geäußert, da der Entwurf eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen „*die systematische und kontinuierliche Übermittlung der PNR-Daten sämtlicher Fluggäste …, die aus der Union nach Kanada reisen*“, vorsah (Rn. 127). Er ist davon ausgegangen, dass „*die Übermittlung der PNR-Daten an Kanada und ihre anschließende Verarbeitung geeignet sind, die Verwirklichung des mit dem geplanten Abkommen verfolgten Ziels des Schutzes der öffentlichen Sicherheit zu gewährleisten*“ (Rn. 153).

Im Hinblick auf die betroffenen Fluggäste hat der Gerichtshof folgende Auffassung vertreten:

|„186 | Das geplante Abkommen gilt für die PNR-Daten sämtlicher Fluggäste, die aus der Union nach Kanada reisen. Die Daten werden an Kanada unabhängig davon übermittelt, ob objektive Anhaltspunkte dafür vorliegen, dass von den Fluggästen eine Gefahr für die öffentliche Sicherheit in Kanada ausgeht.

187 | Die PNR-Daten sind vor allem dazu bestimmt, automatisiert verarbeitet zu werden (siehe oben, Rn. 152 und 169). Wie mehrere Beteiligte geltend gemacht haben, soll mit der automatisierten Verarbeitung ermittelt werden, ob möglicherweise eine Gefahr für die öffentliche Sicherheit von Personen ausgeht, die den zuständigen Stellen zu diesem Zeitpunkt nicht bekannt sind und die wegen dieser Gefahr einer eingehenden Überprüfung unterzogen werden könnten. Die automatisierte Verarbeitung der PNR-Daten vor der Ankunft der Fluggäste in Kanada erleichtert und beschleunigt dabei die Sicherheitskontrollen, insbesondere an den Grenzen. Der Ausschluss bestimmter Kategorien von Personen oder bestimmter Herkunftsländer könnte dem Ziel der automatisierten Verarbeitung der PNR-Daten zuwiderlaufen, das darin besteht, unter sämtlichen Fluggästen mittels einer Überprüfung dieser Daten die Personen zu ermitteln, von

denen eine Gefahr für die öffentliche Sicherheit ausgehen kann. Außerdem könnte diese Überprüfung umgangen werden.

188 | Im Übrigen haben alle Fluggäste nach Art. 13 des Abkommens von Chicago, auf den insbesondere der Rat und die Kommission in ihren Antworten auf die Fragen des Gerichtshofs Bezug genommen haben, beim Ein- und Ausflug sowie während des Aufenthalts im Hoheitsgebiet eines Vertragsstaats die Gesetze und Vorschriften dieses Staates über den Ein- und Ausflug von Fluggästen zu befolgen. Sämtliche Fluggäste, die nach Kanada einreisen oder aus Kanada ausreisen möchten, unterliegen nach diesem Artikel daher den Grenzkontrollen und sind verpflichtet, die Voraussetzungen des geltenden kanadischen Rechts für die Ein- oder Ausreise zu erfüllen. Zudem gehört die Identifizierung von Fluggästen, von denen ein Risiko für die öffentliche Sicherheit ausgehen kann, anhand der PNR-Daten zur Grenzkontrolle (siehe oben, Rn. 152 und 187). Sofern Fluggäste, die nach Kanada einreisen und sich dort aufhalten möchten, Gegenstand dieser Kontrollen sind, unterliegen sie deshalb schon wegen der Art dieser Maßnahme der Überprüfung ihrer PNR-Daten.

189 | Unter diesen Umständen geht das geplante Abkommen dadurch, dass es die Übermittlung der PNR-Daten sämtlicher Fluggäste an Kanada ermöglicht, nicht über das hinaus, was absolut notwendig ist.“

64 Der Verfassungsgerichtshof fragt sich, ob diese Erwägungen auf die PNR-Richtlinie und auf nationale Rechtsvorschriften wie das PNR-Gesetz übertragen werden könnten, das zur Umsetzung der PNR-Richtlinie die allgemeine und unterschiedslose Erfassung, Übermittlung und Verarbeitung der „PNR-Daten“ sämtlicher Passagiere vorschreibt, die mit einem Flugzeug, Zug oder Bus reisen, unabhängig davon, ob die Außengrenzen der Union überschritten werden oder nicht. Dieses System findet nämlich auch auf Personen Anwendung, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte, und geht über das im PNR-Abkommen EU-Kanada vorgesehene System hinaus. Angesichts des Umfangs der genannten Daten stellt sich die Frage, ob diese Maßnahme die Grenzen des „absolut Notwendigen“ einhält. Bevor das vorlegende Gericht in der Sache entscheidet, beschließt es daher, eine vierte Frage zur Vorabentscheidung vorzulegen.

Zu den Zwecken der Verarbeitung der „PNR-Daten“ (Art. 8 des PNR-Gesetzes)

65 Die Klägerin beanstandet die Definition der Zwecke der Verarbeitung der „PNR-Daten“ in Art. 8 des PNR-Gesetzes, die wesentlich weiter gefasst sei als die der „bestimmten Zwecke“, die ihrerseits allein auf terroristische Straftaten und schwere Kriminalität im Sinne der PNR-Richtlinie beschränkt seien. Sie ist der Ansicht, dass diese Zwecke die Grenzen des „absolut Notwendigen“ überschreiten.

Bei den Zwecken der Verarbeitung der „PNR-Daten“, wie sie in Art. 1 Abs. 2 und 6 Abs. 2 der PNR-Richtlinie festgelegt sind, handelt es sich ausschließlich um Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (vgl. auch siebter Erwägungsgrund der PNR-Richtlinie).

Einige der in Art. 8 des PNR-Gesetzes genannten Verarbeitungszwecke entsprechen den in Anhang II der PNR-Richtlinie aufgeführten strafbaren Handlungen, im Einklang mit den in dieser Richtlinie genannten Zwecken der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Hingegen kommen weitere Zwecke der Verarbeitung von „PNR-Daten“ zu den in dieser Richtlinie vorgesehenen Zwecken hinzu. Dies gilt u. a. für die „Beaufsichtigung der in den Artikeln 7 Nr. 1 und 3/1 und 11 § 1 Nr. 1 bis 3 und 5 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Aktivitäten“ (Art. 8 § 1 Nr. 4).

Das vorlegende Gericht prüft, ob diese weiteren Zwecke in klaren, präzisen und auf das absolut Notwendige beschränkten Regelungen zum Ausdruck kommen, und äußert Zweifel hinsichtlich des in Art. 8 § 1 Nr. 4 des PNR-Gesetzes genannten Zwecks.

In der Begründung des PNR-Gesetzes wird ausgeführt, dieser „Zweck [betreffe] die Zuständigkeiten der Nachrichtendienste, d. h. der Staatssicherheit und des Allgemeinen Nachrichten- und Sicherheitsdienstes (SGRS). Zur Durchführung ihrer Aufgaben der Ermittlung, Analyse und Auswertung von Informationen über Tätigkeiten, die die grundlegenden Interessen des Staates gefährden können, müssen diese Dienste in der Lage sein, die Passagierdaten auszuwerten, um konkrete Gefahren so früh wie möglich zu erkennen, die Bewegungen bestimmter Personen zu verfolgen oder Analysen allgemeinerer Phänomene oder Tendenzen zu erstellen. Die Aufgaben der Ermittlung, Analyse und Auswertung von Informationen über Tätigkeiten ausländischer Nachrichtendienste auf belgischem Hoheitsgebiet fallen unter diesen Zweck.“ (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, S. 19-20).

Auch wenn die Aufgaben der Nachrichten- und Sicherheitsdienste im Allgemeinen zur nationalen und internationalen Sicherheit beitragen, erscheint die Verarbeitung der „PNR-Daten“ im Hinblick auf den in Art. 8 § 1 Nr. 4 des PNR-Gesetzes genannten Zweck recht vage und allgemein.

Soweit es um die Vorabüberprüfung der Passagiere geht, dient dieselbe Verarbeitung außer diesem Zweck auch den in Art. 8 § 1 Nr. 1, 2 und 5 des PNR-Gesetzes aufgeführten Zwecken (Art. 24 § 2 und 26 § 2).

In diesem Zusammenhang beschließt der Verfassungsgerichtshof, dem Gerichtshof eine fünfte Frage zur Vorabentscheidung vorzulegen, um zu entscheiden, ob dieser Zweck hinreichend klar, präzise und auf das absolut Notwendige beschränkt ist.

Zur Verwaltung der Passagierdatenbank und zur Verarbeitung der Daten im Rahmen der Vorabüberprüfung der Passagiere und gezielter Recherchen (Art. 16, 24 bis 27, 50 und 51 des PNR-Gesetzes)

66 Die Klägerin ist der Auffassung, dass die verschiedenen Arten der Verarbeitung und des Austauschs personenbezogener Daten offensichtlich unverhältnismäßig sind.

67 Art. 16 des PNR-Gesetzes sieht vor, dass die Passagierdaten im Rahmen der in Art. 8 § 1 erwähnten Zwecke Gegenstand der in Art. 24 bis 27 erwähnten Verarbeitungen sind.

– *Die Vorabüberprüfung der Passagiere (Art. 24 bis 26)*

68 Die Passagierdaten werden im Hinblick auf die Durchführung einer Vorabüberprüfung (*pre-screening*) der Passagiere vor ihrer Ankunft im nationalen Hoheitsgebiet, ihrer Abreise aus dem nationalen Hoheitsgebiet oder ihrer Durchreise durch das nationale Hoheitsgebiet verarbeitet, um diejenigen Personen zu ermitteln, die genauer überprüft werden müssen. „Es geht darum, die potenzielle Bedrohung zu bewerten und zu ermitteln, welche Passagiere für die Wahrnehmung ihrer Aufgaben von Interesse sind oder es z. B. erforderlich machen, eine Maßnahme gegen sie zu ergreifen (Vollstreckung eines Haftbefehls, Durchsuchung usw.)“ (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, S. 28).

Die Vorabüberprüfung beruht auf zwei Ansätzen: zum einen der Korrelation der Passagierdaten mit den Datenbanken und zum anderen der Korrelation der Daten mit im Voraus festgelegten Kriterien.

69 Bezüglich der Korrelation mit den Datenbanken wird in den Vorarbeiten zum PNR-Gesetz ausgeführt, dass „[d]er erste Ansatz … darin [besteht], mit Hilfe der Korrelation der Passagierdaten mit den Daten, die in den von den zuständigen Dienststellen verwalteten Datenbanken verarbeitet werden, nach positiven Übereinstimmungen zu suchen. So kann beispielsweise beurteilt werden, ob eine Person ein erhöhtes Gefährlichkeitspotenzial aufweist, weil sie in einer Polizeidatenbank im Rahmen eines terrorbezogenen Aktenvorgangs verzeichnet ist und aus einer Analyse ihrer Passagierdaten hervorgeht, dass diese Person sich regelmäßig in Länder, in denen sich Trainingslager für Terroristen befinden, oder in Transitländer zu solchen Orten begibt. Es kann sich z. B. auch um eine Person handeln, über die den Nachrichtendiensten Erkenntnisse vorliegen, die darauf hindeuten, dass sie eine Geiselnahme vorbereitet und sich ausweislich der Beförderungsdaten in ein Land begibt, von dem die Nachrichtendienste aufgrund der erhaltenen Informationen wissen, dass diese Person dort zur Durchführung ihrer Pläne andere Personen rekrutieren könnte. Außerdem ist die Wahrscheinlichkeit einer tatsächlichen Bedrohung umso höher, je mehr Treffer in Bezug auf ein und dieselbe Person von mehreren Diensten entdeckt werden.

Ein Treffer kann es auch erforderlich machen, auf Anordnung der Justizbehörden Maßnahmen zu ergreifen wie z. B. die Vollstreckung eines Haftbefehls gegen eine Person, die im Begriff ist, Belgien zu verlassen.

Ein Treffer kann sich auch aus einem Abgleich mit internationalen Datenbanken wie z. B. SIS II oder Interpol (SLTD) ergeben.

Das Ziel besteht natürlich nicht darin, sämtliche Datenbanken der Dienste mit der Passagierdatenbank zu verbinden, sondern darin, den Abgleich mit technischen Mitteln auf die Datenbanken zu begrenzen, die in unmittelbarem Zusammenhang mit den gesetzlich festgelegten Zwecken stehen.

…

Dieser Abgleich kann auch anhand von Personenlisten erfolgen, die die zuständigen Dienste speziell zu diesem Zweck erstellen. Gemäß dem Gesetz über den Schutz des Privatlebens und speziell dessen Art. 4 § 1 Nr. 4 müssen diese Listen regelmäßig aktualisiert werden“ (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, S. 28-29).

70 Zur Korrelation mit im Voraus festgelegten Kriterien wird in den Vorarbeiten zum PNR-Gesetz ausgeführt:

„Der zweite Ansatz besteht darin, mit Hilfe (eines oder mehrerer) von der PNR-Zentralstelle im Voraus festgelegter Kriterien, die auf die Passagierdaten angewandt werden, nach positiven Übereinstimmungen zu suchen. Diese Kriterien bestehen aus einem oder mehreren objektiven Indikatoren, aus denen abgeleitet werden kann, dass die Personen, die diesen Kriterien entsprechen, ein spezifisches Risikoverhalten aufweisen, das im Hinblick auf die Zwecke von Art. 8 § 1 Nr. 1, 4 und 5 des Gesetzes eine Bedrohung darstellen kann.

Zu diesen Kriterien können beispielsweise bestimmte spezifische Verhaltensweisen bei der Reservierung oder der Reise gehören.

Ihre Verwendung bietet den Vorteil, Profile von bislang nicht notwendigerweise bekannten oder in den Datenbanken der Dienste erwähnten Risikopassagieren zutage treten zu lassen.

Diese Kriterien können sich z. B. auf ein Bestimmungs- oder Abreiseland beziehen, verbunden mit bestimmten Reiseinformationen wie Zahlungsmethode und Reservierungsdatum“ (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, S. 29-30).

„Die Vorabüberprüfung im Rahmen des Zwecks der Beobachtung verwaltungspolizeilicher Phänomene und von Gruppierungen im Zusammenhang mit der gewalttätigen Radikalisierung unterliegt weit strengeren Voraussetzungen als die anderen Zwecke …

Für die Vorabüberprüfung im Rahmen der anderen Zwecke ist der Zugang zu allen in Art. 9 aufgeführten Passagierdaten gestattet“ (ebd., S. 31).

„Die positive Übereinstimmung muss in jedem Fall von der PNR-Zentralstelle validiert werden. Um die uneingeschränkte Einhaltung des Rechts auf Schutz personenbezogener Daten … zu gewährleisten, darf nämlich keine Entscheidung, die Rechtsfolgen für eine Person hat oder ihr schweren Schaden zufügen kann, auf der bloßen Grundlage der automatisierten Verarbeitung der Datensätze, die Informationen über ihre Reise enthalten, getroffen werden. Deshalb muss jeder für die betroffene Person verbindlichen Entscheidung eine menschliche Bewertung vorausgehen.

Diese Validierung muss innerhalb von 24 Stunden erfolgen, um das Recht auf Zugang zur Passagierdatenbank zu eröffnen.

Nach dieser Validierung der positiven Übereinstimmung haben die Dienste, auf deren Erkenntnissen diese Übereinstimmung beruht, innerhalb einer angemessenen Frist für die sachdienlichen Maßnahmen zu sorgen. Eine sachdienliche Maßnahme kann ein aktives Eingreifen (Durchsuchung, Festnahme usw.) bedeuten, aber auch darin bestehen, vorläufig nicht aktiv einzugreifen. Diese operative Beurteilung obliegt vollständig den zuständigen Dienststellen“ (ebd., S. 30-31).

71 Als Grundlage der von der PNR-Zentralstelle im Voraus festgelegten Kriterien dürfen keine Daten dienen, aus denen die rassische oder ethnische Herkunft einer Person, ihre religiösen oder weltanschaulichen Überzeugungen, ihre politischen Meinungen, ihre Mitgliedschaft in einer Gewerkschaftsorganisation, ihr Gesundheitszustand, ihr Sexualleben oder ihre sexuelle Orientierung hervorgehen. Die Überprüfung der Passagiere vor ihrer Ankunft, ihrer Durchreise oder ihrer Abreise anhand im Voraus festgelegter Kriterien erfolgt in nichtdiskrimierender Weise. Diese Kriterien dürfen nicht darauf abzielen, eine Person zu identifizieren, und müssen zielgerichtet, verhältnismäßig und bestimmt sein.

72 In seiner Stellungnahme vom 19. August 2016 hat der Beratende Ausschuss für das Übereinkommen Nr. 108 Folgendes ausgeführt:

„*Die Verarbeitung personenbezogener Daten kann alle Passagiere und nicht nur die Menschen betreffen, die gezielt verdächtigt werden, an einer Straftat beteiligt zu sein oder eine unmittelbare Bedrohung der nationalen Sicherheit oder der öffentlichen Ordnung darzustellen.*

…

Die Überprüfung der Passagiere durch den Abgleich von Daten kann die Frage der Vorhersehbarkeit aufwerfen, insbesondere wenn sie auf der Grundlage von prädiktiven Algorithmen unter Verwendung dynamischer Kriterien durchgeführt wird, die sich entsprechend der Selbstlernfähigkeit kontinuierlich weiterentwickeln können.

Die Entwicklung von Data-Mining-Algorithmen sollte sich auf die Ergebnisse regelmäßiger Bewertungen der wahrscheinlichen Auswirkungen der Datenverarbeitung auf die Rechte und Freiheiten der betroffenen Personen stützen.

Die Grundstruktur der Analysen sollte sich auf vordefinierte Risikoindikatoren stützen, die zuvor eindeutig festgelegt wurden.

Die Relevanz der individuellen Ergebnisse dieser automatischen Bewertungen sollte in jedem Einzelfall sorgfältig durch eine Person in nicht automatisierter Weise geprüft werden“ (Europarat, Stellungnahme vom 19. August 2016, T–PD(2016)18 rev, S. 8).

73 Im vorliegenden Fall sind die in Art. 24 aufgeführten Datenbanken genau definiert und stehen in unmittelbarem Zusammenhang mit den in Art. 8 des PNR-Gesetzes genannten Zwecken. Es handelt sich nämlich um die Datenbanken der „zuständigen Behörden“, d. h. der Polizeidienste, der Staatssicherheit, des Allgemeinen Nachrichten- und Sicherheitsdienstes und des Zolls.

Außerdem stellt Art. 24 §§ 4 und 5 sicher, dass die systematische automatisierte Verarbeitung im Fall eines Treffers mit nicht automatisierten Mitteln individuell überprüft wird, um zu beurteilen, ob die zuständige Behörde Maßnahmen im Einklang mit dem nationalen Recht ergreifen muss, wie es Art. 6 Abs. 5 der PNR-Richtlinie verlangt.

74 In seinem Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017 (EU:C:2017:592) hatte der Gerichtshof ebenfalls nachdrücklich auf die Notwendigkeit hingewiesen, eine individuelle Überprüfung mit nicht automatisierten Mitteln vorzunehmen, bevor eine individuelle Maßnahme getroffen wird (Rn. 173).

Das vorgeschriebene menschliche Eingreifen nach einer positiven Übereinstimmung stellt eine Garantie dar, die sicherstellen kann, dass die Vorabüberprüfung nicht allein auf automatisierten Mitteln beruht, und trägt so zur Leistungsfähigkeit des Systems bei.

Eine systematische Vorabüberprüfung der Passagiere ist daher grundsätzlich eine Maßnahme, die für das Ziel, Gefahren für die öffentliche Sicherheit zu erkennen und zu verhüten, relevant ist.

Wie der Gerichtshof jedoch in seinem Gutachten 1/15 vom 26. Juli 2017 festgestellt hat, können durch die Verarbeitungen, die sich aus der Vorabüberprüfung ergeben, „*weitere Informationen über das Privatleben der Fluggäste erlangt werden*“ (Rn. 131), und „*[d]ie Analysen werden zudem durchgeführt, ohne dass konkrete Anhaltspunkte dafür vorliegen, dass von den betreffenden Personen eine Gefahr für die öffentliche Sicherheit ausgehen könnte*“ (ebd., Rn. 132).

Unter Hinweis darauf, dass die automatisierte Verarbeitung der „PNR-Daten“, die auf im Voraus festgelegten Modellen und Kriterien beruht, mit einer nicht zu vernachlässigenden Fehlerquote behaftet ist (ebd. Rn. 169-170), hat der Gerichtshof jedoch die Auffassung vertreten, dass „*die im Voraus festgelegten Modelle und Kriterien deshalb spezifisch und zuverlässig sein [müssten], so dass sie die Identifizierung von Personen ermöglichen, gegen die ein begründeter Verdacht der Beteiligung an terroristischen Straftaten oder grenzübergreifender schwerer Kriminalität bestehen könnte, und … nicht diskriminierend sein [dürften]*“, und dass „*die Datenbanken, mit denen die PNR-Daten abgeglichen werden, zuverlässig und aktuell sein und von Kanada in Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität betrieben werden [müssten]*“ (ebd., Rn. 172). Um schließlich zu gewährleisten, dass diese Bewertung nicht diskriminierend ist und sich auf das absolut Notwendige beschränkt, hat der Gerichtshof ausgeführt, dass „*die Zuverlässigkeit und Aktualität dieser Modelle und Kriterien sowie der verwendeten Datenbanken, unter Berücksichtigung statistischer Daten und der Ergebnisse der internationalen Forschung, Gegenstand der … gemeinsamen Überprüfung [der] Durchführung des geplanten Abkommens sein [muss]*“, und zwar ein Jahr nach dessen Inkrafttreten und danach in regelmäßigen Abständen (ebd., Rn. 174).

75 Darüber hinaus erscheint es technisch unmöglich, die im Voraus festgelegten Kriterien für die Bestimmung von Risikoprofilen weiter zu definieren. Wie bereits erwähnt, müssen diese Kriterien spezifisch, zuverlässig und nicht diskriminierend sein.

76 Obwohl die PNR-Richtlinie und das PNR-Gesetz keinen Hinweis darauf geben, auf welche Weise die der Vorabüberprüfung zugrunde liegenden Kriterien von der PNR-Zentralstelle im Voraus festgelegt werden, reichen die Garantien, mit denen die Ausarbeitung dieser Kriterien versehen ist, offenbar aus, um die angefochtene Maßnahme nicht als unverhältnismäßig anzusehen. Um entscheiden zu können, ob die systematische Vorabüberprüfung hinreichend klar, präzise und auf das absolut Notwendige beschränkt ist, ist dem Gerichtshof jedoch eine sechste Frage zur Vorabentscheidung vorzulegen.

– *Gezielte Recherchen (Art. 27, 50 und 51)*

77 Art. 27 des PNR-Gesetzes gestattet die Verarbeitung der Passagierdaten, um gezielte Recherchen zu den in Art. 8 § 1 Nr. 1, 2, 4 und 5 erwähnten Zwecken und unter den Bedingungen des Art. 46*septies* des Strafprozessgesetzbuches oder des Art. 16/3 des Gesetzes vom 30. November 1998 durchzuführen, die durch Art. 50 bzw. 51 des PNR-Gesetzes eingefügt wurden. Gemäß Art. 20 des PNR-Gesetzes gelten die Voraussetzungen für die Anwendung von Art. 27 auch für Anträge auf Zugang, die nach Ablauf der in Art. 19 vorgesehenen Frist von sechs Monaten gestellt werden.

78 Art. 46*septies* des Strafprozessgesetzbuches betrifft gezielte Recherchen im Rahmen der in Art. 8 § 1 Nr. 1, 2 und 5 des PNR-Gesetzes genannten Zwecke.

Diese Maßnahme ist mit mehreren Garantien versehen, darunter der vorherigen Genehmigung des Prokurators des Königs.

79 Artikel 16/3 des Gesetzes vom 30. November 1998 betrifft seinerseits gezielte Recherchen im Rahmen des in Art. 8 § 1 Nr. 4 des PNR-Gesetzes genannten Zwecks. Diese Maßnahme ist mit mehreren Garantien versehen, darunter der Unterrichtung und Kontrolle des Ständigen Ausschusses N.

80 Die Klägerin hält die entsandten Mitglieder der Polizeidienste, die der PNR-Zentralstelle angehören, für nicht unabhängig genug, um Anträge auf Zugang im Rahmen dieser gezielten Recherchen zu beantworten.

81 Art. 14 § 1 des PNR-Gesetzes bestimmt die Zusammensetzung der PNR-Zentralstelle. Die Vorarbeiten führen hierzu aus: „*Das belgischen Modell beruht auf dem Konzept einer multidisziplinären Einheit, die sich aus einem leitenden Beamten, der die Führungsausgabe wahrnimmt, Verwaltungsmitgliedern und entsandten Mitgliedern der zuständigen Dienste zusammensetzt.*

Die PNR-Zentralstelle setzt sich zusammen aus:

- *einem leitenden Beamten, dem ein Unterstützungsdienst beisteht und der innerhalb des Föderalen Öffentlichen Dienstes Inneres u. a. für die Verwaltung der Datenbank, die Einhaltung der Verpflichtungen durch die Beförderungs- und Reiseunternehmen, die Berichterstattung, den Abschluss von Vereinbarungsprotokollen mit den zuständigen Diensten und die Einhaltung der Bedingungen für die Verarbeitung verantwortlich ist. Der Unterstützungsdienst setzt sich insbesondere aus Analysten, Juristen, Fachleuten für Informations- und Kommunikationstechnologie und dem Datenschutzbeauftragten zusammen, die über die erforderlichen Sicherheitsermächtigungen verfügen,*

- *entsandten Mitgliedern der in § 1 Nr. 2 abschließend aufgeführten zuständigen Dienste, nämlich der Polizeidienste, der Nachrichtendienste und des Zolls. Die präzisen Zwecke stellen als solche die erste Beschränkung dar. Beispielsweise liegt auf der Hand, dass auf der Ebene der integrierten Polizeidienste ein Revierpolizist einer örtlichen Polizeidienststelle niemals Kenntnis von Passagierdaten erlangen darf, weil die Zwecke nicht in seinen Aufgabenbereich fallen.*

Die Entsendung durch die zuständigen Dienste zielt darauf ab, ein gewisses Maß an Sachkunde zu gewährleisten, schließt aber in keiner Weise aus, dass zwischen diesen Diensten Vereinbarungen getroffen werden, um die Entsendungen zu koordinieren“ (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, S. 22).

Der Minister der Sicherheit und des Innern hat hinzugefügt, dass *„auch … ein Datenschutzbeauftragter [ernannt wird], der beauftragt ist, dem Ausschuss für den Schutz des Privatlebens* zu berichten“ (*Doc. parl*, Chambre, 2015-2016, DOC 54-2069/003, S. 24).

Der königliche Erlass vom 21. Dezember 2017 zur Durchführung des PNR-Gesetzes regelt die Einzelheiten der Zusammensetzung und Organisation der PNR-Zentralstelle. In dem Bericht an den König, der diesem Königlichen Erlass vorausging, heißt es: „*Die Datenbank darf nur innerhalb der PNR-Zentralstelle und nur von den Mitgliedern der PNR-Zentralstelle im Rahmen ihrer Aufgaben sowie vom Datenschutzbeauftragten abgefragt werden*“[3].

Das Verfahren der Entsendung wird in Art. 12 bis 21 dieses königlichen Erlasses geregelt. Die Mitwirkung der von den zuständigen Diensten entsandten Mitglieder bei der Tätigkeit der PNR-Zentralstelle soll gewährleisten, dass sich diese Zentralstelle aus Personen zusammensetzt, die über ein gewisses Maß an Sachkunde verfügen, um so die Leistungsfähigkeit der PNR-Zentralstelle zu erhöhen. Diese Möglichkeit der Entsendung ist im Übrigen in Art. 4 Abs. 3 der PNR-Richtlinie ausdrücklich vorgesehen.

Es gibt keinen Grund für die Annahme, dass diese Personen, auch wenn sie ihren Status in ihrem ursprünglichen Dienst behalten, ihre Tätigkeit innerhalb der PNR-Zentralstelle nicht unabhängig ausüben. Die Mitglieder der UIP unterliegen außerdem strafrechtlichen Sanktionen, wenn sie das Berufsgeheimnis nicht wahren oder wissentlich und willentlich Informationen, Daten und Auskünfte zurückhalten, wodurch die in Art. 8 vorgesehenen Zwecke behindert werden (Art. 48 und 49).

82 Was den Zugang zu den „PNR-Daten“ im Rahmen gezielter Recherchen nach Ablauf einer Frist von sechs Monaten betrifft, hat der Gerichtshof in seinem Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017 (EU:C:2017:592) die Auffassung vertreten, dass sich die Verwendung der auf diese Weise gespeicherten PNR-Daten *„auf objektive Kriterien [stützen müsste], die definieren, unter welchen Umständen und unter welchen Voraussetzungen die im geplanten Abkommen genannten kanadischen Behörden Zugang zu diesen Daten haben und sie verwenden dürfen“,* und dass *„eine solche Verwendung – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen werden [müsste], wobei die Entscheidung, mit der die Verwendung genehmigt wird, im Anschluss an einen mit Gründen versehenen Antrag ergeht, der von den zuständigen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Aufdeckung oder Verfolgung von Straftaten gestellt wird“* (Rn. 208).

83 Um zu überprüfen, ob die PNR-Zentralstelle als eine solche „andere nationale Behörde“ im Sinne von Art. 12 Abs. 3 der PNR-Richtlinie angesehen werden kann, ist dem Gerichtshof vor einer Entscheidung in der Sache eine siebte Frage zur Vorabentscheidung vorzulegen.

3 *Moniteur belge* vom 29. Dezember 2017, Ed. 2, S. 116833.

Zur Aufbewahrungsfrist der „PNR-Daten“ (Art. 18 des PNR-Gesetzes)

84 Die Klägerin hält die Frist von fünf Jahren, während der die „PNR-Daten“ aufbewahrt werden, für unverhältnismäßig.

85 Der 25. Erwägungsgrund der PNR-Richtlinie lautet:

„Der Zeitraum, für den die PNR-Daten vorgehalten werden sollen, sollte so lang sein, wie dies für den mit ihnen verfolgten Zweck der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten sowie schwerer Kriminalität erforderlich ist, und in einem angemessenen Verhältnis dazu stehen. Das Wesen der PNR-Daten und ihr Verwendungszweck bringen es mit sich, dass diese so lange gespeichert werden müssen wie nötig, um sie auswerten und für Ermittlungen nutzen zu können. Um einen unverhältnismäßigen Rückgriff auf die Daten auszuschließen, sollten die PNR-Daten nach der anfänglichen Speicherfrist durch Unkenntlichmachung von Datenelementen depersonalisiert werden. Um das höchste Datenschutzniveau zu gewährleisten, sollte Zugriff auf die vollständigen PNR-Daten, die die unmittelbare Identifizierung der betroffenen Person ermöglichen, nach dieser anfänglichen Frist nur unter eingeschränkten, sehr strengen Bedingungen gewährt werden.“

86 Nach der Rechtsprechung des Gerichtshofs muss die Dauer der Aufbewahrung der Daten „stets objektiven Kriterien genügen …, die einen Zusammenhang zwischen den zu speichernden personenbezogenen Daten und dem verfolgten Ziel herstellen“ (Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 93, Beschluss vom 16. März 2017, Tele2 Sverige und Watson u. a., C-203/15 REC und C-698/15 REC, EU:C:2017:222, Rn. 110, und Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017, EU:C:2017:592, Rn. 191).

87 Speziell zu den „PNR-Daten“ hat der Gerichtshof in seinem vorgenannten Gutachten 1/15 vom 26. Juli 2017 ausgeführt, dass „*die Dauer von fünf Jahren nicht über das hinausgeht, was zur Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität absolut notwendig ist*“ (Rn. 209), allerdings mit dem Vorbehalt, dass „*bei Fluggästen, bei denen eine solche Gefahr weder bei ihrer Ankunft in Kanada noch bis zu ihrer Ausreise aus diesem Drittland festgestellt wurde, nach ihrer Ausreise kein Zusammenhang, sei er auch mittelbarer Art, zwischen ihren PNR-Daten und dem mit dem geplanten Abkommen verfolgten Ziel bestehen [dürfte], der … eine dauerhafte Speicherung der PNR-Daten sämtlicher Fluggäste nach ihrer Ausreise aus Kanada zum Zweck eines eventuellen Zugangs zu diesen Daten unabhängig von jedem Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität … rechtfertigen [könnte] (vgl. entsprechend Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 119)*“ (Rn. 205).

88 Art. 18 des PNR-Gesetzes sieht vor, dass die Passagierdaten höchstens fünf Jahre ab ihrer Speicherung in der Passagierdatenbank aufbewahrt und am Ende dieser

Frist vernichtet werden. Gemäß Art. 21 § 1 dieses Gesetzes stellt die PNR-Zentralstelle sicher, dass die Passagierdaten am Ende des in Art. 18 erwähnten Zeitraums dauerhaft aus ihrer Datenbank gelöscht werden.

Die Frist von fünf Jahren ist jedoch in Verbindung mit den Artikeln 19 ff. dieses Gesetzes zu betrachten, die ebenfalls Einzelheiten der Aufbewahrung der Daten regeln. Art. 19 dieses Gesetzes ist seinerseits in Verbindung mit Art. 4 Nr. 14 zu lesen, der die „Depersonalisierung durch Unkenntlichmachung von Datenelementen" als „die in Art. 19 erwähnte Vorgehensweise, mit der diejenigen Datenelemente, mit denen die Identität der betreffenden Person unmittelbar festgestellt werden könnte, für einen Nutzer unsichtbar gemacht werden" definiert.

Art. 20 des PNR-Gesetzes sieht vor, dass die Mitteilung der vollständigen Passagierdaten nach Ablauf des in Art. 19 erwähnten sechsmonatigen Zeitraums nur für die durch Art. 27 vorgeschriebene Datenverarbeitung und auch nur unter den in dieser Bestimmung festgelegten Bedingungen zugelassen ist.

Außerdem wird das in Art. 24 erwähnte Ergebnis der Verarbeitung von der PNR-Zentralstelle nur solange aufbewahrt, wie dies erforderlich ist, um die zuständigen Behörden und die PNR-Zentralstellen anderer Mitgliedstaaten über einen Treffer zu informieren (Art. 21 § 3 Abs. 1).

Art. 22 des PNR-Gesetzes gewährleistet, dass der leitende Beamte und der Datenschutzbeauftragte nur im Rahmen der Ausführung ihrer Aufträge Zugriff auf alle relevanten Daten haben.

Schließlich wird die Datenverarbeitung protokolliert und steht in direktem Zusammenhang mit den in Art. 8 vorgesehenen Zwecken (Art. 23 § 1). Die PNR-Zentralstelle sorgt für die Protokollierung, indem sie Aufzeichnungen über alle ihrer Zuständigkeit unterliegenden Verarbeitungssysteme und -verfahren fünf Jahre lang aufbewahrt (Art. 23 § 2 Abs. 1).

89 Die Dauer der Aufbewahrung der Passagierdaten ist unter Berücksichtigung der Zwecke der Verarbeitung dieser Daten in unmittelbarem Zusammenhang mit den Zwecken der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität zu bestimmen.

90 Der Ausschuss für den Schutz des Privatlebens hatte jedoch festgestellt, dass bei langer Aufbewahrungsfrist und massenhafter Speicherung der Daten „die Gefahr der Erstellung von Profilen der betroffenen Personen ebenso zunimmt wie die Gefahr der Zweckentfremdung (*fonction creep*), d. h. des potenziellen Missbrauchs der Verwendung der Daten im Hinblick auf andere Straftaten, für die ursprünglich keine (politische) Vereinbarung über den Austausch von Daten bestand" (Ausschuss für den Schutz des Privatlebens, Initiativgutachten Nr. 01/2010 vom 13. Januar 2010 zum Entwurf eines Gesetzes über die Zustimmung zu dem am 23. Juli 2007 in Brüssel und am 26. Juli 2007 in Washington geschlossenen Abkommen zwischen der Europäischen Union und

den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS) (PNR-Abkommen von 2007), Nr. 3.3, S. 17-18).

In seinem Gutachten Nr. 55/2015 vom 16. Dezember 2015 zum Vorentwurf des späteren PNR-Gesetzes war der Ausschuss für den Schutz des Privatlebens ebenfalls der Ansicht, dass die Notwendigkeit einer fünfjährigen Frist für die Aufbewahrung der Daten präziser und fundierter gerechtfertigt werden müsse.

In seiner Stellungnahme vom 19. August 2016 hatte der Beratende Ausschuss für das Übereinkommen Nr. 108 ebenfalls ausgeführt, dass „unkenntlich gemachte Daten es nach wie vor ermöglichen, Personen zu identifizieren, und deshalb weiterhin personenbezogene Daten bleiben, und dass ihre Speicherung ebenfalls zeitlich begrenzt werden sollte, um eine ständige allgemeine Überwachung zu verhindern“ (Stellungnahme vom 19. August 2016, T–PD(2016)18rev, S. 9).

91 Zur Prüfung der Frage, ob diese durch die PNR-Richtlinie gestattete Aufbewahrungsfrist von fünf Jahren in Anbetracht der vorstehenden Ausführungen und der oben in Rn. 88 aufgeführten Garantien mit den oben in Rn. 87 erwähnten Feststellungen des Gerichtshofs vereinbar ist, obwohl sie nicht danach unterscheidet, ob die betroffenen Passagiere sich im Rahmen der Vorabüberprüfung als eine mögliche Gefahr für die öffentliche Sicherheit erweisen oder nicht, hält der Verfassungsgerichtshof es für erforderlich, dem Gerichtshof eine achte Frage zur Vorabentscheidung vorzulegen.

3. Zweiter Klagegrund

92 Die Klägerin ist der Auffassung, dass die angefochtenen Vorschriften durch die Ausweitung des „PNR-Systems“ auf Flüge innerhalb der EU indirekt wieder Grenzkontrollen einführen, die gegen die Freizügigkeit verstoßen.

93 Zum Anwendungsbereich des PNR-Gesetzes wird in den Vorarbeiten ausgeführt:

„Die Einbeziehung von Intra-EU-Daten in die Datenerhebung wird es ermöglichen, ein umfassenderes Bild der Bewegungen von Passagieren zu erhalten, die eine potenzielle Bedrohung für die innergemeinschaftliche und nationale Sicherheit darstellen. Die Praxis hat bereits gezeigt, dass bestimmte ‚*returnees*‘ (sogenannte *foreign fighters*, die nach Europa zurückkehren) eine Reihe verschiedener Flüge besteigen, bevor sie ihren endgültigen Zielort erreichen.

Die PNR-Richtlinie räumt den Mitgliedstaaten ausdrücklich die Möglichkeit ein, PNR-Daten von EU-Fluggästen im internationalen Verkehr innerhalb der Europäischen Union zu verarbeiten. Außerdem haben alle Mitgliedstaaten am 21. April 2016 im Rat der Innen- und Justizminister eine Erklärung gebilligt, die darauf abzielt, die PNR-Richtlinie auch für den Verkehr innerhalb der

Europäischen Union in das jeweilige nationale Recht umzusetzen“ (Doc. Parl., Chambre, 2015-2016, DOC 54-2069/001, S. 7).

94 Der Verfassungsgerichtshof weist darauf hin, dass die in Kapitel 11 des PNR-Gesetzes genannten Passagiere, ebenso wie die genannten Daten und die Aufbewahrungsfrist, begrenzt sind.

In den Vorarbeiten wurde nämlich ausgeführt, dass „nur die Passagiere betroffen sind, die die belgischen Außengrenzen zur Einreise oder Ausreise überschreiten wollen oder überschritten haben, unabhängig von der Art der benutzten Beförderung (Seeweg, Eisenbahnweg, Landweg, Luftweg). Daher werden nur die Daten dieser Passagiere durch die Polizeidienste, die mit der Grenzkontrolle beauftragt sind, und durch das Ausländeramt verarbeitet.

Passagiere, die eine Durchreise durch die internationale Transitzone z. B. eines in Belgien gelegenen Flughafens beabsichtigen, sind ebenfalls insoweit betroffen, als die Regelungen über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Entfernen von Ausländern auch für sie gelten. Somit müssen diese Personen über die erforderlichen Reisedokumente verfügen. Bestimmte Personen benötigen ein Flughafentransitvisum; Kontrollen in diesen Zonen sind gestattet und können in bestimmten Fällen zu einer Zurückweisung führen.

… nur die sogenannten ‚API-Daten‘ werden aufgrund dieses Kapitels an die Polizeidienste und an das Ausländeramt übermittelt. Diese Daten sind in Art. 9 § 2 des Vorentwurfs zu diesem Gesetz aufgeführt.

Sie entsprechen im Wesentlichen denen, die die Fluggesellschaften bereits nach dem Königlichen Erlass vom 11. Dezember 2006 übermitteln müssen.

…

Auch die Verwendung der Daten ist auf vierundzwanzig Stunden beschränkt. Wenn der Zugang auf die Passagierdaten nach Ablauf dieser Frist noch notwendig ist, damit das Ausländeramt seine gesetzlichen Aufträge ausführen kann, richtet das Ausländeramt eine gebührend mit Gründen versehene Anfrage an die PNR-Zentralstelle“ (ebd., S. 34-35).

95 Wie oben bereits erwähnt, erlaubt der zehnte Erwägungsgrund der PNR-Richtlinie die Ausdehnung des „PNR-Systems“ auf EU-Flüge. Art. 2 der PNR-Richtlinie regelt die Verfahren zur Ausweitung des Anwendungsbereichs.

Der Zweck der Bekämpfung der illegalen Einwanderung und der Verbesserung der Grenzkontrolle betrifft nur die in Art. 29 § 2 des PNR-Gesetzes aufgeführten Kategorien von Passagieren und beschränkt sich auf die in Art. 9 § 1 Nr. 18 dieses Gesetzes genannten „API-Daten“. Die im Rahmen dieses Zwecks durchgeführten Verarbeitungen sind ebenfalls beschränkt. Die angefochtenen Vorschriften gehören zum Rahmen der Umsetzung der „API-Richtlinie“, die ebenfalls die

Bekämpfung der illegalen Einwanderung und die Verbesserung der Grenzkontrolle zum Ziel hat.

96 In seiner Stellungnahme Nr. 55/2015 vom 16 Dezember 2015 zum Vorentwurf des späteren Gesetzes vom 25. Dezember 2016 fragt sich der Ausschuss für den Schutz des Privatlebens jedoch, ob es mit dem Grundsatz der Freizügigkeit vereinbar ist, dass das eingeführte „PNR-System“ „sowohl Beförderungen nach und aus dem Schengen-Raum (extra-Schengen) als auch Beförderungen innerhalb des Schengen-Raums (intra-Schengen)“ erfasst, was „mittelbar zur Wiedereinführung der Kontrollen an den Binnengrenzen“ führen könnte (Rn. 21-25).

97 Da der Verfassungsgerichtshof Zweifel hinsichtlich der Auslegung und der Gültigkeit der „API-Richtlinie“ 2004/82 im Licht der Charta und des AEU-Vertrags hat, beschließt er, dem Gerichtshof eine neunte Frage zur Vorabentscheidung vorzulegen.

98 Der Verfassungsgerichtshof legt eine letzte Frage zur Vorabentscheidung vor, die sich auf die mögliche zeitliche Beschränkung der Wirkungen seines Urteils bezieht.

IV. Vorlagefragen

Der Verfassungsgerichtshof stellt daher die folgenden Fragen zur Vorabentscheidung:

1. Ist Art. 23 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 (Datenschutz-Grundverordnung) in Verbindung mit Art. 2 Abs. 2 Buchst. d dieser Verordnung so auszulegen, dass er auf einzelstaatliche Rechtsvorschriften wie das Gesetz vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten, mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, sowie die Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln, und die Richtlinie 2010/65/EU des Europäischen Parlaments und des Rates vom 20. Oktober 2010 über Meldeformalitäten für Schiffe beim Einlaufen in und/oder Auslaufen aus Häfen der Mitgliedstaaten und zur Aufhebung der Richtlinie 2002/6/EG umgesetzt wird, anwendbar ist?

2. Ist Anhang I der Richtlinie (EU) 2016/681 mit den Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union in dem Sinne vereinbar, dass die darin aufgeführten Daten sehr weitgehend sind – insbesondere die in Nr. 18 von Anhang I der Richtlinie (EU) 2016/681 erwähnten Daten, die über die in Art.

3 Abs. 2 der Richtlinie 2004/82/EG erwähnten Daten hinausgehen – insofern sie zusammen genommen sensible Daten offenlegen könnten und so über das „absolut Notwendige“ hinausgehen könnten?

3. Sind die Nrn. 12 und 18 des Anhangs I der Richtlinie (EU) 2016/681 mit den Art.7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union vereinbar, insofern unter Berücksichtigung des Wortes „einschließlich“ die dort aufgeführten Daten in beispielhafter und nicht erschöpfender Weise genannt werden, was somit gegen die Anforderung der Präzision und Klarheit der Regeln, die einen Eingriff in das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten nach sich ziehen, verstoßen könnte?

4. Sind Art 3 Nr. 4 der Richtlinie (EU) 2016/681 und Anhang I dieser Richtlinie mit den Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union vereinbar, insofern das System zur allgemeinen Erhebung, Übermittlung und Verarbeitung von Passagierdaten, das mit diesen Bestimmungen eingeführt wird, auf jede Person abzielt, die das betreffende Beförderungsmittel benutzt, unabhängig von einem objektiven Anhaltspunkt für die Annahme, dass von dieser Person eine Gefahr für die öffentliche Sicherheit ausgehen könnte?

5. Ist Art. 6 der Richtlinie (EU) 2016/681 in Verbindung mit den Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das als Verarbeitungszweck der PNR-Daten die Beaufsichtigung der erwähnten Aktivitäten durch die Nachrichten- und Sicherheitsdienste zulässt und so diesen Zweck in die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität aufnimmt?

6. Ist Art. 6 der Richtlinie (EU) 2016/681 mit den Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union vereinbar, insofern die in ihm geregelte Vorabüberprüfung durch eine Korrelation mit Datenbanken und im Voraus festgelegten Kriterien systematisch und allgemein auf die Passagierdaten angewandt wird, unabhängig von einem objektiven Anhaltspunkt für die Annahme, dass von diesen Fluggästen eine Gefahr für die öffentliche Sicherheit ausgehen könnte?

7. Kann der in Art. 12 Abs. 3 der Richtlinie (EU) 2016/681 erwähnte Ausdruck „andere nationale Behörde, die ... zuständig ist“ dahin ausgelegt werden, dass er sich auf die PNR-Zentralstelle bezieht, die durch das Gesetz vom 25. Dezember 2016 geschaffen wurde und die somit den Zugriff auf die PNR-Daten nach einer sechsmonatigen Frist im Rahmen von gezielten Recherchen gestatten dürfte?

8. Ist Art. 12 der Richtlinie (EU) 2016/681 in Verbindung mit den Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das eine allgemeine Aufbewahrungsdauer für die Daten von fünf

Jahren vorsieht, ohne eine Unterscheidung danach vorzunehmen, ob sich im Rahmen der Vorabüberprüfung herausstellt, dass die betroffenen Fluggäste ein Risiko für die öffentliche Sicherheit darstellen können oder nicht?

9. a) Ist die Richtlinie 2004/82/EG mit Art. 3 Abs. 2 des Vertrags über die Europäische Union und mit Art. 45 der Charta der Grundrechte der Europäischen Union vereinbar, insofern die Pflichten, die sie einführt, für Flüge innerhalb der Europäischen Union gelten?

b) Ist die Richtlinie 2004/82/EG in Verbindung mit Art. 3 Abs. 2 des Vertrags über die Europäische Union und mit Art. 45 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass sie einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das zum Zwecke der Bekämpfung der illegalen Einwanderung und der Verbesserung der Grenzkontrollen ein System zur Erhebung und Verarbeitung der Daten „zu den in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet“ beförderten Passagieren gestattet, was indirekt eine Wiedereinführung von Kontrollen an den Binnengrenzen bedeuten könnte?

10. Könnte der Verfassungsgerichtshof, falls er auf der Grundlage der Antworten auf die vorstehenden Vorabentscheidungsfragen zu dem Schluss gelangen sollte, dass das angefochtene Gesetz, mit dem insbesondere die Richtlinie (EU) 2016/681 umgesetzt wird, gegen eine oder mehrere der Verpflichtungen verstößt, die sich aus den in diesen Fragen genannten Bestimmungen ergeben, die Folgen des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten vorläufig aufrechterhalten, um eine Rechtsunsicherheit zu vermeiden und es zu ermöglichen, dass die zuvor gesammelten und auf Vorrat gespeicherten Daten noch für die durch das Gesetz angestrebten Ziele benutzt werden können?