

|                                                |
|------------------------------------------------|
| Geschäftsverzeichnisnr. 6713                   |
| Entscheid Nr. 135/2019<br>vom 17. Oktober 2019 |

## ENTSCHEID

---

*In Sachen:* Klage auf völlige oder teilweise Nichtigerklärung des Gesetzes vom 25. Dezember 2016 «über die Verarbeitung von Passagierdaten», erhoben von der VoG «Ligue des Droits de l'Homme».

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten F. Daoût und A. Alen, und den Richtern T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen und J. Moerman, unter Assistenz des Kanzlers F. Meersschaut, unter dem Vorsitz des Präsidenten F. Daoût,

erlässt nach Beratung folgenden Entscheid:

\*

\*      \*

## I. Gegenstand der Klage und Verfahren

Mit einer Klageschrift, die dem Gerichtshof mit am 24. Juli 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 26. Juli 2017 in der Kanzlei eingegangen ist, erhob die VoG « Ligue des Droits de l'Homme » (nunmehr « Ligue des droits humains »), unterstützt und vertreten durch RÄin C. Forget, in Brüssel zugelassen, Klage auf völlige oder teilweise (Artikel 3 § 1, 8 § 2 und Kapitel 11) Nichtigkeitserklärung des Gesetzes vom 25. Dezember 2016 « über die Verarbeitung von Passagierdaten » (veröffentlicht im *Belgischen Staatsblatt* vom 25. Januar 2017).

Der Ministerrat, unterstützt und vertreten durch RA E. Jacobowitz und RÄin C. Caillet, in Brüssel zugelassen, hat einen Schriftsatz eingereicht, die klagende Partei hat einen Erwidierungsschriftsatz eingereicht und der Ministerrat hat auch einen Gegenerwidierungsschriftsatz eingereicht.

Durch Anordnung vom 26. Juni 2019 hat der Gerichtshof nach Anhörung der referierenden Richter T. Giet und R. Leysen beschlossen, dass die Rechtssache verhandlungsreif ist, dass keine Sitzung abgehalten wird, außer wenn eine Partei innerhalb von sieben Tagen nach Erhalt der Notifizierung dieser Anordnung einen Antrag auf Anhörung eingereicht hat, und dass vorbehaltlich eines solchen Antrags die Verhandlung am 17. Juli 2019 geschlossen und die Rechtssache zur Beratung gestellt wird.

Da keine Sitzung beantragt wurde, wurde die Rechtssache am 17. Juli 2019 zur Beratung gestellt.

Die Vorschriften des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, die sich auf das Verfahren und den Sprachengebrauch beziehen, wurden zur Anwendung gebracht.

## II. Rechtliche Würdigung

(...)

### *In Bezug auf das angefochtene Gesetz und dessen Kontext*

B.1. Die durch die VoG « Ligue des Droits de l'Homme » (nunmehr « Ligue des droits humains ») eingereichte Nichtigkeitsklage richtet sich gegen das Gesetz vom 25. Dezember 2016 « über die Verarbeitung von Passagierdaten » (nachstehend: Gesetz vom 25. Dezember 2016), das eine Verpflichtung für die Beförderungsunternehmen und Reiseunternehmen festlegt, die Daten zu Passagieren, die sogenannten « PNR-Daten » (*Passenger Name Record*), zu übermitteln.

B.2.1. Nach Artikel 2 setzt das Gesetz vom 25. Dezember 2016 drei europäische Richtlinien um.

B.2.2. Zunächst wird mit dem Gesetz vom 25. Dezember 2016 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 » (nachstehend: PNR-Richtlinie) umgesetzt.

Die PNR-Richtlinie sieht die Erhebung und Übermittlung der Fluggastdatensätze von Drittstaatsflügen durch die Fluggesellschaften zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität vor. Diese Richtlinie gilt für die Verarbeitung von PNR-Daten im Bereich des Luftverkehrs, gemäß ihrem Erwägungsgrund 33 schließt sie jedoch die Möglichkeit der Mitgliedstaaten nicht aus, den darin vorgesehenen PNR-Mechanismus nach ihrem jeweiligen nationalen Recht auf andere Beförderungsmittel oder auf andere Wirtschaftsteilnehmer als die Beförderungsunternehmen auszudehnen. Außerdem kann die PNR-Richtlinie gemäß ihrem Artikel 2 auch auf Flüge innerhalb der Europäischen Union angewandt werden.

B.2.3. Mit dem Gesetz vom 25. Dezember 2016 wird außerdem die Richtlinie 2004/82/EG des Rates vom 29. April 2004 « über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln » (nachstehend: API-Richtlinie) umgesetzt.

So regelt es die Verwendung von Passagierdaten für die in der Richtlinie 2004/82/EG vorgesehenen Zwecke, indem es den Inhalt des königlichen Erlasses vom 11. Dezember 2006 « über die Verpflichtung von Fluggesellschaften, Angaben über die beförderten Personen zu übermitteln » (nachstehend: königlicher Erlass vom 11. Dezember 2006) wiederaufnimmt.

B.2.4. Mit dem Gesetz vom 25. Dezember 2016 wird schließlich teilweise 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. Zweck dieser

Richtlinie ist die Vereinfachung und Harmonisierung der Verwaltungsverfahren im Seeverkehr durch die allgemeine Nutzung elektronischer Systeme für die Datenübermittlung und durch die Rationalisierung der Meldeformalitäten (Artikel 1 Absatz 1).

B.3.1. Das Gesetz vom 25. Dezember 2016 zielt darauf ab, « einen rechtlichen Rahmen zu schaffen, um es verschiedenen Sektoren der internationalen Personenbeförderung (Flug-, Schienen-, internationaler Straßen- und Seeverkehr) und Reiseunternehmen aufzuerlegen, ihre Passagierdaten an eine vom FÖD Inneres verwaltete Datenbank zu übermitteln (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 6):

« Le traitement des données de passagers, leur comparaison avec des banques de données et leur soumission à des critères prédéterminés sont nécessaires pour révéler ces modes opératoires, découvrir de nouvelles tendances et de nouveaux phénomènes, mais aussi déterminer les passagers à soumettre à un examen approfondi car ceux-ci, sur la base des résultats du traitement, peuvent être impliqués dans une infraction terroriste, dans des formes de criminalité grave, dans des atteintes à l'ordre public dans le cadre de la radicalisation violente et dans des activités pouvant menacer les intérêts fondamentaux de l'État.

[...]

Transposant la directive européenne relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, l'avant-projet de loi prend au maximum en compte les dispositions prévues au niveau européen. Cela est essentiel pour créer un mécanisme efficace pour le traitement des données relatives aux passagers, de manière à tendre vers une interopérabilité maximale entre les Unités d'information des passagers des États membres.

[...]

L'analyse des données des passagers sera exclusivement confiée à une Unité d'Information des Passagers (UIP) créée au sein du SPF Intérieur et notamment composée, placés sous l'autorité fonctionnelle d'un fonctionnaire dirigeant de l'UIP des membres détachés issus des services de police, de la Sûreté de l'État, du Service général de Renseignement et de Sécurité et des Douanes (en ce qui concerne les Douanes, le traitement des données de passagers est nécessaire à la recherche et à la poursuite de fraudes, comme prévu dans l'Annexe 2, point 7 de la Directive 2016/681) » (ebenda, SS. 5-6).

B.3.2. Das durch die PNR-Richtlinie eingeführte System zur Erhebung der Daten vervollständigt das durch die API-Richtlinie geschaffene System, da die PNR-Daten umfassender sind als die API-Daten:

« Les données API (*Advanced Passenger Information*) sont des données authentiques. Elles proviennent de documents authentiques (en[tre] autre[s] des cartes d'identités) et sont suffisamment précises pour identifier une personne. Il s'agit des données transmises dans le cadre du check-in et l'embarquement. Dans le cadre de la lutte contre le terrorisme et la criminalité grave, l'information qui est contenue dans les données API est suffisante pour identifier les terroristes et les criminels connus à l'aide de systèmes d'avertissement.

Les données PNR, c'est-à-dire les données de réservation, contiennent davantage d'éléments et sont plus rapidement disponibles que les données API. Ces éléments constituent un instrument très important pour la réalisation d'évaluations de risque concernant des personnes et l'établissement de liens entre des personnes connues et des personnes inconnues. De même pour les recherches ponctuelles, les données PNR représentent une plus-value importante » (ebenda, SS. 6-7).

B.3.3. Die Verpflichtung zur Übermittlung der Passagierdaten gilt « sowohl für internationale Flüge, für internationale Hochgeschwindigkeitszüge, für den internationalen Charterverkehr mit Reisebussen und den Seeverkehr aus und in die Europäische Union als auch für Beförderungen in und aus der Europäischen Union » (ebenda, S. 7) gemäß der in Artikel 2 der PNR-Richtlinie vorgesehenen Möglichkeit.

Außerdem ist die gesetzliche Verpflichtung zur Übermittlung der Passagierdaten im Einklang mit der von der PNR-Richtlinie gebotenen Möglichkeit, diese Verpflichtung auch anderen Wirtschaftsteilnehmern als Beförderungsunternehmen aufzuerlegen, nicht nur auf die in der PNR-Richtlinie genannten Beförderungsunternehmen, sondern auch auf Reiseunternehmen anwendbar (ebenda, S. 8).

#### *In Bezug auf den Umfang der Klage*

B.4.1. Der Gerichtshof muss die Tragweite der Nichtigkeitsklage auf der Grundlage des Inhalts der Klageschrift.

Der Gerichtshof kann nur ausdrücklich angefochtene Gesetzesbestimmungen für nichtig erklären, gegen die Klagegründe angeführt werden, sowie gegebenenfalls Bestimmungen, die nicht angefochten werden, jedoch untrennbar mit den für nichtig zu erklärenden Bestimmungen verbunden sind.

B.4.2. Die klagende Partei beantragt zwar mit ihrem ersten Klagegrund die Nichtigkeitserklärung des gesamten Gesetzes vom 25. Dezember 2016, aber aus der Begründung des Klagegrunds geht hervor, dass sich die Beschwerdegünde nur gegen Artikel 3 § 2, Artikel 4 Nr. 9 und 10, Artikel 7 bis 9, Artikel 12 bis 16, Artikel 18, Artikel 24 bis 27, Artikel 50 und Artikel 51 des Gesetzes vom 25. Dezember 2016 richten. Folglich ist die Nichtigkeitsklage nur in diesem Maße zulässig.

Der zweite, hilfsweise vorgebrachte Klagegrund richtet sich gegen Artikel 3 § 1, Artikel 8 § 2 und Kapitel 11 des Gesetzes vom 25. Dezember 2016, das die Artikel 28 bis 31 umfasst.

B.4.3. Sollte sich bei der genaueren Prüfung der Klagegründe herausstellen, dass nur bestimmte Teile der angefochtenen Bestimmungen bemängelt werden, wird die Prüfung gegebenenfalls auf diese Teile beschränkt.

B.5. Die angefochtenen Artikel bestimmen:

#### « 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 des Ausschusses für den Schutz des Privatlebens.

#### 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 4 - *Verpflichtungen der Beförderungsunternehmen und Reiseunternehmen*

[...]

Art. 7. § 1. Beförderungsunternehmen übermitteln die in Artikel 9 § 1 erwähnten Passagierdaten, über die sie verfügen, und vergewissern sich, dass die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, über die sie verfügen, vollständig, exakt und aktuell sind. Zu diesem Zweck überprüfen sie die Übereinstimmung zwischen den Reisedokumenten und der Identität des betreffenden Passagiers.

§ 2. Reiseunternehmen übermitteln die in Artikel 9 § 1 erwähnten Passagierdaten, über die sie verfügen, und vergewissern sich, dass die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, über die sie verfügen, vollständig, exakt und aktuell sind. Zu diesem Zweck treffen sie alle notwendigen Maßnahmen, um die Übereinstimmung zwischen den Reisedokumenten und der Identität des betreffenden Passagiers zu überprüfen.

§ 3. Der König bestimmt durch einen im Ministerrat beratenen Erlass pro Beförderungssektor und für die Reiseunternehmen die Modalitäten in Bezug auf die in den Paragraphen 1 und 2 erwähnte Verpflichtung.

#### 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 in Artikel 90ter § 2 Nr. 1bis, 1ter, 1quater, 1quinqües, 1octies, 4, 5, 6, 7, 7bis, 7ter, 8, 9, 10, 10bis, 10ter, 11, 13, 13bis, 14, 16, 17, 18, 19 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten,

2. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 196, was die Fälschung authentischer und öffentlicher Urkunden betrifft, 198, 199, 199bis, 207, 213, 375 und 505 des Strafgesetzbuches 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 in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen und in Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung erwähnten Straftaten.

§ 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 leitenden Beamten, dem ein Unterstützungsdienst beisteht und 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,
- f) Unterstützung der zuständigen Dienste bei der Ausübung ihrer Befugnisse innerhalb der PNR-Zentralstelle,

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

a) den im Gesetz vom 7. Dezember 1998 zur Organisation eines auf zwei Ebenen strukturierten integrierten Polizeidienstes erwähnten Polizeidiensten,

b) der im Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Staatssicherheit,

c) dem im Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Allgemeinen Nachrichten- und Sicherheitsdienst,

d) der Verwaltung Ermittlung und Fahndung und der Verwaltung Aufsicht, Kontrolle und Feststellung der im Erlass des Präsidenten des Direktionsausschusses vom 16. Oktober 2014 zur Schaffung neuer Dienste der Generalverwaltung Zoll und Akzisen erwähnten Generalverwaltung Zoll und Akzisen.

Während der Entsendung unterliegen die Mitglieder der zuständigen Dienste der funktionellen und hierarchischen Amtsgewalt des leitenden Beamten der PNR-Zentralstelle. Sie behalten jedoch das Statut ihres ursprünglichen Dienstes.

§ 2. Nach Absprache mit dem Datenschutzbeauftragten und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens schließen der leitende Beamte der PNR-Zentralstelle und die zuständigen Dienste das in Artikel 17 erwähnte Vereinbarungsprotokoll ab, um die Modalitäten der Datenübermittlung zu bestimmen. Das Protokoll sieht mindestens folgende Sicherheitsvorkehrungen vor:

- Modalitäten des Datenaustauschs,
- durch das Gesetz für die Datenverarbeitung festgelegte Höchstfristen,
- Benachrichtigung der PNR-Zentralstelle durch die zuständigen Dienste über die Folgemaßnahmen zu validierten Treffern.

§ 3. Gemäß den gesetzlichen Verpflichtungen jeden zuständigen Dienstes homologiert die Nationale Sicherheitsbehörde ein abgesichertes und verschlüsseltes Kommunikations- und Informationssystem im Hinblick auf den automatisierten Versand von Treffern.

§ 4. Der König bestimmt durch einen im Ministerrat beratenen Erlass und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens die Modalitäten der Zusammensetzung und Organisation der PNR-Zentralstelle, das Statut des leitenden Beamten und der Mitglieder der PNR-Zentralstelle sowie die Direktionen oder Abteilungen, die innerhalb der zuständigen Dienste mit der Verarbeitung der Passagierdaten beauftragt sind

## KAPITEL 8. - *Passagierdatenbank*

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

§ 2. Der leitende Beamte der PNR-Zentralstelle ist der für die Verarbeitung Verantwortliche der Passagierdatenbank im Sinne von Artikel 1 § 4 des Gesetzes über den Schutz des Privatlebens.

§ 3. Die in Artikel 10 beziehungsweise 12 des Gesetzes über den Schutz des Privatlebens vorgesehenen Zugriffs- und Berichtigungsrechte in Bezug auf die Passagierdaten werden unmittelbar bei dem Datenschutzbeauftragten ausgeübt.

In Abweichung von Absatz 1 werden diese Rechte beim Ausschuss für den Schutz des Privatlebens ausgeübt, was die in den Artikeln 24 bis 27 erwähnten Treffer und Ergebnisse gezielter Recherchen betrifft.

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

Art. 16. Im Rahmen der in Artikel 8 § 1 erwähnten Zwecke ist die Passagierdatenbank der PNR-Zentralstelle direkt zugänglich für die in den Artikeln 24 bis 27 erwähnten Verarbeitungen gemäß den Bestimmungen von Kapitel 9.

[...]

#### 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.

§ 2. Im Rahmen der Zwecke, die in Artikel 8 § 1 Nr. 1, 4 und 5 erwähnt sind oder sich auf Bedrohungen beziehen, die in den Artikeln 8 Nr. 1 Buchstabe *a)*, *b)*, *c)*, *d)*, *f)*, *g)* und 11 § 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste aufgeführt sind, beruht die Vorabüberprüfung der Passagiere auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und:

1. den Datenbanken, die von den zuständigen Diensten verwaltet werden oder die ihnen im Rahmen ihrer Aufträge unmittelbar zur Verfügung stehen oder zugänglich sind, oder Personenlisten, die von den zuständigen Diensten im Rahmen ihrer Aufträge erstellt werden,

2. den Überprüfungskriterien, die von der PNR-Zentralstelle im Voraus festgelegt sind und in Artikel 25 erwähnt sind.

§ 3. Im Rahmen der in Artikel 8 § 1 Nr. 3 erwähnten Zwecke beruht die Vorabüberprüfung der Passagiere auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und den in § 2 Nr. 1 erwähnten Datenbanken.

§ 4. Der Treffer wird innerhalb von vierundzwanzig Stunden nach Eingang der automatisierten Mitteilung des Treffers von der PNR-Zentralstelle validiert.

§ 5. Ab dieser Validierung sorgt der zuständige Dienst, von dem der Treffer herkommt, schnellstmöglich für die weitere Bearbeitung.

Art. 25. § 1. Die Passagierdaten können von der PNR-Zentralstelle zwecks Aktualisierung der Kriterien oder Aufstellung neuer Kriterien benutzt werden, die dazu bestimmt sind, bei den in Artikel 24 § 2 Nr. 2 erwähnten Vorabüberprüfungen der Passagiere Einzelpersonen ins Visier zu nehmen.

§ 2. Die Überprüfung der Passagiere vor ihrer Ankunft, ihrer Durchreise oder ihrer Abreise anhand im Voraus festgelegter Kriterien erfolgt in nichtdiskriminierender 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.

Art. 26. § 1. Für den in Artikel 8 § 1 Nr. 3 erwähnten Zweck sind nur die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, die sich auf die Person(en) beziehen, für die sich ein Treffer ergeben hat, zugänglich.

§ 2. Für den Zweck, der in Artikel 8 § 1 Nr. 1, 4 und 5 erwähnt ist oder sich auf die Bedrohungen bezieht, die in Artikel 8 Nr. 1 Buchstabe a), b), c), d), f), g) und 11 § 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste aufgeführt sind, sind alle in Artikel 9 erwähnten Passagierdaten zugänglich.

## *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<sup>septies</sup> des Strafprozessgesetzbuches oder in Artikel 16/3 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste 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.

§ 2. Es findet Anwendung unbeschadet der Verpflichtungen, die den mit der Grenzkontrolle beauftragten Polizeidiensten und dem Ausländeramt obliegen, personenbezogene Daten oder Informationen aufgrund von Gesetzes- oder Verordnungsbestimmungen zu übermitteln.

Art. 29. § 1. Die Passagierdaten werden den mit der Grenzkontrolle beauftragten Polizeidiensten und dem Ausländeramt innerhalb der im vorliegenden Artikel vorgesehenen Grenzen zu den in Artikel 28 § 1 erwähnten Zwecken übermittelt, damit sie ihre gesetzlichen Aufträge ausführen können.

§ 2. Nur die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten 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 Polizeidiensten, die mit der Kontrolle an den Außengrenzen Belgiens beauftragt sind, 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. Wenn das Ausländeramt die in § 2 erwähnten Passagierdaten für die Ausführung seiner gesetzlichen Aufträge benötigt, werden sie ihm 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.

Wenn der Zugriff auf die in § 2 erwähnten 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.

Das Ausländeramt übermittelt dem Ausschuss für den Schutz des Privatlebens monatlich einen Bericht über die Anwendung von Absatz 2.

Der König bestimmt durch einen im Ministerrat beratenen Erlass nach Stellungnahme des Ausschusses für den Schutz des Privatlebens die in Absatz 2 erwähnten Zugriffsbedingungen.

Art. 30. § 1. Die technischen Sicherungs- und Zugriffsmodalitäten sowie die Modalitäten der Übermittlung der Passagierdaten an die mit der Grenzkontrolle beauftragten Polizeidienste und an das Ausländeramt werden in einem Protokoll dargelegt, das in Absprache mit dem Datenschutzbeauftragten und nach Stellungnahme des Ausschusses für

den Schutz des Privatlebens zwischen dem leitenden Beamten der PNR-Zentralstelle einerseits und dem Generalkommissar der föderalen Polizei und dem leitenden Beamten des Ausländeramtes andererseits für ihren jeweiligen Bereich abgeschlossen wird.

§ 2. Diese Modalitäten beziehen sich mindestens auf:

1. den Bedarf des Ausländeramtes, die Daten zu kennen,
2. die Kategorien von Personalmitgliedern, die auf der Grundlage der Ausführung ihrer Aufträge unmittelbaren Zugriff auf die übermittelten Daten haben,
3. die Pflicht zur Wahrung des Berufsgeheimnisses durch alle Personen, die die Passagierdaten unmittelbar oder mittelbar zur Kenntnis nehmen,
4. die Sicherheitsmaßnahmen in Zusammenhang mit 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 § 2 erwähnten Passagierdaten, die sie gemäß Artikel 7 übermitteln.

[...]

## KAPITEL 15. - *Abänderungsbestimmungen*

### *Abschnitt 1. - Abänderung des Strafprozessgesetzbuches*

Art. 50. In das Strafprozessgesetzbuch wird ein Artikel 46<sup>septies</sup> mit folgendem Wortlaut eingefügt:

‘ Art. 46<sup>septies</sup>. 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.

Die Begründung spiegelt die Verhältnismäßigkeit unter Berücksichtigung des Privatlebens und die Subsidiarität gegenüber jeder anderen Ermittlungsaufgabe wider.

Die Maßnahme kann eine Gesamtheit von Daten in Bezug auf eine spezifische Ermittlung betreffen. In diesem Fall bestimmt der Prokurator des Königs die Dauer der Maßnahme, die einen Monat ab dem Beschluss nicht überschreiten darf, unbeschadet einer Erneuerung.

In Fällen äußerster Dringlichkeit kann jeder Gerichtspolizeioffizier mit der mündlichen und vorherigen Zustimmung des Prokurators des Königs durch einen mit Gründen versehenen schriftlichen Beschluss den leitenden Beamten der PNR-Zentralstelle auffordern, die Passagierdaten mitzuteilen. Der Gerichtspolizeioffizier teilt dem Prokurator des Königs

diesen mit Gründen versehenen schriftlichen Beschluss sowie die erhaltenen Informationen binnen vierundzwanzig Stunden mit und begründet außerdem die äußerste Dringlichkeit '.

*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.

§ 2. Der in § 1 erwähnte Beschluss wird von einem Dienstleiter gefasst und der in Kapitel 7 des vorerwähnten Gesetzes erwähnten PNR-Zentralstelle schriftlich übermittelt. Der Beschluss wird zusammen mit seiner Begründung dem Ständigen Ausschuss N notifiziert.

Der Ständige Ausschuss N verbietet den Nachrichten- und Sicherheitsdiensten, die gesammelten Daten unter Bedingungen zu benutzen, die die gesetzlichen Bedingungen nicht einhalten.

Der Beschluss kann eine Gesamtheit von Daten in Bezug auf eine spezifische nachrichtendienstliche Untersuchung betreffen. In diesem Fall wird dem Ständigen Ausschuss N einmal pro Monat die Liste der Abfragen der Passagierdaten übermittelt. ’ ».

*In Bezug auf das Inkrafttreten und den Anwendungsbereich des Gesetzes vom 25. Dezember 2016*

B.6. Nach Artikel 54 des Gesetzes vom 25. Dezember 2016 bestimmt der König durch einen im Ministerrat beratenen Erlass pro Beförderungssektor und für die Reiseunternehmen das Datum des Inkrafttretens dieses Gesetzes.

B.7. Im königlichen Erlass vom 18. Juli 2017 « zur Ausführung des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten und zur Festlegung der Pflichten der Fluggesellschaften » (nachstehend: königlicher Erlass vom 18. Juli 2017) sind insbesondere die Pflichten der Fluggesellschaften und die Übermittlungsmodalitäten der Passagierdaten festgelegt.

Aufgrund von Artikel 12 des königlichen Erlasses vom 18. Juli 2017 ist das Gesetz vom 25. Dezember 2016 in Bezug auf die Fluggesellschaften am selben Tag wie dieser königliche Erlass, das heißt am 7. August 2017, in Kraft getreten.

B.8. Ebenso legt der königliche Erlass vom 3. Februar 2019 « zur Ausführung des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten und zur Festlegung der Pflichten der HST-Beförderungsunternehmen und der HST-Fahrkartenverkäufer » die Pflichten der HST-Beförderungsunternehmen (Hochgeschwindigkeitszug - grenzüberschreitender Personenverkehrsdienst auf der Schiene) und der HST-Fahrkartenverkäufer sowie die Übermittlungsmodalitäten der Passagierdaten fest.

Aufgrund von Artikel 10 des vorerwähnten königlichen Erlasses vom 3. Februar 2019 ist das Gesetz vom 25. Dezember 2016 in Bezug auf die HST-Beförderungsunternehmen und die HST-Fahrkartenverkäufer am selben Tag wie dieser königliche Erlass, das heißt am 22. Februar 2019, in Kraft getreten.

B.9. Schließlich legt der königliche Erlass vom 3. Februar 2019 « zur Ausführung des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten und zur Festlegung der Pflichten der Busunternehmen » die Pflichten der Busunternehmen sowie die Übermittlungsmodalitäten der Passagierdaten fest.

Aufgrund von Artikel 10 des vorerwähnten königlichen Erlasses vom 3. Februar 2019 ist das Gesetz vom 25. Dezember 2016 in Bezug auf die Busunternehmen am selben Tag wie dieser königliche Erlass, das heißt am 22. Februar 2019, in Kraft getreten.

B.10. Aus dem Vorstehenden ergibt sich, dass das Gesetz vom 25. Dezember 2016 in Bezug auf (1) die Fluggesellschaften, (2) die HST-Beförderungsunternehmen und die HST-Fahrkartenverkäufer und (3) die Busunternehmen in Kraft ist.

*In Bezug auf die Änderungen des Gesetzes vom 25. Dezember 2016*

B.11.1. Artikel 15 § 3 des Gesetzes vom 25. Dezember 2016 wurde durch Artikel 280 Absatz 4 des Gesetzes vom 30. Juli 2018 « über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten » (nachstehend: Gesetz vom 30. Juli 2018) aufgehoben.

Gemäß Artikel 281 Absatz 1 des Gesetzes vom 30. Juli 2018 ist diese Aufhebung am Tag der Veröffentlichung des Gesetzes vom 30. Juli 2018 im *Belgischen Staatsblatt*, das heißt am 5. September 2018, in Kraft getreten.

B.11.2. In den Vorarbeiten zum Gesetz vom 30. Juli 2018 ist bezüglich der Aufhebung von Artikel 15 § 3 des Gesetzes vom 25. Dezember 2016 erläutert:

« Dans le dernier alinéa le système d'accès direct et indirect des personnes concernées à leurs données prévu par l'article 15 de la loi PNR est supprimé. En effet, ce système ne convenait pas à la nature confidentielle des données traitées, et souffre d'une faille. Le caractère binaire de ce système aurait pu permettre à un passager de savoir, en fonction de l'entité auprès de laquelle il aurait pu exercer l'accès à ses données, si celles-ci ont fait l'objet d'une correspondance positive ou d'une recherche ponctuelle, et ainsi savoir s'il était recherché ou suivi par les services compétents. Le système susmentionné ainsi supprimé, ce sont les dispositions présentes dans la loi relative à la protection à l'égard des données à caractère personnel qui s'appliquent et qui prévoient un accès direct ou indirect en fonction du Titre de la présente loi qui s'applique. Cela permet également de répondre au point 247 de l'avis de la Commission vie privée qui s'interroge sur la conformité d'un tel système avec les dispositions de la présente loi » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3126/001, SS. 254-255).

B.11.3. Gegen Artikel 280 Absatz 4 des Gesetzes vom 30. Juli 2018 ist keinerlei Klage auf Nichtigkeitserklärung erhoben worden.

Daraus ergibt sich, dass die vorliegende Nichtigkeitsklage endgültig gegenstandslos geworden ist, insofern sie sich auf Artikel 15 § 3 des Gesetzes vom 25. Dezember 2016 bezieht.

B.11.4. Das Gesetz vom 30. Juli 2018 legt außerdem den Rahmen für die Verarbeitung von personenbezogenen Daten, insbesondere im Rahmen der in Artikel 8 des Gesetzes vom 25. Dezember 2016 aufgezählten Zwecke, fest.

B.11.5. In den Vorarbeiten zu dem Gesetz vom 30. Juli 2018 wurde diesbezüglich ausgeführt:

« Les traitements en vue de l'amélioration des contrôles de personnes aux frontières extérieures et en vue de lutter contre l'immigration illégale, visés à l'article 8, § 2, de la loi précitée du 25 décembre 2016, qui constitue une transposition de la Directive API, sont classés sous le titre 1er de la présente loi.

Les traitements dans le cadre des finalités visées à l'article 8, § 1er, 1°, 2°, 3° et 5°, de la loi précitée du 25 décembre 2016 sont classés sous le titre 2 puisqu'il s'agit de traitements de données à caractère personnel (données des passagers) effectués par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Les traitements dans le cadre de la finalité visée à l'article 8, § 1er, 4°, de la loi précitée du 25 décembre 2016 sont classés sous le titre 3 puisqu'il s'agit de traitements de données à caractère personnel (données des passagers) dans le cadre des missions des services de renseignement et de sécurité visés aux articles 7 et 11 de la loi du 30 novembre 1998.

La loi du 25 décembre 2016 précitée contient plusieurs dispositions concernant la protection des données telles que la désignation d'un délégué à la protection des données, la prévision d'une validation manuelle ou encore l'interdiction de traiter des données sensibles. Certains points déjà repris dans la loi du 25 décembre 2016 ne doivent par conséquent plus être repris dans la présente loi » (ebenda, SS. 188-189).

B.11.6. Daraus ergibt sich, dass der Gerichtshof zur Beurteilung der Tragweite des angefochtenen Artikels 8 des Gesetzes vom 25. Dezember 2016 das Gesetz vom 30. Juli 2018 berücksichtigen muss.

B.12.1. Durch die Artikel 62 bis 70 des Gesetzes vom 15. Juli 2018 « zur Festlegung verschiedener Bestimmungen im Bereich Inneres » (nachstehend: Gesetz vom 15. Juli 2018), veröffentlicht im *Belgischen Staatsblatt* vom 25. September 2018, wurde das Gesetz vom 25. Dezember 2016 ebenfalls abgeändert.

Die Artikel 62 bis 68 ändern mehrere der angefochtenen Artikel des Gesetzes vom 25. Dezember 2016 wie folgt ab:

« Art. 62. Artikel 8 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten wird wie folgt abgeändert:

1. Paragraph 1 Nr. 1 wird wie folgt ersetzt:

‘ 1. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 90ter § 2 Nr. 2, 3, 7, 8, 11, 14, 17 bis 20, 22, 24 bis 28, 30, 32, 33, 34, 36 bis 39, 43 bis 45 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten, ’.

2. Paragraph 1 Nr. 5 wird wie folgt ersetzt:

‘ 5. Ermittlung und Verfolgung der Straftaten, erwähnt in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen, in Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung, in Artikel 5 des Gesetzes vom 15. Mai 2007 über die Ahndung der Nachahmung und der Piraterie von geistigen Eigentumsrechten, in Artikel 26 des Dekretes der Deutschsprachigen Gemeinschaft vom 20. Februar 2017 zum Schutz des beweglichen Kulturgutes von außerordentlicher Bedeutung sowie in Artikel 24 des Dekretes der Flämischen Gemeinschaft vom 24. Januar 2003 ‘ houdende bescherming van het roerend cultureel erfgoed van uitzonderlijk belang ’ (Schutz des beweglichen Kulturerbes von außerordentlicher Bedeutung), im Ministeriellen Erlass vom 7. Februar 2012 zur Einführung einer Lizenzpflicht für die Einfuhr von Waren, deren Ursprung oder Herkunft Syrien ist, abgeändert durch den Ministeriellen Erlass vom 1. Juli 2014, im Ministeriellen Erlass vom 23. März 2004 zur Aufhebung des Ministeriellen Erlasses vom 17. Januar 2003 zur Einführung der Pflicht, für die Ein-, Aus- und Durchfuhr von Waren, deren Ursprung, Herkunft oder Bestimmung der Irak ist, über eine vorherige Ermächtigung zu verfügen und für die Ein-, Aus- und Durchfuhr bestimmter Waren, deren Ursprung, Herkunft oder Bestimmung der Irak ist, über eine Lizenz zu verfügen, sowie Ermittlung der Verstöße, erwähnt in Artikel 5 des Gesetzes vom 28. Juli 1981 zur Billigung des Übereinkommens über den internationalen Handel mit gefährdeten Arten freilebender Tiere und Pflanzen und der Anlagen, abgeschlossen in Washington am 3. März 1973, und der Änderung des Übereinkommens, angenommen in Bonn am 22. Juni 1979 ’.

Art. 63. Artikel 14 desselben Gesetzes wird wie folgt abgeändert:

1. In Paragraph 1 Nr. 2 wird Buchstabe d) wie folgt ersetzt:

‘ d) den Enquetendiensten, Ermittlungsdiensten und Diensten der Generalverwaltung Zoll und Akzisen, die mit der Aufsicht, Kontrolle und Feststellung beauftragt sind. ’

2. Paragraph 4 wird wie folgt ersetzt:

‘ § 4. Der König bestimmt durch einen im Ministerrat beratenen Erlass und nach Stellungnahme der für die Aufsicht über die Verarbeitung personenbezogener Daten zuständigen Behörde die Modalitäten der Zusammensetzung und Organisation der PNR-Zentralstelle sowie das Statut des leitenden Beamten und der Mitglieder der PNR-Zentralstelle. ’

Art. 64. In Artikel 15 § 2 desselben Gesetzes wird das Wort ‘ Passagierdatenbank ’ durch das Wort ‘ Passagierdaten ’ ersetzt.

Art. 65. Artikel 17 desselben Gesetzes wird wie folgt ersetzt:

‘ Art. 17. Nach Absprache mit dem Datenschutzbeauftragten und nach Stellungnahme der für die Aufsicht über die Verarbeitung personenbezogener Daten zuständigen Behörde schließen der leitende Beamte der PNR-Zentralstelle und die zuständigen Dienste ein Vereinbarungsprotokoll ab, das der Umsetzung der technischen Sicherungs- und Zugriffsmodalitäten dient.

Mit diesem Protokoll:

1. wird gewährleistet, dass die verarbeiteten Daten denselben Sicherheits- und Schutzanforderungen unterliegen,

2. wird sichergestellt, dass die notwendigen Schutzmaßnahmen getroffen werden, damit:

- alle Verpflichtungen erfüllt werden, die sich aus den Regeln in Bezug auf die im vorliegenden Gesetz festgelegten Fristen, die Aufbewahrung und Vernichtung der in der Passagierdatenbank aufbewahrten Daten ergeben,

- die Daten für alle Personen, die nicht zum Zugriff darauf befugt sind, gesperrt werden,

- gewährleistet wird, dass die von den Mitgliedern der PNR-Zentralstelle vorgenommenen Verarbeitungen mit dem Gesetz vom 11. Dezember 1998 über die Klassifizierung und die Sicherheitsermächtigungen, -bescheinigungen und -stellungen in Übereinstimmung stehen,

3. wird vorgesehen, dass den Personen, die auf die Passagierdaten zugreifen können, Berechtigungen zum Zugriff auf die Passagierdaten erteilt und gemeinsame und spezifische Benutzerprofile zugewiesen werden,

4. wird gewährleistet, dass die Daten im Hoheitsgebiet der Europäischen Union aufbewahrt werden. ’.

Art. 66. In Artikel 24 § 2 desselben Gesetzes wird der einleitende Satz von Absatz 1 wie folgt ersetzt:

‘ Im Rahmen der Zwecke, die in Artikel 8 § 1 Nr. 1, 2, 4 und 5 erwähnt sind oder sich auf Bedrohungen beziehen, die in den Artikeln 8 Nr. 1 Buchstabe *a)*, *b)*, *c)*, *d)*, *f)*, *g)* und 11 § 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste aufgeführt sind, beruht die Vorabüberprüfung der Passagiere auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und: ’.

Art. 67. In Artikel 26 desselben Gesetzes wird § 2 wie folgt ersetzt:

‘ § 2. Für den Zweck, der in Artikel 8 § 1 Nr. 1, 2, 4 und 5 erwähnt ist oder sich auf die Bedrohungen bezieht, die in Artikel 8 Nr. 1 Buchstabe *a)*, *b)*, *c)*, *d)*, *f)*, *g)* und 11 § 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste aufgeführt sind, sind alle in Artikel 9 erwähnten Passagierdaten zugänglich. ’.

Art. 68. In Artikel 31 desselben Gesetzes werden die Wörter ‘ Artikel 9 § 2 ’ durch die Wörter ‘ Artikel 9 § 1 Nr. 18 ’ ersetzt. ’ ».

B.12.2. Diese Abänderungen sind am 5. Oktober 2018 in Kraft getreten.

B.12.3. Der Gerichtshof hat zu prüfen, inwieweit diese Abänderungen sich auf den Klagegegenstand auswirken.

B.12.4.1. Artikel 62 des Gesetzes vom 15. Juli 2018 ersetzt Artikel 8 § 1 Nrn. 1 und 5 des Gesetzes vom 25. Dezember 2016.

Artikel 63 des Gesetzes vom 15. Juli 2018 ersetzt Artikel 14 § 1, Nr. 2, Buchstabe *d*) und § 4 des Gesetzes vom 25. Dezember 2016.

Artikel 65 des Gesetzes vom 15. Juli 2018 ersetzt Artikel 17 des Gesetzes vom 25. Dezember 2016.

Artikel 66 des Gesetzes vom 15. Juli 2018 ersetzt Artikel 24 § 2 Absatz 1 einleitender Satz des Gesetzes vom 25. Dezember 2016.

Artikel 67 des Gesetzes vom 15. Juli 2018 ersetzt Artikel 26 § 2 des Gesetzes vom 25. Dezember 2016.

B.12.4.2. Wegen dieser Abänderungen wird die Klage grundsätzlich gegenstandslos, insofern sie sich gegen Artikel 8 § 1 Nrn. 1 und 5, Artikel 14 § 1 Nr. 2 Buchstabe *d*) und § 4, Artikel 17, Artikel 24 § 2 Absatz 1 einleitender Satz und Artikel 26 § 2 des Gesetzes vom 25. Dezember 2016 richtet.

B.12.4.3. Gegen die vorerwähnten Artikel des Gesetzes vom 15. Juli 2018, mit denen das Gesetz vom 25. Dezember 2016 abgeändert wurde, ist keinerlei Klage auf Nichtigkeitsklärung erhoben worden.

B.12.4.4. Die vorliegende Klage richtet sich gegen die ursprüngliche Fassung des Gesetzes vom 25. Dezember 2016. Auch wenn Artikel 8 § 1 Nrn. 1 und 5, Artikel 14 § 1 Nr. 2 Buchstabe *d*) und § 4, Artikel 17, Artikel 24 § 2 Absatz 1 einleitender Satz und Artikel 26 § 2 des Gesetzes vom 25. Dezember 2016 durch die vorerwähnten Artikel des Gesetzes vom 15. Juli 2018 ersetzt wurden, hat die Nichtigkeitsklage, insofern sie gegen

Artikel 8 § 1 Nrn. 1 und 5, Artikel 14 § 1 Nr. 2 Buchstabe *d*) und § 4, Artikel 17, Artikel 24 § 2 Absatz 1 einleitender Satz und Artikel 26 § 2 des Gesetzes vom 25. Dezember 2016 gerichtet ist, weiterhin einen Gegenstand, sofern das Gesetz vom 15. Juli 2018 diese angefochtenen Artikel des Gesetzes vom 25. Dezember 2016 nicht wesentlich abändert.

Der Gerichtshof prüft folglich für jede dieser Bestimmungen und in Bezug auf jeden Beschwerdegund, in welchem Maße die Nichtigkeitsklage weiterhin einen Gegenstand hat.

B.12.5.1. Artikel 64 des Gesetzes vom 15. Juli 2018 ersetzt in Artikel 15 § 2 des Gesetzes vom 25. Dezember 2016 das Wort « Passagierdatenbank » durch das Wort « Passagierdaten ».

Artikel 68 des Gesetzes vom 15. Juli 2018 ersetzt in Artikel 31 des Gesetzes vom 25. Dezember 2016 die Wörter « Artikel 9 § 2 » durch die Wörter « Artikel 9 § 1 Nr. 18 ».

B.12.5.2. Diese Abänderungen betreffen nur technische Korrekturen der Artikel 15 § 2 und 31 des Gesetzes vom 25. Dezember 2016, ohne diese Bestimmungen zu ersetzen, sodass sie nicht als Abänderungen angesehen werden können, die sich auf den Gegenstand der vorliegenden Klage auswirken.

B.12.6. Im Übrigen berücksichtigt der Gerichtshof die vorerwähnten Abänderungen, insbesondere um die Tragweite der angefochtenen Bestimmungen zu bestimmen.

B.13.1. Durch die Artikel 2 bis 11 des Gesetzes vom 2. Mai 2019 « zur Abänderung verschiedener Bestimmungen über die Verarbeitung von Passagierdaten » (nachstehend: Gesetz vom 2. Mai 2019), veröffentlicht im *Belgischen Staatsblatt* vom 24. Mai 2019, wurde das Gesetz vom 25. Dezember 2016 ebenfalls abgeändert.

Die Artikel 2 und 4 bis 7 des Gesetzes vom 2. Mai 2019 ändern mehrere der angefochtenen Artikel des Gesetzes vom 25. Dezember 2016 wie folgt ab:

« Art. 2. Aux articles 3, § 2, 14, § 2, 15, § 4, 23, § 2, alinéa 2, 29, § 4, 30, § 1er, 44, § 2, 7° et 9°, et § 4, de la loi du 25 décembre 2016 relative au traitement des données des passagers, les mots ‘ la Commission de la protection de la vie privée ’ sont chaque fois

remplacés par les mots ‘ l’autorité compétente de contrôle des traitements de données à caractère personnel ’ ».

« Art. 4. À l’article 15 de la même loi, modifié par les lois du 15 juillet 2018 et du 30 juillet 2018, les modifications suivantes sont apportées :

1° Aux paragraphes 2 et 4, les mots ‘ loi relative à la protection de la vie privée ’ sont chaque fois remplacés par les mots ‘ loi relative à la protection des données ’

2° Au paragraphe 2, les mots ‘ l’article 1er, § 4 ’ sont remplacés par ‘ l’article 26, 8° ’.

Art. 5. L’article 24, § 2, de la même loi, modifié par la loi du 15 juillet 2018 est complété par un alinéa rédigé comme suit :

‘ Dans le cadre de la finalité visée à l’alinéa 1er pour laquelle la correspondance positive a été obtenue, l’exploitation des données des passagers dans le cadre de l’évaluation préalable repose, pendant une période de vingt-quatre heures à partir de la validation visée au paragraphe 4, sur :

1° les données des passagers pertinentes du même transport que celui dont est issu la correspondance positive, pour autant que ces données soient corrélées avec les données reprises dans la correspondance positive.

2° les autres données des passagers enregistrées dans la banque de données des passagers de la personne ayant fait l’objet de la correspondance positive, sans préjudice de l’application des articles 19 et 20 ’.

Art. 6. L’article 27 de la même loi est remplacé par ce qui suit :

‘ Art. 27. Les données des passagers sont exploitées en vue de procéder à des recherches ponctuelles aux fins visées à l’article 8, § 1er, 1°, 2°, 4° et 5°, et aux conditions prévues à l’article 46septies du Code d’instruction criminelle, à l’article 16/3 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ou à l’article 281, § 4 de la loi générale sur les douanes et accises, coordonnée le 18 juillet 1977 ’.

Art. 7. À l’article 29 de la même loi, les modifications suivantes sont apportées :

1° au paragraphe 1er, les mots ‘ chargés du contrôle aux frontières ’ sont remplacés par les mots ‘ visés à l’article 14, § 1er, 2°, a) ’;

2° au paragraphe 3, les mots ‘ chargés du contrôle aux frontières extérieures de la Belgique ’ sont remplacés par ‘ visés à l’article 14, § 1er, 2°, a) ’».

B.13.2. Diese Abänderungen sind am 3. Juni 2019 in Kraft getreten.

B.13.3. Wie in B.12.5.2 erwähnt, betreffen die Artikel 2, 4 und 7 des Gesetzes vom 2. Mai 2019 nur technische Korrekturen der Artikel 3 § 2, 14 § 2, 15 § 4, 29 und 30 § 1 des

Gesetzes vom 25. Dezember 2016, sodass sich diese Abänderungen nicht auf den Klagegegenstand auswirken.

B.13.4. Wie in B.12.4.4 erwähnt, hat die Nichtigkeitsklage – obgleich durch Artikel 6 des Gesetzes vom 2. Mai 2019 der angefochtene Artikel 27 des Gesetzes vom 25. Dezember 2016 ersetzt wird – insofern sie gegen diese Bestimmung gerichtet ist, weiterhin einen Gegenstand, sofern der Inhalt von Artikel 6 des Gesetzes vom 2. Mai 2019 mit der ursprünglichen Fassung dieses Artikels 27 identisch ist.

B.13.5. Im Übrigen berücksichtigt der Gerichtshof die Abänderung, die durch Artikel 5 des Gesetzes vom 2. Mai 2019 an Artikel 24 § 2 des Gesetzes vom 25. Dezember 2016 vorgenommen wurde, insbesondere um die Tragweite der angefochtenen Bestimmung zu bestimmen.

#### *Zur Hauptsache*

##### *In Bezug auf den ersten Klagegrund*

B.14. Der erste, hauptsächlich vorgebrachte Klagegrund ist abgeleitet aus einem Verstoß gegen Artikel 22 der Verfassung, gegebenenfalls in Verbindung mit Artikel 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 – nachstehend: DSGVO), mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union und mit Artikel 8 der Europäischen Menschenrechtskonvention.

Nach Auffassung der klagenden Partei verletzt das Gesetz vom 25. Dezember 2016 das Recht auf Achtung des Privatlebens und das Recht auf den Schutz personenbezogener Daten, die durch diese Bestimmungen gewährleistet werden. Das Gesetz vom 25. Dezember 2016 verstoße gegen das Legalitätsprinzip. Die systematische und unterschiedslose Erhebung, Übermittlung und Verarbeitung von PNR-Daten mit einem « Pre-Screening »-Verfahren seien

weder notwendig noch durch ein dem Gemeinwohl dienendes Ziel gerechtfertigt und mehrere eingeführte Maßnahmen seien unverhältnismäßig.

*Was die Bezugsnormen betrifft*

B.15.1. Artikel 22 der Verfassung bestimmt:

« Jeder hat ein Recht auf Achtung vor seinem Privat- und Familienleben, außer in den Fällen und unter den Bedingungen, die durch Gesetz festgelegt sind.

Das Gesetz, das Dekret oder die in Artikel 134 erwähnte Regel gewährleistet den Schutz dieses Rechtes ».

B.15.2. Artikel 8 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist ».

B.15.3. Der Verfassungsgeber hat eine möglichst weitgehende Übereinstimmung zwischen Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention angestrebt (*Parl. Dok.*, Kammer, 1992-1993, Nr. 997/5, S. 2).

Die Tragweite dieses Artikels 8 entspricht derjenigen der vorgenannten Verfassungsbestimmung, sodass die durch die beiden Bestimmungen gewährleisteten Garantien eine untrennbare Einheit bilden.

B.16.1. Das Recht auf Achtung des Privat- und Familienlebens, so wie es durch die vorerwähnten Verfassungs- und Vertragsbestimmungen gewährleistet wird, bezweckt im Wesentlichen, die Personen gegen Einmischungen in ihr Privatleben und Familienleben zu schützen.

Dieses Recht hat eine weitreichende Tragweite und umfasst unter anderem den Schutz der personenbezogenen Daten und der persönlichen Information. Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zeigt, dass, u. a. folgende personenbezogene Daten und Informationen unter den Schutzbereich dieses Rechts fallen: der Name, die Adresse, die professionellen Aktivitäten, die persönlichen Beziehungen, digitale Fingerabdrücke, Kamerabilder, Fotos, Kommunikationsdaten, DNA-Daten, gerichtliche Daten (Verurteilung oder Verdacht), finanzielle Daten und Informationen über Eigentum (siehe insbesondere EuGHMR, 26. März 1987, *Leander gegen Schweden*, §§ 47-48; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, §§ 66-68; 17. Dezember 2009, *B.B. gegen Frankreich*, § 57; 10. Februar 2011, *Dimitrov-Kazakov gegen Bulgarien*, §§ 29-31; 18. Oktober 2011, *Khelili gegen Schweiz*, §§ 55-57; 9. Oktober 2012, *Alkaya gegen Türkei*, § 29; 18. April 2013, *M.K. gegen Frankreich*, § 26; 18. September 2014, *Brunet gegen Frankreich*, § 31).

Der Gerichtshof ist ebenfalls der Auffassung, dass sich die Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbar natürliche Person betrifft (EuGH, Große Kammer, 9. November 2010, C-92/09 und C-93/09, *Volker und Markus Schecke und Eifert*, Randnr. 52; 16. Januar 2019, C-496/17, *Deutsche Post AG*, Randnr. 54).

B.16.2. Die durch Artikel 22 der Verfassung und durch Artikel 8 der Europäischen Menschenrechtskonvention gewährleisteten Rechte sind jedoch nicht absolut.

Sie schließen eine behördliche Einmischung in das Recht auf Achtung des Privatlebens nicht aus, verlangen jedoch, dass diese durch eine ausreichend präzise Gesetzesbestimmung erlaubt wird, einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entspricht und im Verhältnis zu der damit verfolgten gesetzmäßigen Zielsetzung steht. Diese Bestimmungen beinhalten außerdem die positive Verpflichtung für die Behörden, Maßnahmen zu ergreifen, die eine tatsächliche Achtung des Privatlebens gewährleisten, selbst in der Sphäre der gegenseitigen Beziehungen zwischen Einzelpersonen (EuGHMR, 27. Oktober 1994, *Kroon und andere gegen Niederlande*, § 31; Große Kammer, 12. November 2013, *Söderman gegen Schweden*, § 78).

B.17.1. Artikel 7 der Charta der Grundrechte der Europäischen Union bestimmt:

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

B.17.2. Artikel 8 der Charta der Grundrechte der Europäischen Union 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 ».

B.17.3. Artikel 52 Paragraph 1 der Charta der Grundrechte der Europäischen Union 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 notwendig sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen ».

B.17.4.1. Artikel 52 Paragraph 3 der Charta der Grundrechte der Europäischen Union bestimmt:

« So weit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt ».

B.17.4.2. Wenn die Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte garantierten Rechten entsprechen, « haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird ». Diese Bestimmung bringt die Bedeutung und Tragweite der in der Charta garantierten Rechte mit

den entsprechenden durch die Europäische Menschenrechtskonvention garantierten Rechten in Einklang.

In den Erläuterungen zur Charta (2007/C 303/02), die im *Amtsblatt* vom 14. Dezember 2007 veröffentlicht wurden, ist angegeben, dass unter den Artikeln, « die dieselbe Bedeutung und Tragweite wie die entsprechenden Artikel der Europäischen Menschenrechtskonvention haben », Artikel 7 der Charta Artikel 8 der Europäischen Menschenrechtskonvention entspricht.

Der Gerichtshof weist diesbezüglich darauf hin, dass « Artikel 7 der Charta, der das Recht auf Achtung des Privat- und Familienlebens betrifft, Rechte enthält, die den in Artikel 8 Absatz 1 der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (im Folgenden: EMRK) gewährleisteten Rechten entsprechen, und dass diesem Artikel 7 gemäß Artikel 52 Absatz 3 der Charta somit die gleiche Bedeutung und Tragweite beizumessen ist wie Artikel 8 Absatz 1 EMRK in seiner Auslegung durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte » (EuGH, 17. Dezember 2015, C-419/14, *WebMindLicenses Kft*, Randnrn. 70; 14. Februar 2019, C-345/17, *Buivids*, Randnr. 65).

B.17.4.3. Bezüglich Artikel 8 der Charta ist der Gerichtshof der Auffassung, dass, « wie aus Artikel 52 Absatz 3 Satz 2 der Charta hervorgeht, Artikel 52 Absatz 3 Satz 1 der Charta dem nicht [entgegensteht], dass das Recht der Union einen weiter gehenden Schutz gewährt als die EMRK. Zudem betrifft Artikel 8 der Charta ein anderes als das in ihrem Art. 7 verankerte Grundrecht, für das es in der EMRK keine Entsprechung gibt » (EuGH, Große Kammer, 21. Dezember 2016, C-203/15 und C-698/15, *Tele2 Sverige*, Randnr. 129).

B.17.4.4. Wie in B.16.1 erwähnt, ist der Gerichtshof ebenfalls der Auffassung, dass sich die Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft (EuGH, Große Kammer, 9. November 2010, C-92/09 und C-93/09, *Volker und Markus Schecke und Eifert*, Randnr. 52; 16. Januar 2019, C-496/17, *Deutsche Post AG*, Randnr. 54).

In seinem Gutachten 1/15 vom 26. Juli 2017 über den Entwurf eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von

Fluggastdatensätzen stellt der Gerichtshof fest, dass die PNR-Daten Informationen über bestimmte oder bestimmbare natürliche Personen enthalten und ihre Erhebung und Verarbeitung und der Zugang zu diesen Daten somit das in Artikel 7 der Charta garantierte Recht auf Achtung des Privatlebens und das durch Artikel 8 der Charta garantierte Recht auf den Schutz personenbezogener Daten berühren können (EuGH, Große Kammer, 26. Juli 2017, Gutachten 1/15, *PNR-Abkommen EU-Kanada*, Randnrn. 122-126).

Hinsichtlich der Einschränkungen, denen Artikel 7 und 8 der Charta unterliegen können, ist der Gerichtshof folgender Auffassung: « Die in den Art. 7 und 8 der Charta niedergelegten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden » (ebenda, Randnr. 136):

« 137. Insoweit ist auch darauf hinzuweisen, dass nach Artikel 8 Absatz 2 der Charta personenbezogene Daten nur ‘ für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage ’ verarbeitet werden dürfen.

138. Überdies muss nach Artikel 52 Absatz 1 der Charta jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten (Satz 1); 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 (Satz 2) » (ebenda).

B.18. Artikel 23 der DSGVO 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 oder 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 ».

B.19.1. Der Ministerrat macht hauptsächlich eine Einrede der Unzulässigkeit des ersten Klagegrunds geltend, insofern er aus einem Verstoß gegen Artikel 23 der DSGVO abgeleitet ist, der nicht auf das Gesetz vom 25. Dezember 2016 anwendbar sei.

#### B.19.2.1. Artikel 2 der DSGVO bestimmt:

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

2. Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten:

[...]

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.

[...] ».

#### B.19.2.2. Im Erwägungsgrund 12 der DSGVO heißt es:

« Artikel 16 Absatz 2 AEUV ermächtigt das Europäische Parlament und den Rat, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten zu erlassen ».

Der nach der DSGVO gebotene Schutz stützt sich auf Artikel 16 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (nachstehend: AEUV).

#### B.19.2.3. Der Erwägungsgrund 19 der DSGVO bestimmt:

« Der 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, sowie der freie Verkehr dieser Daten sind in einem eigenen Unionsrechtsakt geregelt. Deshalb sollte diese Verordnung auf Verarbeitungstätigkeiten dieser Art keine Anwendung finden. Personenbezogene Daten, die von Behörden nach dieser Verordnung verarbeitet werden, sollten jedoch, wenn sie zu den vorstehenden Zwecken verwendet werden, einem spezifischeren Unionsrechtsakt, nämlich der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates unterliegen. Die Mitgliedstaaten können die zuständigen Behörden im Sinne der Richtlinie (EU) 2016/680 mit Aufgaben betrauen, die nicht zwangsläufig für die 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, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich dieser Verordnung fällt,

als sie in den Anwendungsbereich des Unionsrechts fällt. In Bezug auf die Verarbeitung personenbezogener Daten durch diese Behörden für Zwecke, die in den Anwendungsbereich dieser Verordnung fallen, sollten die Mitgliedstaaten spezifischere Bestimmungen beibehalten oder einführen können, um die Anwendung der Vorschriften dieser Verordnung anzupassen. In den betreffenden Bestimmungen können die Auflagen für die Verarbeitung personenbezogener Daten durch diese zuständigen Behörden für jene anderen Zwecke präziser festgelegt werden, wobei der verfassungsmäßigen, organisatorischen und administrativen Struktur des betreffenden Mitgliedstaats Rechnung zu tragen ist. Soweit diese Verordnung für die Verarbeitung personenbezogener Daten durch private Stellen gilt, sollte sie vorsehen, dass die Mitgliedstaaten einige Pflichten und Rechte unter bestimmten Voraussetzungen mittels Rechtsvorschriften beschränken können, wenn diese Beschränkung in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz bestimmter wichtiger Interessen darstellt, wozu auch die öffentliche Sicherheit und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung zählen, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Dies ist beispielsweise im Rahmen der Bekämpfung der Geldwäsche oder der Arbeit kriminaltechnischer Labors von Bedeutung ».

Wie aus diesem Erwägungsgrund hervorgeht, fällt die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung grundsätzlich nicht unter die DSGVO, sondern unter die 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 » (nachstehend: Polizeirichtlinie).

B.19.2.4. Die Polizeirichtlinie legt in den Bereichen der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit spezifische Vorschriften 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.

Artikel 1 Absatz 1 der Polizeirichtlinie bestimmt:

« Diese Richtlinie enthält Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit ».

Artikel 9 Absätze 1 und 2 derselben Richtlinie bestimmt:

« 1. Personenbezogene Daten, die von zuständigen Behörden für die in Artikel 1 Absatz 1 genannten Zwecke erhoben werden, dürfen nicht für andere als die in Artikel 1 Absatz 1 genannten Zwecke verarbeitet werden, es sei denn, eine derartige Verarbeitung ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig. Wenn personenbezogene Daten für solche andere Zwecke verarbeitet werden, gilt die Verordnung (EU) 2016/679, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

2. Sind nach dem Recht der Mitgliedstaaten zuständige Behörden mit der Wahrnehmung von Aufgaben betraut, die sich nicht mit den für die in Artikel 1 Absatz 1 genannten Zwecke wahrgenommenen Aufgaben decken, gilt die Verordnung (EU) 2016/679 für die Verarbeitung zu diesen Zwecken — wozu auch im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke zählen —, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt ».

Im Erwägungsgrund 11 der Polizeirichtlinie ist diesbezüglich präzisiert, dass

« diesen Bereichen durch eine Richtlinie Rechnung getragen werden [sollte], die spezifische Vorschriften 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, enthält, wobei den Besonderheiten dieser Tätigkeiten Rechnung getragen wird. Diese zuständigen Behörden können nicht nur staatliche Stellen wie die Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden einschließen, sondern auch alle anderen Stellen oder Einrichtungen, denen durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für die Zwecke dieser Richtlinie übertragen wurde. Wenn solche Stellen oder Einrichtungen jedoch personenbezogene Daten zu anderen Zwecken als denen dieser Richtlinie verarbeiten, gilt die Verordnung (EU) 2016/679. Daher gilt die Verordnung (EU) 2016/679 in Fällen, in denen eine Stelle oder Einrichtung personenbezogene Daten zu anderen Zwecken erhebt und diese personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der sie unterliegt, weiterverarbeitet. Zum Beispiel speichern Finanzinstitute zum Zwecke der Ermittlung, Aufdeckung oder Verfolgung von Straftaten bestimmte personenbezogene Daten, die sie verarbeiten, und stellen sie nur den zuständigen nationalen Behörden in bestimmten Fällen und in Einklang mit dem Recht der Mitgliedstaaten zur Verfügung. Eine Stelle oder Einrichtung, die personenbezogene Daten im Rahmen des Anwendungsbereichs dieser Richtlinie für solche Behörden verarbeitet, sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments und durch die für Auftragsverarbeiter

nach dieser Richtlinie geltenden Bestimmungen gebunden sein, wobei die Anwendung der Verordnung (EU) 2016/679 in Bezug auf die Verarbeitung personenbezogener Daten, die der Auftragsverarbeiter außerhalb des Anwendungsbereichs dieser Richtlinie durchführt, unberührt bleibt ».

Im Erwägungsgrund 34 der Polizeirichtlinie ist weiter erläutert:

« [...] Wurden personenbezogene Daten ursprünglich von einer zuständigen Behörde für einen der Zwecke dieser Richtlinie erhoben, so sollte die Verordnung (EU) 2016/679 für die Verarbeitung dieser Daten für andere Zwecke als diejenigen dieser Richtlinie gelten, wenn eine solche Verarbeitung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist. Insbesondere sollte die Verordnung (EU) 2016/679 für die Übermittlung personenbezogener Daten für Zwecke gelten, die außerhalb des Anwendungsbereichs dieser Richtlinie liegen. Für die Verarbeitung personenbezogener Daten durch einen Empfänger, der keine zuständige Behörde im Sinne dieser Richtlinie ist oder nicht als solche handelt und gegenüber dem personenbezogene Daten von einer zuständigen Behörde rechtmäßig offengelegt werden, sollte die Verordnung (EU) 2016/679 gelten. [...] ».

B.19.3.1. Das Gesetz vom 25. Dezember 2016 regelt die Erhebung und Übermittlung von PNR-Daten, die Schaffung einer Passagierdatenbank, die von der « PNR-Zentralstelle » (nachstehend: PNR-Zentralstelle) verwaltet wird, die Verarbeitungszwecke dieser Datenbank und den Zugriff auf diese Datenbank.

Im Wesentlichen setzt das Gesetz vom 25. Dezember 2016 die PNR-Richtlinie um, aber es geht, wie in seinem Artikel 2 angegeben ist, inhaltlich auch über die Umsetzung dieser Richtlinie hinaus.

B.19.3.2. In seinem Gutachten 1/15 vom 26. Juli 2017 über den Entwurf eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen hat der Gerichtshof die Auffassung vertreten, dass die Bestimmungen dieses Abkommens zwei Ziele verfolgten, sodass das geplante Abkommen demnach « zwei Komponenten » habe. « Die eine betrifft die Erforderlichkeit der Gewährleistung der öffentlichen Sicherheit, die andere den Schutz personenbezogener Daten » (EuGH, Große Kammer, 26. Juli 2017, Gutachten 1/15, Randnr. 90). In Anbetracht dieser beiden Komponenten, die untrennbar miteinander verbunden sind und die beide als wesentlich anzusehen sind (ebenda, Randnr. 94) war der Gerichtshof der Meinung, dass der Beschluss des Rates über den Abschluss des geplanten Abkommens sowohl auf Artikel 16 Absatz 2 als auch auf Artikel 87 Absatz 2 Buchstabe a des AEUV gestützt werden müsste,

« sofern eine solche Kombination von Rechtsgrundlagen nicht [...] ausgeschlossen ist », weil sich die für die beiden Rechtsgrundlagen jeweils vorgesehenen Verfahren nicht miteinander vereinbaren lassen (ebenda, Randnr. 104).

Bestimmungen zur Regelung der Erhebung, Übermittlung und Verarbeitung von PNR-Daten können somit sowohl unter den Datenschutz (Artikel 16 des AEUV) als auch unter die polizeiliche Zusammenarbeit (Artikel 87 des AEUV) fallen.

B.19.3.3. Im Erwägungsgrund 5 der PNR-Richtlinie ist angegeben, 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 Erwägungsgrund 38 der PNR-Richtlinie gibt jedoch an, dass die Ziele der Richtlinie « die Übermittlung von PNR-Daten durch Fluggesellschaften und deren Verarbeitung zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität » sind, was bedeuten könnte, dass diese Ziele gegenüber dem Datenschutz überwiegen.

B.19.4. Der Gerichtshof stellt außerdem fest, dass Artikel 15 Absatz 1 des Gesetzes vom 30. Juli 2018 bestimmt:

« En application de l'article 23 du Règlement, les articles 12 à 22 et 34 du Règlement, ainsi que le principe de transparence du traitement visé à l'article 5 du Règlement, ne s'appliquent pas aux traitements de données à caractère personnel par l'Unité d'information des passagers, tels que visés au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers ».

Diese Bestimmung schließt somit nicht das gesamte Gesetz vom 25. Dezember 2016 aus dem Anwendungsbereich von Artikel 23 der DSGVO aus.

B.19.5. Um daher bestimmen zu können, ob die in Artikel 23 der DSGVO enthaltenen Anforderungen auf das Gesetz vom 25. Dezember 2016 anwendbar sind, mit dem – wie in B.2.2 erwähnt – unter anderem und hauptsächlich die PNR-Richtlinie umgesetzt wird, ist

folglich dem Gerichtshof der Europäischen Union die im Tenor wiedergegebene erste Vorabentscheidungsfrage zu stellen.

B.19.6. Im Übrigen steht die vom Ministerrat geltend gemachte Einrede der Unzulässigkeit mit der Tragweite des Gesetzes vom 25. Dezember 2016 im Zusammenhang, sodass sich ihre Prüfung mit der Prüfung der Sache selbst deckt.

*Was die Reihenfolge der Prüfung der Beschwerdegründe betrifft*

B.20. Aus der Prüfung des ersten Klagegrunds und der angefochtenen Bestimmungen geht hervor, dass die klagende Partei mehrere Aspekte des Gesetzes vom 25. Dezember 2016 bemängelt, die der Gerichtshof in der folgenden Reihenfolge prüft:

1. die Ausführungsmodalitäten des Gesetzes vom 25. Dezember 2016 (Artikel 3 § 2 und Artikel 7 § 3);
2. die Begriffe « Identitätsdokumente » und « Reisedokumente » (Artikel 7 §§ 1 und 2);
3. die fraglichen Daten (Artikel 4 Nr. 9 und Artikel 9);
4. den Begriff des « Passagiers » (Artikel 4 Nr. 10);
5. die Verarbeitungszwecke der PNR-Daten (Artikel 8);
6. die Verwaltung der Passagierdatenbank und die Verarbeitung der Daten im Rahmen der Vorabüberprüfung der Passagiere und der gezielten Recherchen (Artikel 12 bis 16 und 24 bis 27 und Artikel 50 und 51);
7. die Aufbewahrungsdauer der PNR-Daten (Artikel 18).

*1. Die Ausführungsmodalitäten des Gesetzes vom 25. Dezember 2016 (Artikel 3 § 2 und Artikel 7 § 3)*

B.21. Die klagende Partei ist zunächst der Auffassung, dass die Artikel 3 § 2 und 7 § 3 des Gesetzes vom 25. Dezember 2016 dadurch, dass sie es dem König überlassen, die wesentlichen Elemente zu bestimmen, gegen das Legalitätsprinzip verstoßen, das in den im Klagegrund erwähnten Bestimmungen gewährleistet ist.

B.22.1. Indem Artikel 22 der Verfassung dem zuständigen Gesetzgeber die Befugnis vorbehält, festzulegen, in welchen Fällen und unter welchen Bedingungen vom Recht auf Achtung des Privatlebens abgewichen werden kann, gewährleistet er einem jedem Rechtsunterworfenen, dass keinerlei Einmischung in dieses Recht erfolgen darf, außer aufgrund von Regeln, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

Eine Ermächtigung einer anderen Gewalt steht jedoch nicht im Widerspruch zum Legalitätsprinzip, sofern die Ermächtigung ausreichend präzise beschrieben ist und sich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Gesetzgeber festgelegt wurden.

B.22.2. Neben dem formalen Erfordernis der Legalität wird durch Artikel 22 der Verfassung ebenfalls die Verpflichtung auferlegt, dass die Einmischung in das Recht auf Achtung des Privatlebens deutlich und ausreichend präzise formuliert wird, damit es möglich ist, die Fälle vorherzusehen, in denen der Gesetzgeber eine solche Einmischung in das Recht auf Achtung des Privatlebens erlaubt.

Ebenso beinhaltet das Erfordernis der Vorhersehbarkeit, die das Gesetz erfüllen muss, damit davon ausgegangen wird, dass es Artikel 8 der Europäischen Menschenrechtskonvention entspricht, dass dessen Formulierung ausreichend präzise ist, damit jeder - gegebenenfalls mit einer geeigneten Beratung - unter den gegebenen Umständen in vernünftigem Maße die Folgen einer bestimmten Handlung vorhersehen kann (EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, § 55; Große Kammer, 17. Februar 2004, *Maestri gegen Italien*, § 30). Die Gesetzgebung muss einem jeden ausreichende Hinweise über die Umstände und die Bedingungen geben, unter denen die Behörden von Maßnahmen Gebrauch machen können, mit denen die durch die Konvention gewährleisteten

Rechte beeinträchtigt werden können (EuGHMR, Große Kammer, 12. Juni 2014, *Fernández Martínez gegen Spanien*, § 117).

B.22.3. Aus Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 22 der Verfassung ergibt sich somit, dass ausreichend präzise festgelegt werden muss, unter welchen Umständen eine Verarbeitung von personenbezogenen Daten erlaubt ist (EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, § 57; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, § 99).

Das erforderliche Maß der Präzision der betreffenden Gesetzgebung - in der nicht alle Fälle vorgesehen werden können - hängt, nach Darlegung des Europäischen Gerichtshofes für Menschenrechte, unter anderem von dem Bereich ab, der geregelt wird, sowie von der Anzahl und der Eigenschaft der Personen, an die sich das Gesetz richtet (EuGHMR, Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, §§ 95 und 96). So hat der Europäische Gerichtshof für Menschenrechte geurteilt, dass das Erfordernis der Vorhersehbarkeit in Bereichen, die die nationale Sicherheit betreffen, nicht die gleiche Tragweite haben kann wie in anderen Bereichen (EuGHMR, 26. März 1987, *Leander gegen Schweden*, § 51; 8. Juni 2006, *Lupsa gegen Rumänien*, § 33).

B.22.4. Der Gerichtshof vertritt ebenfalls die Auffassung, dass « das Erfordernis, dass jede Einschränkung der Ausübung der Grundrechte gesetzlich vorgesehen sein muss, bedeutet, dass die gesetzliche Grundlage für den Eingriff in die Grundrechte den Umfang der Einschränkung der Ausübung des betreffenden Rechts selbst festlegen muss » (EuGH, 17. Dezember 2015, C-419/14, *WebMindLicenses Kft*, Randnr. 81; Große Kammer, 26. Juli 2017, Gutachten 1/15, Randnr. 139).

B.23.1. Mit den angefochtenen Bestimmungen wird der König ermächtigt, durch einen im Ministerrat beratenen Erlass für jeden Beförderungssektor und für die Reiseunternehmen einerseits die zu übermittelnden Passagierdaten sowie ihre Übermittlungsmodalitäten nach Stellungnahme des Ausschusses für den Schutz des Privatlebens, nunmehr die Datenschutzbehörde, zu bestimmen (Artikel 3 § 2) und andererseits die Modalitäten in Bezug auf die Verpflichtung der Beförderungsunternehmen und Reiseunternehmen, sich zu vergewissern, dass diese Daten, über die sie verfügen, vollständig, exakt und aktuell sind,

indem sie die Übereinstimmung zwischen den Reisedokumenten und der Identität des betreffenden Passagiers überprüfen, zu bestimmen (Artikel 7 § 3).

Wie in B.17.4.4 erwähnt, stellen diese Maßnahmen eine Einmischung in das Recht auf Achtung des Privat- und Familienlebens dar.

B.23.2. Jeder Person muss hinreichend genau bekannt sein, in welchen Fällen und unter welchen Bedingungen ein Eingriff in ihr Privatleben, insbesondere durch die automatische Verarbeitung personenbezogener Daten, gestattet ist. Deshalb muss es jeder Person möglich sein, einen hinreichend deutlichen Einblick in die zu verarbeitenden Daten, in die von der Verarbeitung betroffenen Personen sowie die Bedingungen und die Ziele der Verarbeitung zu haben.

B.23.3. Es ist zu prüfen, ob unter Berücksichtigung der verschiedenen im Gesetz vom 25. Dezember 2016 enthaltenen Elemente jede von der Erhebung, Übermittlung und Verarbeitung der PNR-Daten betroffene Person hinreichend genau wissen kann, in welchen Fällen und unter welchen Bedingungen diese Erhebung, Übermittlung und Verarbeitung, gegebenenfalls gemäß den vom König bestimmten technischen Modalitäten, erlaubt sind.

B.24.1. Artikel 4 Nr. 9 des Gesetzes vom 25. Dezember 2016 definiert « PNR » als « 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 ».

Was die Daten des Eincheckstatus und des Anbordgehens betrifft, so sind die unter Artikel 9 § 1 Nr. 18 erwähnten erweiterten Passagierdaten (API-Daten –*Advanced Passenger Information*) erschöpfend in den 16 Nummern von Artikel 9 § 2 des Gesetzes vom 25. Dezember 2016 aufgezählt.

Was die Buchungsdaten betrifft, so enthalten die Passagierdaten (PNR-Daten –*Passenger Name Record*) höchstens die neunzehn Bestandteile, die in Artikel 9 § 1 des Gesetzes vom 25. Dezember 2016 erschöpfend aufgezählt sind, darunter die in Artikel 9 § 1 Nr. 18 erwähnten API-Daten.

B.24.2. Nach Artikel 5 des Gesetzes vom 25. Dezember 2016 werden die PNR-Daten von den Beförderungsunternehmen und Reiseunternehmen erhoben und übermittelt, damit sie in der in Artikel 15 erwähnten Passagierdatenbank, die von der im Föderalen Öffentlichen Dienst Inneres geschaffenen PNR-Zentralstelle verwaltet wird, gespeichert werden (Artikel 12 ff.). Die Passagiere werden darüber informiert, dass ihre Daten der PNR-Zentralstelle übermittelt werden und später zu den in Artikel 8 erwähnten Zwecken verarbeitet werden können (Artikel 6).

Die Zwecke der Verarbeitung der PNR-Daten sind in Artikel 8 des Gesetzes vom 25. Dezember 2016 aufgelistet: Es handelt sich einerseits um die Ermittlung und Verfolgung von Straftaten (Artikel 8 § 1) und andererseits unter den in Kapitel 11 erwähnten Bedingungen um die Verbesserung der Personenkontrolle an den Außengrenzen und die Bekämpfung der illegalen Einwanderung (Artikel 8 § 2).

Im Rahmen der in Artikel 8 § 1 erwähnten Zwecke sieht Artikel 16 des Gesetzes vom 25. Dezember 2016 vor, dass die Passagierdatenbank der PNR-Zentralstelle für die in den Artikeln 24 bis 27 erwähnten Verarbeitungen gemäß den Bestimmungen in Kapitel 9 direkt zugänglich ist.

Im Rahmen der in Artikel 8 § 2 erwähnten Zwecke werden nur die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten (API-Daten) in Bezug auf die in Artikel 29 § 2 des Gesetzes vom 25. Dezember 2016 erwähnten Kategorien von Passagieren übermittelt.

Die Aufbewahrungsdauer der Daten ist in den Artikeln 18 ff. des Gesetzes vom 25. Dezember 2016 geregelt.

B.24.3. Angesichts des Vorstehenden enthält das Gesetz vom 25. Dezember 2016 die Elemente zur Definition der verarbeiteten Daten, der von dieser Datenverarbeitung betroffenen Personen und die Bedingungen und Zwecke dieser Verarbeitung.

Es sind nun die Ermächtigungen zu prüfen, die in den Artikeln 3 § 2 und 7 § 3 des Gesetzes vom 25. Dezember 2016 enthalten sind.

*a) Artikel 3 § 2 des Gesetzes vom 25. Dezember 2016*

B.25.1. In Bezug auf den Geltungsbereich des Gesetzes vom 25. Dezember 2016 heißt es in den Vorarbeiten:

« La directive européenne PNR prévoit la collecte de données des passagers en premier lieu pour le trafic aérien. Elle laisse explicitement la possibilité aux États membres d'imposer cette obligation à d'autres transporteurs. Les États membres peuvent donc adopter une réglementation nationale visant d'autres modes de transport.

La directive européenne PNR prévoit explicitement la possibilité pour les États membres d'établir, en vertu de leur droit national, et dans le respect des principes fondamentaux de l'Union, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs, tels que des agences ou des opérateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR, ou de transporteurs autres que ceux que la présente directive mentionne.

Le projet de loi prévoit dans ce sens l'obligation légale pour les opérateurs de voyage de transmettre les données des passagers à la banque de données des passagers » (*Parl. Dok., Kammer, 2015-2016, DOC 54-2069/001, S. 8*).

B.25.2.1. Artikel 3 § 2 des Gesetzes vom 25. Dezember 2016 in der durch Artikel 2 des Gesetzes vom 2. Mai 2019 abgeänderten Fassung bestimmt:

« Le Roi détermine par arrêté délibéré en Conseil des ministres par secteur de transport et pour les opérateurs de voyage, les données des passagers à transmettre et leurs modalités de transmission, après avis de l'autorité compétente de contrôle des traitements de données à caractère personnel ».

B.25.2.2. In Bezug auf diese Bestimmung heißt es in den Vorarbeiten zum Gesetz vom 25. Dezember 2016:

« L'article trois a pour seule ambition de définir d'emblée le champ d'application de la loi vis-à-vis des transporteurs professionnels de passagers et des opérateurs de voyage. Les transporteurs et les opérateurs de voyage ne doivent pas recueillir plus de données que celles dont ils disposent.

Afin de tenir compte au maximum de la spécificité de chaque secteur de transport ainsi que des opérateurs, un arrêté royal déterminera, après avis de la Commission pour la protection de la vie privée, pour chaque secteur quelles données des passagers précisément (mentionnées à l'article 9) devront être transmises et selon quelles modalités.

La délégation importante faite au Roi s'explique par les spécificités des divers secteurs de transport. La rédaction des AR veillera à répondre au respect des principes de pertinence, de proportionnalité par rapport aux objectifs de la loi et d'égalité de traitement entre les agents économiques des différents secteurs de transport, souligné par le CE » (ebenda, S. 15).

B.25.2.3. In Bezug auf die in Artikel 3 § 2 des Gesetzes vom 25. Dezember 2016 enthaltene Ermächtigung hat die Gesetzgebungsabteilung des Staatsrats folgende Anmerkungen geäußert:

« L'habilitation conférée au Roi ne concerne donc, dans la mise en œuvre de l'article 3, que la détermination des données qui, parmi celles prévues à l'article 9 de l'avant-projet, doivent être transmises par les transporteurs en fonction du secteur dont ils relèvent.

Il en résulte que ce n'est qu'au moment où le ou les projets d'arrêté royal auront été élaborés que pourra être opéré un contrôle du caractère nécessaire, adéquat, pertinent et proportionnel au regard des finalités, des données personnelles des passagers que le transporteur devra collecter et transmettre. En l'état actuel du dispositif, la section de législation n'est pas en mesure de se livrer à un tel contrôle.

Il en va de même en ce qui concerne le respect du principe d'égalité qui devra être assuré entre les agents économiques actifs dans les différents secteurs du transport ainsi qu'entre les passagers lors de l'adoption de cet ou ces arrêtés royaux. Sur ce point également, la section de législation ne dispose pas, à ce moment, d'éléments suffisants pour se prononcer en connaissance de cause » (ebenda, S. 92).

B.26.1. Artikel 3 § 2 des Gesetzes vom 25. Dezember 2016 ermächtigt den König, für jeden Beförderungssektor und für die Reiseunternehmen die zu übermittelnden Passagierdaten sowie die Übermittlungsmodalitäten zu bestimmen.

Gemäß Artikel 3 § 2 des Gesetzes vom 25. Dezember 2016 ist die Stellungnahme des Ausschusses für den Schutz des Privatlebens, nunmehr die Datenschutzbehörde, für die Annahme des königlichen Erlasses, der für jeden Beförderungssektor und für die Reiseunternehmen die zu übermittelnden Passagierdaten sowie die Übermittlungsmodalitäten bestimmt, erforderlich.

B.26.2. Die in Artikel 3 § 2 des Gesetzes vom 25. Dezember 2016 enthaltene Ermächtigung ermöglicht es zunächst, die Pflichten anzupassen, die im Gesetz vom

25. Dezember 2016 für jeden Beförderungssektor und für die Reiseunternehmen, auf die das Gesetz vom 25. Dezember 2016 für anwendbar erklärt wird, vorgesehen sind.

Wie in B.2.2 und B.25.1 erwähnt, zielt die PNR-Richtlinie im Wesentlichen auf den Luftverkehrssektor ab, aber es steht den Mitgliedstaaten frei, das PNR-System auf andere Beförderungssektoren auszudehnen. Wie in B.7 bis B.10 erwähnt, ist das Gesetz vom 25. Dezember 2016 durch die königlichen Erlasse vom 18. Juli 2017 und 3. Februar 2019 jeweils auf die Fluggesellschaften, auf die Busunternehmen und auf die HST-Beförderungsunternehmen und die HST-Fahrkartenverkäufer für anwendbar erklärt worden.

In Kapitel 1 des königlichen Erlasses vom 18. Juli 2017 ist präzisiert, dass er teilweise die API-Richtlinie und die PNR-Richtlinie umsetzt. Nach einer Definition der in ihm verwendeten Begriffe (Kapitel 2 des königlichen Erlasses vom 18. Juli 2017 und Kapitel 1 der königlichen Erlasse vom 3. Februar 2019) werden die Modalitäten bezüglich der jeweiligen Pflichten der Fluggesellschaften, der Busunternehmen und der HST-Beförderungsunternehmen und HST-Fahrkartenverkäufer (Kapitel 3 des königlichen Erlasses vom 18. Juli 2017 und Kapitel 2 der königlichen Erlasse vom 3. Februar 2019), die Modalitäten zur Übermittlung der Passagierdaten (Kapitel 4 des königlichen Erlasses vom 18. Juli 2017 und Kapitel 3 der königlichen Erlasse vom 3. Februar 2019) und das Datum des Inkrafttretens des Gesetzes vom 25. Dezember 2016 für den entsprechenden Beförderungssektor (Kapitel 5 des königlichen Erlasses vom 18. Juli 2017 und Kapitel 4 der königlichen Erlasse vom 3. Februar 2019) festgelegt.

B.26.3. Die klagende Partei bemängelt nicht den Umstand, dass es die Ermächtigung in Artikel 3 § 2 des Gesetzes vom 25. Dezember 2016 dem König erlaubt, die verschiedenen Beförderungssektoren ins Auge zu fassen, sondern nur den Umstand, dass sich diese Ermächtigung auf die Passagierdaten und ihre Übermittlungsmodalitäten bezieht.

B.26.4.1. Bezüglich der Kritik, die sich auf die betreffenden Daten bezieht, betrifft die Ermächtigung in Artikel 3 § 2 des Gesetzes vom 25. Dezember 2016 jedoch nur die Auswahl der zu übermittelnden Passagierdaten aus den Daten zu den Passagieren, die in Artikel 9 des Gesetzes vom 25. Dezember 2016 gesetzlich und erschöpfend aufgezählt sind, für jeden Beförderungssektor und für die Reiseunternehmen.

Dieser Auffassung war im Übrigen auch die Gesetzgebungsabteilung des Staatsrats:

« L’habilitation conférée au Roi ne concerne donc, dans la mise en œuvre de l’article 3, que la détermination des données qui, parmi celles prévues à l’article 9 de l’avant-projet, doivent être transmises par les transporteurs en fonction du secteur dont ils relèvent » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 92).

Auch der Ausschuss für den Schutz des Privatlebens war der Meinung:

« La Commission fait remarquer par ailleurs que si l’article 3, § 2 de la loi PNR prévoit que les données des passagers à transmettre sont déterminées par arrêté royal, ces données sont établies – à juste titre – directement dans la loi, à l’article 9 de la loi PNR. Ces données sont d’ailleurs issues de l’annexe 1 de la directive PNR à laquelle renvoient les articles 6 et 8 de cette directive » (Ausschuss für den Schutz des Privatlebens, Stellungnahme Nr. 23/2017 vom 24. Mai 2017, Nummer 10; siehe ebenfalls Datenschutzbehörde, Stellungnahme Nr. 85/2018 vom 26. September 2018, Nummer 12).

Der König könnte als nicht die Übermittlung von neuen Daten, die nicht in Artikel 9 des Gesetzes vom 25. Dezember 2016 aufgeführt sind, vorsehen (siehe in diesem Sinne Datenschutzbehörde, Stellungnahme Nr. 85/2018 vom 26. September 2018, Nummer 15).

B.26.4.2. Die Ermächtigung in Artikel 3 § 2 des Gesetzes vom 25. Dezember 2016 ermöglicht es dem König außerdem, für jeden Beförderungssektor und für die Reiseunternehmen die Übermittlungsmodalitäten der Passagierdaten zu bestimmen.

Diese Ermächtigung betrifft also nur rein technische Aspekte der Übermittlung der Passagierdaten.

Im königlichen Erlass vom 18. Juli 2017 werden die Methode und die Zeitpunkte der Übermittlung der Passagierdaten durch die Fluggesellschaften präzisiert. Dieser königliche Erlass regelt die « *Push-Methode* » – die in Artikel 8 der PNR-Richtlinie vorgesehen ist, nach der die Fluggesellschaften die PNR-Daten an die Behörde übermitteln, ohne dass diese sie wie bei der « *Pull-Methode* » aus dem Buchungssystem extrahieren muss – die für die Übermittlung der Passagierdaten an die Passagierdatenbank vorgesehen ist. In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 wurde außerdem angegeben, dass diese « *Push-Methode* » « ein besseres Schutzniveau der Daten bietet » und « daher vorzuziehen

ist » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 16). Im Übrigen sind die Datenformate und die Übermittlungsprotokolle, die die Fluggesellschaften verwenden müssen, im Durchführungsbeschluss (EU) 2017/759 der Kommission vom 28. April 2017 « über die gemeinsamen Protokolle und Datenformate, die von den Fluggesellschaften für die Übermittlung von Fluggastdatensätzen (PNR-Daten) an PNR-Zentralstellen zu verwenden sind », festgelegt.

Die königlichen Erlasse vom 3. Februar 2019 sehen jeweils die Methode und die Zeitpunkte der Datenübermittlung durch die Busunternehmen und die HST-Beförderungsunternehmen und die HST-Fahrkartenverkäufer vor. In diesen königlichen Erlassen ist vorgesehen, dass das Datenformat, das Übermittlungsprotokoll und die technische Organisation der Übermittlung in einem Vereinbarungsprotokoll zwischen dem leitenden Beamten der PNR-Zentralstelle und dem betreffenden Beförderungs-/Reiseunternehmen festgelegt werden.

Schließlich sehen die königlichen Erlasse vom 18. Juli 2017 und 3. Februar 2019 vor, dass die Daten 48 Stunden vor der planmäßigen Abflug-/Abfahrtzeit und unmittelbar nach Abfertigungsschluss des Fluges, des Busses oder des Hochgeschwindigkeitszuges unter Bedingungen zur Sicherung der Daten übermittelt werden. Im Bericht an den König vor dem königlichen Erlass vom 18. Juli 2017 ist präzisiert, dass dies « in keiner Weise Last-Minute-Buchungen und Last-Minute-Änderungen verhindert, denn bei der zweiten Übermittlung wird die aktuellste Information versandt » (*Belgisches Staatsblatt* vom 28. Juli 2017, S. 75934).

B.26.5. Die Ermächtigung in Artikel 3 § 2 des Gesetzes vom 25. Dezember 2016 ermöglicht es also, die Passagierdaten unter den in Artikel 9 des Gesetzes vom 25. Dezember 2016 gesetzlich festgelegten Daten zu identifizieren und die Übermittlungsmodalitäten der PNR-Daten je nach den Besonderheiten des jeweiligen Beförderungssektors, auf den das Gesetz vom 25. Dezember 2016 für anwendbar erklärt wird, zu bestimmen.

Wie in B.22.1 erwähnt, verstößt eine solche Befugnisübertragung nicht gegen das in Artikel 22 der Verfassung enthaltene Legalitätsprinzip, da sich diese Ermächtigung ausschließlich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente, wie in B.24 dargelegt, durch den Gesetzgeber festgelegt wurden.

Es obliegt gegebenenfalls dem zuständigen Richter zu prüfen, ob die Nutzung dieser Ermächtigung durch den König den im Klagegrund angeführten Verfassungs- und Vertragsbestimmungen entspricht, wie sie in B.22 präzisiert wurden.

*b) Artikel 7 § 3 des Gesetzes vom 25. Dezember 2016*

B.27.1. Artikel 7 des Gesetzes vom 25. Dezember 2016 bestimmt:

« § 1. Beförderungsunternehmen übermitteln die in Artikel 9 § 1 erwähnten Passagierdaten, über die sie verfügen, und vergewissern sich, dass die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, über die sie verfügen, vollständig, exakt und aktuell sind. Zu diesem Zweck überprüfen sie die Übereinstimmung zwischen den Reisedokumenten und der Identität des betreffenden Passagiers.

§ 2. Reiseunternehmen übermitteln die in Artikel 9 § 1 erwähnten Passagierdaten, über die sie verfügen, und vergewissern sich, dass die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, über die sie verfügen, vollständig, exakt und aktuell sind. Zu diesem Zweck treffen sie alle notwendigen Maßnahmen, um die Übereinstimmung zwischen den Reisedokumenten und der Identität des betreffenden Passagiers zu überprüfen.

§ 3. Der König bestimmt durch einen im Ministerrat beratenen Erlass pro Beförderungssektor und für die Reiseunternehmen die Modalitäten in Bezug auf die in den Paragraphen 1 und 2 erwähnte Verpflichtung ».

B.27.2.1. In Bezug auf diese Bestimmung wurde in den Vorarbeiten des Gesetzes vom 25. Dezember erklärt:

« L'incident dans le Thalys a à nouveau démontré à quel point il est important de pouvoir retracer les déplacements de certains individus. L'obligation d'émettre un titre de transport nominatif a peu de sens si les instances compétentes ne vérifient même pas que la bonne personne effectue son voyage au moyen de ce titre de transport. Ce manque de contrôle a également pour conséquence que nos services ne savent même pas si des individus suspects figurant sur une liste, prennent l'avion ou le train, le bus ou le bateau pour effectuer un voyage international.

Il n'existe aucune obligation européenne qui impose aux transporteurs de contrôler la correspondance entre l'identité et le titre de transport. Neuf États membres européens imposent néanmoins cette obligation légale, entre autres aux compagnies aériennes (entre autres le Portugal, l'Espagne, l'Italie, la Grèce, la Bulgarie, la Hongrie et la Roumanie).

La législation belge ne prévoyait pas jusqu'à présent cette obligation. Il va de soi que l'obligation de transmettre les données des passagers, dont disposent les transporteurs et les opérateurs de voyage, doit pouvoir s'appuyer sur une obligation de vérifier la conformité des documents.

Cette obligation tient compte des spécificités des transporteurs et opérateurs de voyage. Dans cette optique, les opérateurs de voyage seront soumis à une obligation de moyen.

L'identité du passager peut être déterminée sur la base d'un document authentique qui est accepté dans le pays d'origine du passager concerné en tant que document d'identité valide. Ceci pour ne pas créer une limitation à la libre circulation des personnes au sein de l'espace Schengen » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 16-17).

Der Minister der Sicherheit und des Inneren hat ebenfalls erläutert, dass « die Kontrolle der Gültigkeit der Identitätsdokumente nicht [der] Verantwortung [der Beförderungsunternehmen und Reiseunternehmen] unterliegt » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/003, S. 24).

B.27.2.2. In Bezug auf die in Artikel 7 § 3 des Gesetzes vom 25. Dezember 2016 enthaltene Ermächtigung hat die Gesetzgebungsabteilung des Staatsrats folgende Anmerkungen geäußert:

« Cette obligation nouvelle imposée aux transporteurs, en dehors de tout dispositif européen contraignant, *a fortiori* lorsqu'elle concerne également les opérateurs de voyage qui ne sont pas visés par la directive 2016/681/UE du Parlement européen et du Conseil du 27 avril 2016 'relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière ' (ci-après : ' la directive 2016/681/UE ') doit, dans son principe et ses modalités, respecter l'article 22 de la Constitution et la loi du 8 décembre 1992. En l'état actuel du dossier soumis à la section de législation, ce contrôle n'a pu être effectué quant aux modalités de l'obligation nouvelle prévue par l'article 6, § 3, de l'avant-projet pas plus que celui relatif au respect du principe d'égalité garanti par les articles 10 et 11 de la Constitution » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 93).

B.28.1. Nach Artikel 7 § 3 des Gesetzes vom 25. Dezember 2016 bestimmt der König durch einen im Ministerrat beratenen Erlass pro Beförderungssektor und für die Reiseunternehmen die Modalitäten der Verpflichtung der Beförderungsunternehmen und der Reiseunternehmen, die PNR-Daten, über die sie verfügen, zu übermitteln (Artikel 9 § 1), aber auch sich zu vergewissern, dass die API-Daten (Artikel 9 § 1 Nr. 18) « vollständig, exakt und aktuell » sind, indem sie « die Übereinstimmung zwischen den Reisedokumenten und der Identität des betreffenden Passagiers » überprüfen.

Mit dieser Verpflichtung soll die Wirksamkeit des Systems zur Erhebung und Übermittlung der Passagierdaten an die Passagierdatenbank sichergestellt werden, die grundsätzlich durch Artikel 5 des Gesetzes vom 25. Dezember 2016 für Beförderungs- und Reiseunternehmen festgelegt wird.

B.28.2. Mit dieser Bestimmung wird der König somit ermächtigt, die Modalitäten zu regeln, nach denen die Beförderungs- und Reiseunternehmen die Richtigkeit der erweiterten Daten des Eincheckstatus und des Anbordgehens prüfen müssen. Wie es in den Vorarbeiten heißt, wird mit dieser Bestimmung nur eine Verpflichtung zur Wahl eines geeigneten Mittels geschaffen.

B.28.3. Mit der Ermächtigung des Königs in Artikel 7 § 3 des Gesetzes vom 25. Dezember 2016 sollen die Modalitäten dieser Prüfung der Richtigkeit der Daten je nach den Besonderheiten des jeweiligen Beförderungsektors angepasst werden.

Im Bericht an den König vor dem königlichen Erlass vom 18. Juli 2017 heißt es diesbezüglich:

« Le contrôle de conformité, décrit à l'article 4 du présent arrêté royal, vise à vérifier si la personne qui dispose du document de voyage pour un transport précis est effectivement la personne qui monte à bord de l'avion. Ceci se fera en comparant le nom et le prénom mentionnés sur le document de voyage avec le nom et le prénom sur le document d'identité. Le transfert des données des passagers et le traitement de celles-ci n'ont aucun sens s'il n'existe aucune certitude que les passagers sont bien montés à bord de l'avion. L'exécution du contrôle de conformité contribue à l'exactitude des données.

Enfin, si les compagnies aériennes constatent que les données visées à l'article 9, § 1er, 18° de la loi dont elles disposent, ne sont pas actuelles, pas exactes ou incomplètes, elles prennent les mesures nécessaires afin de corriger ces données au plus tard au moment du deuxième transfert. Il faut entendre par données des passagers comme visées à l'article 9, § 1er, 18° de la loi, les données énumérées à l'article 9, § 2, de la loi, à savoir les données d'enregistrement et d'embarquement, transférées par les compagnies aériennes lorsqu'elles en disposent. Les données visées à l'article 9, § 1er, 18°, visent aussi les champs similaires repris dans le même paragraphe (comme le nom et le prénom à l'article 9, § 1er, 4° de la loi) » (*Belgisches Staatsblatt* vom 28. Juli 2017, SS. 75934-75935).

Aufgrund des königlichen Erlasses vom 18. Juli 2017 und der königlichen Erlasse vom 3. Februar 2019 erfolgt diese Kontrolle der Übereinstimmung zu dem Zeitpunkt, an dem die

Passagiere an Bord des Flugzeugs gehen bzw. den Hochgeschwindigkeitszug oder den Bus besteigen. Wenn die betreffenden Beförderungsunternehmen feststellen, dass die API-Daten, über die sie verfügen, nicht aktuell, exakt oder vollständig sind, ergreifen sie alle erforderlichen Maßnahmen, um diese Daten spätestens zum Zeitpunkt der zweiten Übermittlung, die nach Abfertigungsschluss des Fluges, des Busses oder des Hochgeschwindigkeitszuges erfolgt, zu korrigieren.

B.28.4. Die Ermächtigung in Artikel 7 § 3 des Gesetzes vom 25. Dezember 2016 betrifft also nur die technischen Aspekte einer Verpflichtung, die im Gesetz vom 25. Dezember 2016 festgelegt ist.

B.28.5. Wie in B.22.1 erwähnt, verstößt eine solche Befugnisübertragung nicht gegen das in Artikel 22 der Verfassung enthaltene Legalitätsprinzip, da sich diese Ermächtigung ausschließlich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente, wie in B.24 dargelegt, durch den Gesetzgeber festgelegt wurden.

Es obliegt gegebenenfalls dem zuständigen Richter zu prüfen, ob die Nutzung dieser Ermächtigung durch den König den im Klagegrund angeführten Verfassungs- und Vertragsbestimmungen entspricht, wie sie in B.22 präzisiert wurden.

B.29. Insofern er gegen die Artikel 3 § 2 und 7 § 3 des Gesetzes vom 25. Dezember 2016 gerichtet ist, ist der Klagegrund unbegründet.

## *2. Die Begriffe « Identitätsdokumente » und « Reisedokumente » (Artikel 7 §§ 1 und 2)*

B.30. Die klagende Partei bemängelt außerdem die fehlende gesetzliche Definition der Begriffe « Identitätsdokumente » und « Reisedokumente », die in Artikel 7 §§ 1 und 2 des Gesetzes vom 25. Dezember 2016 erwähnt sind.

B.31.1. Der Umstand, dass das Gesetz vom 25. Dezember 2016 keine gesetzliche Definition der « Identitätsdokumente » und « Reisedokumente » enthält, bedeutet nicht, dass gegen das Legalitätsprinzip verstoßen wird, sofern diese Begriffe nicht zu einer Rechtsunsicherheit führen.

B.31.2. Aus den Vorarbeiten zum Gesetz vom 25. Dezember 2016 geht zunächst hervor, dass der Gesetzgeber die Identitätsdokumente im weiten Sinne aufgefasst hat, indem er den Standpunkt vertreten hat, dass die Identität des Passagiers « auf der Grundlage eines echten Dokuments bestimmt werden kann, das im Herkunftsland des betreffenden Passagiers als gültiges Identitätsdokument akzeptiert wird » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 17).

Diese Vorarbeiten ermöglichen es also, den Begriff « Identitätsdokumente » als einen weit gefassten Begriff zu interpretieren, der sich nicht von seiner normalen sprachlichen Bedeutung im Herkunftsland des Passagiers unterscheidet.

B.31.3. Dieser Ansatz wird im Übrigen durch die königlichen Erlasse vom 18. Juli 2017 und 3. Februar 2019 bestätigt, in denen die « Identitätsdokumente » in gleicher Weise als die « Dokumente, die von einer offiziellen Behörde ausgestellt sind und auf deren Grundlage die Identität des Passagiers bestimmt werden kann, das heißt die nationalen Personalausweise, die international anerkannten Reisepässe oder die gesetzlichen Ersatzdokumente » definiert werden (Artikel 2 Nr. 3 des königlichen Erlasses vom 18. Juli 2017 (Luftverkehr); Artikel 1 Nr. 6 des königlichen Erlasses vom 3. Februar 2019 (HST-Verkehr) und Artikel 1 Nr. 4 des königlichen Erlasses vom 3. Februar 2019 (Busverkehr)).

B.32.1. In Bezug auf die « Reisedokumente » konnte der Gesetzgeber der Auffassung sein, dass eine gesetzliche Definition nicht notwendig ist, da es im vorliegenden Fall angebracht ist, sich auf die normale sprachliche Bedeutung dieses Begriffs zu beziehen, das heißt die Dokumente, mit denen dem Passagier eine « Fahrkarte » ausgestellt wird, die es ihm erlaubt, das betreffende Verkehrsmittel gemäß der Praxis in dem betreffenden jeweiligen Beförderungssektor zu benutzen.

B.32.2. Die in den königlichen Erlassen vom 18. Juli 2017 und 3. Februar 2019 enthaltenen Definitionen bestätigen diesen Ansatz.

So definiert Artikel 2 Nr. 4 des königlichen Erlasses vom 18. Juli 2017 die « Reisedokumente » als die « Dokumente, mit denen dem Passagier eine Fahrkarte für die in Artikel 4 Nr. 3 des Gesetzes erwähnte Beförderung », das heißt die Beförderung auf dem

Luftweg, eingeräumt wird. Ebenso definieren die königlichen Erlasse vom 3. Februar 2019 die « Reisedokumente » als die Dokumente, mit denen dem Passagier eine Fahrkarte für die Beförderung eingeräumt wird, die jeweils in Artikel 4 Nr. 4 und Artikel 4 Nr. 5 des Gesetzes vom 25. Dezember 2016 erwähnt ist, das heißt die Beförderung auf dem Landweg oder auf der Schiene.

B.33. Insofern er gegen Artikel 7 §§ 1 und 2 gerichtet ist, ist der Klagegrund unbegründet.

### *3. Die fraglichen Daten (Artikel 4 Nr. 9 und Artikel 9)*

B.34. Die klagende Partei vertritt zunächst die Meinung, dass der sehr weit gefasste Anwendungsbereich der in Artikel 4 Nr. 9 und Artikel 9 des Gesetzes vom 25. Dezember 2016 erwähnten Passagierdaten offenkundig in keinem Verhältnis zur verfolgten Zielsetzung steht. Die klagende Partei führt an, dass es zumindest angebracht wäre, die Kategorie der unter Artikel 9 § 1 Nr. 12 des angefochtenen Gesetzes fallenden Daten zu beschränken.

Zudem könnten aus den fraglichen Daten nach Ansicht der klagenden Partei sensible Daten wie die Zugehörigkeit zu einer Gewerkschaftsorganisation, persönliche Neigungen und persönliche oder berufliche Beziehungen hervorgehen.

B.35.1. Eine Einmischung der Behörden in das Recht auf Achtung des Privatlebens muss nicht nur auf einer ausreichend präzisen Gesetzesbestimmung beruhen, sondern auch einem zwingenden gesellschaftlichen Bedarf in einer demokratischen Gesellschaft entsprechen und im Verhältnis zu dem damit angestrebten rechtmäßigen Ziel stehen.

Der Gesetzgeber verfügt in dem Zusammenhang über einen Ermessensspielraum. Dieser Ermessensspielraum ist gleichwohl nicht grenzenlos: Damit eine gesetzliche Regelung sich mit dem Recht auf Achtung des Privatlebens vereinbaren lässt, ist es erforderlich, dass der Gesetzgeber ein gerechtes Gleichgewicht zwischen allen betroffenen Rechten und Interessen schafft.

B.35.2. Bei der Beurteilung dieses Gleichgewichts berücksichtigt der Europäische Gerichtshof für Menschenrechte u. a. die Bestimmungen des Übereinkommens Nr. 108 (vgl. EuGHMR, 25. Februar 1997, *Z gegen Finnland*, § 95; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, § 103).

Dieses Übereinkommen Nr. 108 beinhaltet u. a. die Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten: Rechtmäßigkeit, Ordnungsmäßigkeit, Transparenz, Zweckbindung, Verhältnismäßigkeit, Richtigkeit, Speicherbegrenzung, Integrität, Vertraulichkeit und Rechenschaftspflicht.

Dasselbe Übereinkommen wird durch ein Änderungsprotokoll aktualisiert, das am 10. Oktober 2018 zur Unterzeichnung aufgelegt wurde.

B.35.3. Ein Eingriff in das Recht auf Achtung des Privatlebens durch Verarbeitung von personenbezogenen Daten, hier durch Zugang seitens öffentlicher Behörden zu bestimmten personenbezogenen Daten und deren Nutzung mithilfe besonderer Techniken (EuGHMR, 26. März 1987, *Leander gegen Schweden*, § 48; Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, § 46; EuGH, Große Kammer, 8. April 2014, C-293/12, *Digital Rights Ireland Ltd*, und C-594/12, *Kärntner Landesregierung u.a.*), muss deshalb eine angemessene Rechtfertigungsgrundlage haben und den vom Gesetzgeber verfolgten Zielen entsprechen.

B.35.4. In Rahmen der Verhältnismäßigkeit berücksichtigen der Europäische Gerichtshof für Menschenrechte und der Gerichtshof der Europäischen Union das etwaige Vorhandensein der in B.22.2 erwähnten materiellen und prozessualen Garantien in der einschlägigen Regelung.

Bei der Beurteilung der Verhältnismäßigkeit von Maßnahmen in Bezug auf die Verarbeitung personenbezogener Daten sind mithin u. a. deren automatischer Charakter, die verwendeten Techniken, der Genauigkeitsgrad, die Relevanz, der gegebenenfalls außergewöhnliche Charakter der zu verarbeitenden Daten, das etwaige Vorhandensein von Maßnahmen zur Begrenzung der Datenspeicherfrist, das etwaige Vorhandensein eines unabhängigen Überwachungssystems, mit dem geprüft werden kann, ob eine Datenspeicherung weiterhin erforderlich ist, das etwaige Vorhandensein von ausreichenden Kontrollrechten und Rechtsbehelfen für die betroffenen Personen, das etwaige Vorhandensein

von Garantien zur Vermeidung einer Stigmatisierung der Personen, deren Daten verarbeitet werden, der unterscheidende Charakter der Regelung und das etwaige Vorhandensein von Garantien zur Vermeidung einer falschen Nutzung und von Missbrauch der verarbeiteten personenbezogenen Daten durch öffentliche Behörden zu berücksichtigen (vgl. EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, § 59; Entscheidung, 29. Juni 2006, *Weber und Saravia gegen Deutschland*, § 135; 28. April 2009, *K.H. u.a. gegen Slowakei*, §§ 60-69; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, §§ 101-103, 119, 122 und 124; 18. April 2013, *M.K. gegen Frankreich*, §§ 37 und 42-44; 18. September 2014, *Brunet gegen Frankreich*, §§ 35-37; 12. Januar 2016, *Szabó und Vissy gegen Ungarn*, § 68; EuGH, Große Kammer, 8. April 2014, C-293/12, *Digital Rights Ireland Ltd*, und C-594/12, *Kärntner Landesregierung u.a.*, §§ 56-66).

B.35.5. In seinem Gutachten 1/15 vom 26. Juli 2017 hat der Gerichtshof ebenfalls darauf hingewiesen, dass eine Einmischung in das Recht auf Schutz personenbezogener Daten auf das « absolut Notwendige » beschränkt sein muss:

« 140. Zum Grundsatz der Verhältnismäßigkeit ist festzustellen, dass der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das absolut Notwendige beschränken (Urteil vom 16. Dezember 2008, *Satakunnan Markkinapörssi und Satamedia*, C-73/07, EU:C:2008:727, Rn. 56, vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU:C:2014:238, Rn. 51 und 52, vom 6. Oktober 2015, *Schrems*, C-362/14, EU:C:2015:650, Rn. 92, und vom 21. Dezember 2016, *Tele2 Sverige und Watson u. a.*, C-203/15 und C-698/15, EU:C:2016:970, Rn. 96 und 103).

141. Um diesem Erfordernis zu genügen, muss die betreffende Regelung, die den Eingriff enthält, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren Daten übermittelt 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, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass der Eingriff auf das absolut Notwendige beschränkt wird. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden. Dies gilt insbesondere, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU:C:2014:238, Rn. 54 und 55, sowie vom 21. Dezember 2016, *Tele2 Sverige und Watson u. a.*, C-203/15 und C-698/15, EU:C:2016:970, Rn. 109 und 117; vgl. in diesem Sinne EGMR, 4. Dezember 2008, *S. und Marper/Vereinigtes Königreich*, CE:ECHR:2008:1204JUD003056204, § 103) ».

B.36.1. In Artikel 4 Nr. 9 des Gesetzes vom 25. Dezember 2016 ist « PNR » als « der Datensatz mit den zu jedem einzelnen Passagier notwendigen Reisedaten, der die in Artikel 9 erwähnten Informationen enthält, » definiert. Wie in B.24.1 erwähnt, werden in Artikel 9 des Gesetzes vom 25. Dezember 2016 einerseits die in Artikel 9 § 1 Nr. 18 erwähnten erweiterten Daten des Eincheckstatus und des Anbordgehens (API-Daten), die in Artikel 9 § 2 des Gesetzes vom 25. Dezember 2016 erschöpfend aufgelistet sind, und andererseits die Buchungsdaten (PNR-Daten) unterschieden, die höchstens die 19 Elemente umfassen, die in Artikel 9 § 1 des Gesetzes vom 25. Dezember 2016 erschöpfend aufgezählt sind, darunter die in Artikel 9 § 1 Nr. 18 erwähnten API-Daten.

Die Unterscheidung zwischen den API-Daten und den PNR-Daten ist in den in B.3.1 zitierten Vorarbeiten ausdrücklich angegeben.

B.36.2.1. In den Vorarbeiten zu Artikel 9 des Gesetzes vom 25. Dezember 2016 wurde ausgeführt:

« L'article 9 détermine les données des passagers qui devront être transmises. Ces données sont transmises par le biais d'un format de données imposé et uniforme par secteur de transport et opérateur de voyage pour lequel il est fait usage d'une norme acceptée au niveau international (pour les compagnies aériennes il s'agit par exemple du format PNRGOV, développé par IATA/ICAO/WCO).

L'article 9 fait une distinction entre, d'une part, les données de réservation prévues au § 1er et, d'autre part, les données d'enregistrement et d'embarquement mentionnées au § 2 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 20-21).

Diese Unterscheidung entspricht der Unterscheidung zwischen den Daten, auf die sich die API-Richtlinie bezieht, und den Daten, auf die sich die PNR-Richtlinie bezieht.

B.36.2.2. Die Übermittlung von Passagierdaten, die im Gesetz vom 25. Dezember 2016 geregelt wird, schreibt es den Beförderungs- und Reiseunternehmen jedoch nicht vor, weitere Daten als diejenigen, über die sie bereits verfügen, zu erheben:

« Les transporteurs et opérateurs de voyage collectent et traitent déjà les données de leurs passagers à des fins commerciales. En ce qui concerne, par exemple, les compagnies aériennes, celles-ci conservent aussi des données de passagers à remettre préalablement (données API) comme données PNR, mais ce n'est pas une généralité. Les données API sont,

entre autres, les données lues par la ‘ *machine readable zone* ’ du document d’identité. Conformément à la directive PNR, les transporteurs et opérateurs de voyages ne doivent transmettre que les données dont ils disposent et ne doivent pas recueillir ou conserver des données supplémentaires auprès des passagers. Ils ne devraient pas non plus obliger les passagers à communiquer des données en sus de celles qui leur sont déjà transmises » (ebenda, SS. 15-16).

In den Erwägungsgründen 8 und 9 der PNR-Richtlinie ist diesbezüglich ebenfalls angegeben:

« (8) Die Fluggesellschaften erheben und verarbeiten bereits PNR-Daten ihrer Fluggäste für ihre eigenen geschäftlichen Zwecke. Durch diese Richtlinie sollten weder Fluggesellschaften dazu verpflichtet werden, weitere Fluggastdaten zu erheben oder vorzuhalten, noch sollte von den Fluggästen verlangt werden, dass sie neben den Daten, die die Fluggesellschaften bereits von ihnen erhalten, noch zusätzliche Daten bereitstellen.

(9) Einige Fluggesellschaften halten API-Daten, die sie erheben, als Teil der PNR-Daten vor, während andere dies nicht tun. Die Verwendung von PNR-Daten zusammen mit API-Daten bietet einen Mehrwert, indem sie den Mitgliedstaaten die Feststellung der Identität einer Person erleichtert, mithin den Nutzen dieses Ergebnisses für die Verhütung, Aufdeckung und Ermittlung von Straftaten erhöht und die Gefahr minimiert, dass Überprüfungen und Ermittlungen zu unschuldigen Personen durchgeführt werden. Es muss daher sichergestellt werden, dass Fluggesellschaften, die API-Daten erheben, diese übermitteln, unabhängig davon, ob sie API-Daten auf andere technische Weise als PNR-Daten vorhalten ».

B.37.1. In Bezug auf die API-Daten sieht Artikel 3 Absatz 2 der API-Richtlinie vor, dass zu den Angaben über die Personen, die sie zu einer zugelassenen Grenzübergangsstelle befördern werden, über die diese Personen in das Hoheitsgebiet eines Mitgliedstaats einreisen werden, die folgenden Angaben zählen:

- « - die Nummer und die Art des mitgeführten Reisedokuments,
- die Staatsangehörigkeit,
- der vollständige Name,
- das Geburtsdatum,
- die Grenzübergangsstelle für die Einreise in das Hoheitsgebiet der Mitgliedstaaten,
- die Beförderungs-Codenummer,
- die Abreise- und Ankunftszeit,

- die Gesamtzahl der mit der betreffenden Beförderung beförderten Personen,
- der ursprüngliche Abreiseort ».

B.37.2.1. Vorher waren die Fluggesellschaften bereits verpflichtet, die API-Daten gemäß dem königlichen Erlass vom 11. Dezember 2006, aufgehoben durch Artikel 10 des königlichen Erlasses vom 18. Juli 2017, zu übermitteln.

In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 wurde nämlich bestätigt:

« Le projet de loi reprend en substance le régime prévu par l'arrêté royal du 11 décembre 2006 concernant l'obligation pour les transporteurs aériens de communiquer les données relatives aux passagers, mentionné plus haut. La liste des données ' API ' prévue par l'avant-projet de loi correspond donc en substance à celle établie par cet arrêté.

Toutefois, l'avant-projet de loi a un champ d'application plus large que celui de la directive 2004/82/CE car l'obligation faite aux transporteurs est généralisée à tous les secteurs de transport » (ebenda, S. 11).

B.37.2.2. Vor seiner Aufhebung durch den königlichen Erlass vom 18. Juli 2017 waren in Artikel 3 § 2 des königlichen Erlasses vom 11. Dezember 2006 als Angaben, die von den Fluggesellschaften zu übermitteln sind, genannt:

- « 1° le numéro et le type du document de voyage utilisé;
- 2° la nationalité;
- 3° le nom complet;
- 4° la date de naissance;
- 5° le point de passage frontalier utilisé pour entrer sur le territoire belge;
- 6° le numéro de vol;
- 7° les heures de départ et d'arrivée du vol;
- 8° le nombre total des personnes transportées;
- 9° le point d'embarquement initial ».

Diese Liste der Angaben übernahm also die in Artikel 3 Absatz 2 der API-Richtlinie vorgesehene Mindestliste.

B.38.1. In Bezug auf die PNR-Daten heißt es im Erwägungsgrund 15 der PNR-Richtlinie:

« Eine Liste mit den PNR-Daten, die für eine PNR-Zentralstelle bestimmt sind, sollte erstellt und inhaltlich so zusammengesetzt sein, dass sie sowohl den legitimen Bedürfnissen der Behörden im Zusammenhang mit der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gerecht werden und damit einen Beitrag zur inneren Sicherheit in der Union leisten als auch dem Grundrechtsschutz und insbesondere dem Schutz der Privatsphäre des Einzelnen und seiner personenbezogenen Daten Genüge tun. Zu diesem Zweck sollten hohe Standards zur Anwendung kommen, die mit der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“), dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) und der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) im Einklang stehen. Eine solche Liste sollte nicht auf der Rasse oder ethnischen Herkunft, der Religion oder der Weltanschauung, der politischen oder sonstigen Meinungen, der Mitgliedschaft in einer Gewerkschaft, dem Gesundheitszustand, dem Sexualleben oder der sexuellen Orientierung einer Person beruhen. Die PNR-Daten sollten nur jene Details über den Buchungsvorgang und die Reiseroute von Fluggästen beinhalten, mit deren Hilfe die zuständigen Stellen diejenigen Fluggäste ermitteln können, die eine Bedrohung für die innere Sicherheit darstellen ».

B.38.2. Artikel 3 Nr. 5 der PNR-Richtlinie definiert den « Fluggastdatensatz » oder « PNR » als « einen Datensatz mit den für die Reise notwendigen Angaben zu jedem einzelnen Fluggast, die die Bearbeitung und Überprüfung der von einer Person oder in ihrem Namen getätigten Reservierungen für jede Reise durch die buchenden und beteiligten Fluggesellschaften ermöglichen, unabhängig davon, ob er in Buchungssystemen, Abfertigungssystemen (Departure Control Systems) zum Einchecken von Passagieren auf Flüge, oder gleichwertigen Systemen, die die gleichen Funktionen bieten, enthalten ist ».

Diese Definition des PNR-Datensatzes wurde in fast identischer Weise in Artikel 4 Nr. 9 des Gesetzes vom 25. Dezember 2016 übernommen.

B.38.3.1. Anhang I der PNR-Richtlinie mit der Überschrift « Von Fluggesellschaften erhobene PNR-Daten » bestimmt:

- « 1. PNR-Buchungscode (Record Locator)
- 2. Datum der Buchung/Flugscheinausstellung

3. Planmäßiges Abflugdatum bzw. planmäßige Abflugdaten
4. Name(n)
5. Anschrift und Kontaktangaben (Telefonnummer, E-Mail-Adresse)
6. Alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift
7. Gesamter Reiseverlauf für bestimmte PNR-Daten
8. ‘ Vielflieger-Eintrag ’
9. Reisebüro/Sachbearbeiter
10. Reisestatus des Fluggasts mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Flüge (No show) und Fluggäste mit Flugschein, aber ohne Reservierung (Go show)
11. Angaben über gesplittete/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 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)
13. Flugscheindaten einschließlich Flugscheinnummer, Ausstellungsdatum, einfacher Flug (One-way), automatische Tarifanzeige (Automated Ticket Fare Quote fields)
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 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)
19. Alle vormaligen Änderungen der unter den Nummern 1 bis 18 aufgeführten PNR-Daten ».

B.38.3.2. Durch Nummer 18 von Anhang I der PNR-Richtlinie wird also der Begriff der API-Daten, auf den sich Artikel 3 Absatz 2 der API-Richtlinie bezog, erweitert.

B.39.1.1. In Bezug auf die Buchungsdaten bezeichnet Artikel 9 § 1 des Gesetzes vom 25. Dezember 2016 als PNR-Daten höchstens:

« 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 ».

B.39.1.2. Die in Artikel 9 § 1 des Gesetzes vom 25. Dezember 2016 erwähnten PNR-Daten übernehmen somit die in Anhang I der PNR-Richtlinie erwähnten Daten.

B.39.2.1. In Bezug auf die erweiterten Daten des Eincheckstatus und des Anbordgehens bezeichnet Artikel 9 § 2 des Gesetzes vom 25. Dezember 2016 als API-Daten:

« 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 ».

B.39.2.2. Mit den in Artikel 9 § 2 des Gesetzes vom 25. Dezember 2016 erwähnten API-Daten werden im Wesentlichen die in Nummer 18 von Anhang I der PNR-Richtlinie erwähnten Daten übernommen und diese sind somit umfassender als die Daten, die unter Artikel 3 Absatz 2 der API-Richtlinie fielen.

B.40.1. Wie in B.3 erwähnt, hat das Gesetz vom 25. Dezember 2016 die Zielsetzung, die öffentliche Sicherheit zu gewährleisten, indem eine Übermittlung von Passagierdaten und deren Verwendung im Rahmen der Bekämpfung terroristischer Straftaten und grenzübergreifender schwerer Kriminalität eingeführt wird.

Diese Ziele stellen eine dem Gemeinwohl dienende Zielsetzung dar, die Eingriffe in das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten rechtfertigen können (EuGH, Große Kammer, 8. April 2014, C-293/12, *Digital Rights Ireland Ltd*, Randnr. 42). Der Gerichtshof hat außerdem bestätigt, dass diese dem Gemeinwohl dienende Zielsetzung die Übermittlung und Verarbeitung von Fluggastdatensätzen rechtfertigen kann (EuGH, Große Kammer, 26. Juli 2017, Gutachten 1/15, Randnrn. 148 und 149).

B.40.2. Es ist nun zu prüfen, ob diese Eingriffe, wie in B.35 erwähnt, unter Berücksichtigung des im Gesetz vom 25. Dezember 2016 erwähnten Umfangs der Daten ausreichend präzise, verhältnismäßig und auf das « absolut Notwendige » beschränkt sind.

B.41.1. Die Erhebung der unter das Gesetz vom 25. Dezember 2016 fallenden Passagierdaten ist in Bezug auf den Inhalt dieser Daten mit Garantien versehen.

B.41.2. Wie in B.24.1 erwähnt, sind diese Daten zunächst in erschöpfender Weise in Artikel 9 des Gesetzes vom 25. Dezember 2016 bestimmt.

Diese Daten sind Informationen, die direkt mit der Reise zusammenhängen, die zu der in den Anwendungsbereich des Gesetzes vom 25. Dezember 2016 fallenden Beförderung Anlass gibt. Wie in B.36.2.2 erwähnt, handelt es sich um Daten, über die die Beförderungs- und Reiseunternehmen grundsätzlich bereits verfügen. Außerdem entsprechen diese Daten dem Anhang I der Leitlinien der International Civil Aviation Organization (ICAO) (EuGH, 26. Juli

2017, Gutachten 1/15, Randnr. 156). Diese Daten sind somit sachdienlich in Bezug auf die Zielsetzung des Gesetzes vom 25. Dezember 2016.

B.41.3.1. Im Übrigen bestimmen die nicht angefochtenen Artikel 10 und 11 des Gesetzes vom 25. Dezember 2016:

« Art. 10. Die Passagierdaten dürfen 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.

Art. 11. Wenn die von den Beförderungsunternehmen und Reiseunternehmen übermittelten Passagierdaten andere als die in Artikel 9 aufgeführten Daten beinhalten oder wenn sie Daten, wie in Artikel 10 aufgeführt, beinhalten, werden diese zusätzlichen Daten von der PNR-Zentralstelle unmittelbar nach ihrem Eingang dauerhaft gelöscht ».

B.41.3.2. In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 wird diesbezüglich bestätigt:

« Les données des passagers ne peuvent en aucun cas avoir trait à l'origine raciale ou ethnique de l'intéressé, ni à ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à une organisation syndicale, sa santé, sa vie sexuelle ou son orientation sexuelle. Les données doivent en revanche comporter des informations détaillées sur la réservation effectuée par le passager et sur son itinéraire, qui permettront aux instances compétentes de déterminer quels passagers sont susceptibles de constituer un risque pour la sécurité.

[...]

Les listes de données relatives aux passagers sont limitées à ce qui est strictement nécessaire pour répondre aux exigences légitimes des autorités compétentes dans le cadre des objectifs fixés dans la loi. Les autres données que celles énoncées aux articles 9 et 10 de la présente loi ne sont pas collectées et sont effacées immédiatement » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 21).

B.41.4. Diese Bestimmungen gewährleisten daher, dass sensible Daten im Rahmen der Passagierdaten, die unter das Gesetz vom 25. Dezember 2016 fallen, grundsätzlich nicht erhoben oder gespeichert werden dürfen.

B.41.5. In seinem vorerwähnten Gutachten 1/15 vom 26. Juli 2017 war der Gerichtshof in Bezug auf sensible Daten ebenfalls der Auffassung, dass « Artikel 7, Artikel 8, Artikel 21 und Artikel 52 Absatz 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 » (Randnr. 167).

Diese Anmerkung kann auf den vorliegenden Fall übertragen werden.

B.42.1. Auch wenn Garantien bezüglich der unter das Gesetz vom 25. Dezember 2016 fallenden Passagierdaten bestehen, ist dennoch zu fragen, ob diese Garantien angesichts der Umfangs der fraglichen Daten ausreichend sind.

B.42.2. Die in Artikel 9 § 1 des Gesetzes vom 25. Dezember 2016 aufgeführten Daten, mit denen die in Anhang I der PNR-Richtlinie erwähnten Daten übernommen werden, umfassen nämlich sehr weitgehende Daten, neben den Daten des Eincheckstatus und des Anbordgehens insbesondere: den gesamten Reiseverlauf für den Passagier, das Reisebüro, die Sitzplatznummer, vollständige Gepäckangaben, Zahlungsinformationen einschließlich Rechnungsanschrift, allgemeine Hinweise, « einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren » (Artikel 9 § 1 Nr. 12).

B.42.3.1. In seinem vorerwähnten Gutachten 1/15 vom 26. Juli 2017 hat der Gerichtshof außerdem angemerkt, 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 Artikel 2 Buchstabe e des geplanten Abkommens liefern [können] » (Randnr. 128).

B.42.3.2. In seiner Stellungnahme vom 19. August 2016 « über die datenschutzrechtlichen Auswirkungen der Verarbeitung von Passagierdaten » hat der Beratende Ausschuss für das Übereinkommen Nr. 108 des Europarates « zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten » ebenfalls angemerkt:

« Les PNR contiennent des informations visant à faciliter le voyage d'un passager, et peuvent comprendre un certain nombre de données sensibles (données pouvant servir à indiquer l'origine raciale, les opinions politiques, les convictions religieuses et autres, l'état de santé ou l'orientation sexuelle d'une personne), non seulement sous certaines données 'codées' mais aussi dans le champ ouvert contenant des observations générales (telles que les demandes diététiques et médicales, ou le fait qu'une association politique ou religieuse a bénéficié de billets à prix réduit pour le voyage de ses membres), ce qui pourrait conduire à une discrimination directe » (Europarat, Stellungnahme vom 19. August 2016, T-PD(2016)18rev, S. 7).

B.42.3.3. Die Agentur der Europäischen Union für Grundrechte hat ebenfalls angemerkt, dass die PNR-Daten « sensible oder besondere Daten [...] in dem Posten 'allgemeine Hinweise' enthalten [können] » (Gutachten 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; siehe auch ebenda, S. 13).

B.42.4. Angesichts ihres sehr weit gefassten Anwendungsbereichs könnten daher die in Artikel 9 des Gesetzes vom 25. Dezember 2016 erwähnten Daten, auch wenn sie nicht direkt sensible Daten enthalten dürfen, dennoch indirekt sensible Elemente offenlegen, die unter den Schutz personenbezogener Daten und die Achtung des Privatlebens fallen.

Unter Berücksichtigung des in B.35.5 erwähnten Gutachtens 1/15 des Gerichtshofs ist die Frage zu stellen, ob die in Artikel 9 des Gesetzes vom 25. Dezember 2016 erwähnten Daten, mit denen die in Anhang I der PNR-Richtlinie aufgeführten Daten übernommen werden, nicht über das « absolut Notwendige » hinausgehen, um die Zielsetzung der PNR-Richtlinie zu erreichen.

B.42.5. Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union ermächtigt den Gerichtshof der Europäischen Union, im Wege der Vorabentscheidung sowohl über die Auslegung der Verträge und der Handlungen der Einrichtungen der Union als auch über die Gültigkeit dieser Handlungen zu entscheiden. Nach dem dritten Absatz dieser Bestimmung ist ein einzelstaatliches Gericht verpflichtet, den Gerichtshof anzurufen, wenn dessen Entscheidungen – wie die des Verfassungsgerichtshofs – selbst nicht mehr mit Rechtsmitteln des innerstaatlichen Rechts angefochten werden können. Im Fall von Zweifeln bezüglich der Auslegung oder der Gültigkeit einer Bestimmung des Rechts der Europäischen

Union, die für die Lösung eines schwebenden Verfahrens bei einem einzelstaatlichen Gericht wichtig ist, muss dieses, auch von Amts wegen, dem Gerichtshof eine Vorabentscheidungsfrage stellen.

Vor der Urteilsfällung zur Sache ist folglich dem Gerichtshof der Europäischen Union die im Tenor wiedergegebene zweite Vorabentscheidungsfrage zu stellen.

B.43.1. In seinem vorerwähnten Gutachten 1/15 vom 26. Juli 2017 hat der Gerichtshof außerdem die folgenden Anmerkungen in Bezug auf die Anforderung einer klaren und präzisen Definition der Daten, die unter den Entwurf eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen fallen, geäußert:

« 155. Das geplante Abkommen müsste hinsichtlich der Daten, auf die es sich bezieht, klar und präzise definieren, welche PNR-Daten die Fluggesellschaften in Anwendung des Abkommens an Kanada übermitteln müssen.

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 Artikel 4 Absatz 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 ».

B.43.2. Da einige dieser Anmerkungen wegen der beispielhaften und nicht erschöpfenden Beschaffenheit einiger Daten, die in dem mit Artikel 9 des Gesetzes vom 25. Dezember 2016 umgesetzten Anhang I der PNR-Richtlinie enthalten sind, auf den vorliegenden Fall anwendbar sein könnten, ist folglich vor der Urteilsfällung zur Sache dem

Gerichtshof der Europäischen Union die im Tenor wiedergegebene dritte Vorabentscheidungsfrage zu stellen.

#### *4. Der Begriff des « Passagiers » (Artikel 4 Nr. 10)*

B.44. Die klagende Partei bemängelt den weit gefassten Begriff « Passagier », der zu einer nicht gezielten systematischen und automatisierten Verarbeitung von Daten aller Passagiere führe.

B.45.1. Artikel 4 Nr. 10 des angefochtenen Gesetzes definiert den « Passagier » als « 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 ».

In diesem Artikel wird der Inhalt von Artikel 3 Nr. 4 der PNR-Richtlinie übernommen, der den « Fluggast » ebenfalls als « 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 » definiert.

B.45.2. Die Definition des « Passagiers » hat zur Folge, dass die Erhebung, Übermittlung und Verarbeitung der PNR-Daten dieser « Passagiere » allgemeine und unterschiedslose Verpflichtungen darstellen, die für alle Personen gelten, die befördert werden oder befördert werden sollen und auf der Passagierliste eingetragen sind.

Die Verpflichtungen, die das Gesetz vom 25. Dezember 2016 vorschreibt, gelten somit unabhängig davon, ob schwerwiegende Gründe zu der Annahme vorliegen, dass die betroffenen Personen eine Straftat begangen haben oder eine Straftat begehen werden, oder wegen einer Straftat verurteilt wurden.

B.45.3. In seiner Stellungnahme vom 19. August 2016 « über die datenschutzrechtlichen Auswirkungen der Verarbeitung von Passagierdaten » hat der Beratende Ausschuss für das Übereinkommen Nr. 108 des Europarates « zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten » diesbezüglich angemerkt:

« Le traitement des données PNR – qui a l’avantage unique de permettre l’identification des personnes d’intérêt – est un filtrage général et non sélectif de tous les passagers, y compris de ceux qui ne sont pas soupçonnés d’avoir commis une quelconque infraction pénale, par différentes autorités compétentes, et il concerne des données collectées initialement à des fins commerciales par des entités privées. Eu égard à l’ampleur de l’atteinte aux droits à la vie privée et à la protection des données qui découlerait du traitement des données PNR, il doit être clairement établi que ledit traitement est une mesure nécessaire dans une société démocratique dans un but légitime; il faut en outre que les garanties appropriées soient mises en place. Il est indispensable de démontrer expressément la nécessité de la collecte et de l’exploitation ultérieure des données PNR » (Stellungnahme vom 19. August 2016, T-PD(2016)18rev, S. 5).

Der Ausschuss hat auch die Notwendigkeit einer regelmäßigen Bewertung eines solchen PNR-Systems betont, um festzustellen, ob es noch gerechtfertigt ist:

« Dans le cas des systèmes existants de traitement des données PNR par les autorités publiques compétentes, une plus grande transparence sur l’évaluation de l’efficacité de ces systèmes doit être recherchée en vue de permettre une évaluation fondée et indépendante de la nécessité du système. Si cette transparence doit être détaillée, elle ne doit toutefois pas aller à l’encontre de l’objectif légitime. Par exemple, des informations objectives et quantifiables concernant les résultats atteints, comme le nombre de personnes arrêtées, les menaces terroristes qui pourraient être évitées, les autres effets dissuasifs, la modification des comportements des délinquants (par exemple, le renoncement à des actes criminels envisagés), la probabilité d’une augmentation importante du coût et de la difficulté de la perpétration d’infractions (tels que des attentats terroristes) permettraient d’éclairer l’évaluation de la nécessité d’un système de traitement des PNR.

Il convient de procéder à intervalles réguliers à un examen de la nécessité du système des PNR afin de déterminer s’il est toujours justifié » (ebenda, S. 6).

B.45.4.1. Artikel 19 der PNR-Richtlinie mit der Überschrift « Überprüfung » sieht vor, dass die Kommission anhand von Informationen der Mitgliedstaaten, einschließlich der statistischen Daten, bis zum 25. Mai 2020 eine Überprüfung aller Elemente dieser Richtlinie vornimmt und dem Europäischen Parlament und dem Rat einen Bericht vorlegt und diesen erläutert.

Artikel 19 Absatz 3 der PNR-Richtlinie sieht vor, dass « die Kommission [...] dabei die Erfahrungen der Mitgliedstaaten, insbesondere jener Mitgliedstaaten, die gemäß Absatz 2 diese Richtlinie auf EU-Flüge anwenden, » berücksichtigt und « auch [prüft], ob es erforderlich ist, Wirtschaftsteilnehmer, die keine Beförderungsunternehmen sind, wie etwa Reisebüros oder Reiseveranstalter, die Dienstleistungen im Zusammenhang mit Reisen – einschließlich Flugbuchungen – erbringen, in den Anwendungsbereich dieser Richtlinie aufzunehmen ».

B.45.4.2. Artikel 52 § 1 des Gesetzes vom 25. Dezember 2016 sieht vor, dass « vorliegendes Gesetz [...] drei Jahre nach seinem Inkrafttreten einer Bewertung unterzogen » wird.

B.46.1. Im Bereich der elektronischen Kommunikation hat der Gerichtshof der Europäischen Union durch ein Urteil der Großen Kammer vom 21. Dezember 2016 über eine nationale Regelung, die eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsah, und über die Pflicht der Betreiber elektronischer Kommunikationsdienste, diese Daten systematisch und kontinuierlich ohne jede Ausnahme zu speichern, befunden (EuGH, 21. Dezember 2016, Große Kammer, C-203/15, *Tele2 Sverige AB gegen Post-och telestyrelsen* und C-698/15, *Secretary of State for the Home Department gegen Tom Watson u.a.*).

Dem Gerichtshof zufolge « kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen; eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen » (Randnr. 103).

Der Europäische Gerichtshof hat Folgendes entschieden:

« 104. Eine solche Regelung hat zum einen in Anbetracht ihrer in Rn. 97 des vorliegenden Urteils beschriebenen charakteristischen Merkmale zur Folge, 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.

105. Zum anderen sieht eine nationale Regelung wie die im Ausgangsverfahren, 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. 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 Mindestanforderungen 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 ».

B.46.2. Auf die zweite Vorabentscheidungsfrage in der Rechtssache C-203/15 und auf die erste Vorabentscheidungsfrage in der Rechtssache C-698/15 antwortet der Gerichtshof, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7, 8 und 11 sowie des Artikel 52 Absatz 1 der Charta dahin auszulegen sei, « 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 » (Randnummer 125).

B.46.3. Seinerseits hat der Europäische Gerichtshof für Menschenrechte mittlerweile in seinem Urteil *Centrum för Rättvisa gegen Schweden* vom 19. Juni 2018 erkannt, dass die schwedischen Rechtsvorschriften über die Massenüberwachung elektronischer Kommunikationen mit Artikel 8 der Europäischen Menschenrechtskonvention in Übereinstimmung stehen. Um zu der Schlussfolgerung zu gelangen, dass keine Verletzung vorliegt, stützt er sich auf die Kriterien, die er in seiner früheren Rechtsprechung entwickelt hat (siehe insbesondere EuGHMR, Große Kammer, 4. Dezember 2015, *Roman Zakharov gegen Russland*). Er hebt insbesondere Folgendes hervor:

« La Cour a expressément reconnu que les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder la sécurité nationale (cf. *Weber et Saravia*, précité, § 106). Dans les affaires *Weber et Saravia* et *Liberty e.a.*, la Cour a admis que les régimes d'interception massive n'excèdent pas en eux-mêmes cette marge d'appréciation. Au vu de la motivation de la Cour dans ces décisions et compte tenu des menaces auxquelles sont confrontés de nombreux États contractants (dont le fléau du terrorisme international et d'autres formes graves de criminalité telles que le trafic de stupéfiants, la traite d'êtres humains, l'exploitation sexuelle des enfants et la cybercriminalité) des progrès technologiques qui permettent aux terroristes et aux criminels d'échapper plus facilement à la détection sur internet et de l'impossibilité de prévoir les voies par lesquelles les communications électroniques seront transmises, la Cour considère que la décision de recourir à un régime d'interception massive afin de repérer des menaces jusqu'alors inconnues pour la sécurité nationale relève de la marge d'appréciation des États » (EuGHMR, 19. Juni 2018, *Centrum för Rättvisa gegen Schweden*, § 112).

Der Europäische Gerichtshof für Menschenrechte hat hingegen geurteilt, dass das englische Gesetz über die Überwachung von Kommunikation gegen Artikel 8 der Europäischen Menschenrechtskonvention verstoße, da es die Kriterien in seiner Rechtsprechung nicht einhalte. Er war ebenfalls der Auffassung, dass « die Arbeitsweise von Massenüberwachungssystemen grundsätzlich in den Ermessensspielraum des Staates fällt. Die Massenüberwachung ist per definitionem nicht gezielt und sie dem Vorhandensein eines « begründeten Verdachts » unterzuordnen, würde ihre Durchführung unmöglich machen » (EuGHMR, 13. September 2018, *Big Brother Watch u.a. gegen Vereinigtes Königreich*, § 317).

B.46.4. Es stellt sich die Frage, in welchem Maße die vorerwähnte Rechtsprechung, die die allgemeine und unterschiedslose Vorratsspeicherung von Daten im Bereich elektronischer Kommunikation betrifft, auf die allgemeine und unterschiedslose Erhebung, Übermittlung

und Verarbeitung von Passagierdaten übertragbar ist, wie sie durch das Gesetz vom 25. Dezember 2016 geregelt werden.

B.47.1. In seinem vorerwähnten Gutachten 1/15 vom 26. Juli 2017 hat der Gerichtshof über ein ähnliches PNR-System, das aber einen enger gefassten Anwendungsbereich hat, befunden, denn der Entwurf des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen sah « die systematische und kontinuierliche Übermittlung der PNR-Daten sämtlicher Fluggäste [...], die aus der Union nach Kanada reisen » vor (Randnr. 127).

Der Gerichtshof war der Auffassung, 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 » (Randnr. 153).

In Bezug auf die betroffenen Fluggäste war der Gerichtshof der Auffassung:

« 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, Randnrn. 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 Artikel 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, Randnrn. 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 ».

B.47.2. Es stellt sich jedoch die Frage, ob diese Erwägungen hinsichtlich der PNR-Richtlinie und nationalen Rechtsvorschriften wie dem Gesetz vom 25. Dezember 2016, das zur Umsetzung der PNR-Richtlinie die allgemeine und unterschiedslose Erhebung, Übermittlung und Verwendung von PNR-Daten für sämtliche Passagiere einführt, die per Luftverkehr, Schienenverkehr oder Bus reisen, unabhängig davon, ob sie eine Außengrenze der Union überschreiten, übertragen werden könnten.

Dieses System gilt nämlich für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte (vergl. mit EuGH, Große Kammer, 8. April 2014, C-293/12, *Digital Rights Ireland Ltd*, Randnr. 58) und ist weiter gefasst als das durch das PNR-Abkommen mit Kanada vorgesehene System. In Anbetracht des Umfangs der fraglichen Daten stellt sich die Frage, ob diese Maßnahme sich noch in den Grenzen des « absolut Notwendigen » bewegt.

Vor der Urteilsfällung zur Sache ist folglich dem Gerichtshof der Europäischen Union die im Tenor wiedergegebene vierte Vorabentscheidungsfrage zu stellen.

##### 5. *Die Verarbeitungszwecke der PNR-Daten (Artikel 8)*

B.48. Die klagende Partei bemängelt die in Artikel 8 des Gesetzes vom 25. Dezember 2016 enthaltene Definition der Verarbeitungszwecke der PNR-Daten, die sehr viel umfassender seien als die « spezifischen Zwecke » der PNR-Richtlinie, die allein auf

terroristische Straftaten und schwere Kriminalität beschränkt seien. Sie ist der Ansicht, dass diese Zwecke über das « absolut Notwendige » hinausgehen.

B.49.1. Artikel 1 Absatz 2 der PNR-Richtlinie bestimmt:

« Die nach Maßgabe dieser Richtlinie erhobenen PNR-Daten dürfen ausschließlich zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gemäß Artikel 6 Absatz 2 Buchstaben a, b und c verarbeitet werden ».

Artikel 6 Absatz 2 der PNR-Richtlinie bestimmt:

« 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 ».

Im Erwägungsgrund 7 der PNR-Richtlinie ist weiter erläutert:

« Anhand einer Überprüfung von PNR-Daten können Personen ermittelt werden, die vor einer solchen Überprüfung nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein, und die von den zuständigen Behörden genauer überprüft werden sollten. Durch die Verwendung von PNR-Daten ist es möglich, die Bedrohung durch terroristische Straftaten und schwere Kriminalität anders anzugehen, als dies durch Verarbeitung anderer Kategorien personenbezogener Daten möglich wäre. Damit die Verarbeitung von PNR-Daten jedoch auf das Erforderliche beschränkt bleibt, sollten die Aufstellung und Anwendung von Prüfkriterien auf terroristische Straftaten und schwere Kriminalität, für die die Anwendung solcher Kriterien maßgeblich ist, beschränkt werden. Darüber hinaus sollten die Prüfkriterien so festgelegt werden, dass die Zahl unschuldiger

Personen, die fälschlicherweise vom System identifiziert werden, auf ein Minimum beschränkt wird ».

B.49.2. Die Verarbeitungszwecke der PNR-Daten, wie sie in der PNR-Richtlinie vorgesehen sind, bestehen also ausschließlich in der Zielsetzung der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.

B.49.3. Artikel 3 Nummer 8 der PNR-Richtlinie definiert « terroristische Straftaten » als « die nach nationalem Recht strafbaren Handlungen im Sinne der Artikel 1 bis 4 des Rahmenbeschlusses 2002/475/JI ».

Artikel 3 Nummer 9 der PNR-Richtlinie definiert « schwere Kriminalität » als « die in Anhang II aufgeführten strafbaren Handlungen, die nach dem nationalen Recht eines Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind ».

Anhang II mit der Überschrift « Liste der strafbaren Handlungen gemäß Artikel 3 Nummer 9 » der PNR-Richtlinie bestimmt:

- « 1. Beteiligung an einer kriminellen Vereinigung
- 2. Menschenhandel
- 3. Sexuelle Ausbeutung von Kindern und Kinderpornografie
- 4. Illegaler Handel mit Drogen und psychotropen Stoffen
- 5. Illegaler Handel mit Waffen, Munition und Sprengstoffen
- 6. Korruption
- 7. Betrugsdelikte, einschließlich Betrug zum Nachteil der finanziellen Interessen der Union
- 8. Wäsche von Erträgen aus Straftaten und Geldfälschung, einschließlich Euro-Fälschung
- 9. Computerstraftaten/Cyberkriminalität
- 10. Umweltkriminalität, einschließlich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten

11. Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt
12. Vorsätzliche Tötung, schwere Körperverletzung
13. Illegaler Handel mit menschlichen Organen und menschlichem Gewebe
14. Entführung, Freiheitsberaubung und Geiselnahme
15. Diebstahl in organisierter Form oder mit Waffen
16. Illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen
17. Betrügerische Nachahmung und Produktpiraterie
18. Fälschung von amtlichen Dokumenten und Handel damit
19. Illegaler Handel mit Hormonen und anderen Wachstumsförderern
20. Illegaler Handel mit nuklearen und radioaktiven Substanzen
21. Vergewaltigung
22. Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen
23. Flugzeug- und Schiffsentführung
24. Sabotage
25. Handel mit gestohlenen Kraftfahrzeugen
26. Wirtschaftsspionage ».

B.50.1. In seiner ursprünglichen Fassung lautete Artikel 8 des Gesetzes vom 25. Dezember 2016:

« § 1. Die Passagierdaten werden zu folgenden Zwecken verarbeitet:

1. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 90<sup>ter</sup> § 2 Nr. 1<sup>bis</sup>, 1<sup>ter</sup>, 1<sup>quater</sup>, 1<sup>quinqües</sup>, 1<sup>octies</sup>, 4, 5, 6, 7, 7<sup>bis</sup>, 7<sup>ter</sup>, 8, 9, 10, 10<sup>bis</sup>, 10<sup>ter</sup>, 11, 13, 13<sup>bis</sup>, 14, 16, 17, 18, 19 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten,

2. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 196, was die Fälschung authentischer und öffentlicher Urkunden betrifft, 198, 199, 199<sup>bis</sup>, 207, 213, 375 und 505 des Strafgesetzbuches 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 in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen und in Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung erwähnten Straftaten.

§ 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 ».

Aufgrund von Artikel 13 § 2 des Gesetzes vom 25. Dezember 2016 « darf die PNR-Zentralstelle » unbeschadet anderer gesetzlicher Bestimmungen « die aufgrund von Kapitel 9 aufbewahrten Daten nicht zu anderen als den in Artikel 8 erwähnten Zwecken benutzen ».

B.50.2.1. Wie in B.13 erwähnt, ist Artikel 8 § 1 Nr. 1 und 5 des Gesetzes vom 25. Dezember 2016 außerdem durch Artikel 62 des Gesetzes vom 15. Juli 2018 ersetzt worden.

B.50.2.2. Artikel 62 des Gesetzes vom 15. Juli 2018 ersetzt zunächst Artikel 8 § 1 Nr. 1 des Gesetzes vom 25. Dezember 2016. Ursprünglich waren die « in Artikel 90ter § 2 Nr. 1bis, 1ter, 1quater, 1quinquies, 1octies, 4, 5, 6, 7, 7bis, 7ter, 8, 9, 10, 10bis, 10ter, 11, 13, 13bis, 14, 16, 17, 18, 19 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten » aufgeführt. Seit der Abänderung durch Artikel 62 des Gesetzes vom 15. Juli 2018 sind die « in Artikel 90ter § 2 Nr. 2, 3, 7, 8, 11, 14, 17 bis 20, 22, 24 bis 28, 30, 32, 33, 34, 36 bis 39, 43 bis 45 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten » aufgeführt.

Angesichts dieser Abänderungen ist die Nichtigkeitsklage gegenstandslos geworden, insofern in Artikel 8 § 1 Nr. 1 des Gesetzes vom 25. Dezember 2016 die in Artikel 90ter § 2 Nr. 1bis, 1ter, 1quater, 1quinquies, 1octies, 4, 5, 6, 7bis, 7ter, 9, 10, 10bis, 10ter, 13, 13bis und 16 des Strafprozessgesetzbuches erwähnten Straftaten aufgeführt sind. Hingegen behält die Nichtigkeitsklage ihren Gegenstand, insofern sie sich gegen Artikel 8 § 1 Nr. 1 des Gesetzes vom 25. Dezember 2016 richtet, insoweit in diesem Artikel die in Artikel 90ter § 2

Nr. 7, 8, 11, 14, 17, 18, 19 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten aufgeführt sind.

Die in Artikel 90ter § 2 Nr. 7, 8, 11, 14, 17, 18, 19 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten sind die Straftaten, die in Artikel 210bis des Strafgesetzbuches (Informatikfälschung), in den Artikeln 246, 247, 248, 249 und 250 desselben Gesetzbuches (Korruption von Personen, die ein öffentliches Amt ausüben), in den Artikeln 324bis und 324ter desselben Gesetzbuches (Teilnahme an einer kriminellen Organisation), in Artikel 347bis desselben Gesetzbuches (Geiselnahmen), in den Artikeln 379, 380 und 383bis §§ 1 und 3 desselben Gesetzbuches (Anstiftung Jugendlicher zur Unzucht und Prostitution und Verstoß gegen die guten Sitten), in Artikel 393 desselben Gesetzbuches (Tötung) und in den Artikeln 394 und 397 desselben Gesetzbuches (Totschlag und Vergiftung) aufgeführt sind.

B.50.2.3. Artikel 62 des Gesetzes vom 15. Juli 2018 ersetzt anschließend Artikel 8 § 1 Nr. 5 des Gesetzes vom 25. Dezember 2016. Ursprünglich waren die « in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen und Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung erwähnten Straftaten » aufgeführt. Seit der Abänderung durch Artikel 62 des Gesetzes vom 15. Juli 2018 sind die « Straftaten, erwähnt in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen, in Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung, in Artikel 5 des Gesetzes vom 15. Mai 2007 über die Ahndung der Nachahmung und der Piraterie von geistigen Eigentumsrechten, in Artikel 26 des Dekretes der Deutschsprachigen Gemeinschaft vom 20. Februar 2017 zum Schutz des beweglichen Kulturgutes von außerordentlicher Bedeutung sowie in Artikel 24 des Dekretes der Flämischen Gemeinschaft vom 24. Januar 2003 ‘ houdende bescherming van het roerend cultureel erfgoed van uitzonderlijk belang ’ (Schutz des beweglichen Kulturerbes von außerordentlicher Bedeutung), im Ministeriellen Erlass vom 7. Februar 2012 zur Einführung einer Lizenzpflicht für die Einfuhr von Waren, deren Ursprung oder Herkunft Syrien ist, abgeändert durch den Ministeriellen Erlass vom 1. Juli 2014, im Ministeriellen Erlass vom 23. März 2004 zur Aufhebung des Ministeriellen Erlasses vom 17. Januar 2003 zur Einführung der Pflicht, für die Ein-, Aus- und Durchfuhr von Waren, deren Ursprung, Herkunft oder Bestimmung der Irak ist, über eine vorherige Ermächtigung zu verfügen und für die Ein-, Aus- und Durchfuhr bestimmter Waren, deren Ursprung, Herkunft oder

Bestimmung der Irak ist, über eine Lizenz zu verfügen, sowie Ermittlung der Verstöße, erwähnt in Artikel 5 des Gesetzes vom 28. Juli 1981 zur Billigung des Übereinkommens über den internationalen Handel mit gefährdeten Arten freilebender Tiere und Pflanzen und der Anlagen, abgeschlossen in Washington am 3. März 1973, und der Änderung des Übereinkommens, angenommen in Bonn am 22. Juni 1979 » aufgeführt.

Da die Abänderung von Artikel 8 § 1 Nr. 5 des Gesetzes vom 25. Dezember 2016 durch Artikel 62 des Gesetzes vom 15. Juli 2018 nur den Anwendungsbereich der aufgeführten Straftaten erweitert, behält die Nichtigkeitsklage ihren Gegenstand, insofern sie gegen Artikel 8 § 1 Nr. 5 des Gesetzes vom 25. Dezember 2016 gerichtet ist, insoweit in diesem Artikel die « in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen und Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung erwähnten Straftaten » aufgeführt sind.

Unter diese Straftaten fallen die organisierte oder nicht organisierte schwere Steuerhinterziehung im Rahmen von Verstößen gegen die Rechtsvorschriften über Zölle und Akzisen.

B.50.3. In Bezug auf die an die PNR-Richtlinie angelehnten Zwecke heißt es in der Begründung des Gesetzes vom 25. Dezember 2016:

« L'article 8 détermine limitativement les finalités pour lesquelles le traitement des données des passagers sera autorisé.

Le § 1er concerne les [cinq] finalités qui forment le *corpus* et l'essence même de l'utilisation des données des passagers en vue d'améliorer le niveau de sécurité notamment par une analyse précise, objective et professionnelle du risque et de la menace que peuvent représenter certains passagers.

La première finalité concerne la recherche et la poursuite des infractions graves en ce compris terroristes qui sont inscrites à l'article 90ter, § 2, 1°bis, 1°ter, 1°quater, 1°quinquies, 1°octies, 4°, 5°, 6°, 7°, 7°bis, 7°ter, 8°, 9°, 10°, 10°bis, 10°ter, 11°, 13°, 13°bis, 14°, 16°, 17°, 18°, 19° et § 3 du Code d'instruction criminelle. L'article 90ter du C.i.cr constitue dans notre droit matériel la référence dans le cadre de la prise de connaissance de communications et télécommunications privées mais également dans de nombreuses autres procédures afin de garantir le principe de proportionnalité (par exemple en matière de recherche proactive ou de témoignage anonyme).

La liste limitative de l'article 90<sup>ter</sup> C.i.cr. énumère les infractions graves qui sont à même de menacer gravement la sécurité intérieure et européenne et rejoint dès lors précisément l'objectif du présent projet.

L'exécution des peines et des mesures limitatives de liberté en relation avec lesdites infractions figurent textuellement dans la finalité. Par exemple, un passager est signalé parce qu'il a été condamné, en Belgique, par défaut à 4 ans de prison pour infraction en matière de trafic de stupéfiants et dont l'arrestation immédiate est ordonnée ou dans le cadre d'une mesure de liberté sous conditions dans un dossier lié à un foreign fighter, le juge d'instruction a posé pour condition une interdiction de quitter le territoire.

Cette finalité est judiciaire et relève dès lors des compétences des services de police, des Douanes et des autorités judiciaires.

La deuxième finalité concerne les catégories d'infractions énumérées à l'annexe II de la directive européenne PNR qui ne sont pas inclus[es] dans l'article 90<sup>ter</sup> C.i.cr: falsification de documents administratifs et trafic de faux, viol et trafic de véhicules volés. La référence à l'article 196 du Code pénal porte dès lors sur les écritures authentiques et publiques et n'englobe donc pas les écritures de commerce ou de banque ou écritures privées dont il est question à l'article 196, conformément à la Directive.

Le traitement des données des passagers pour cette finalité est limitée [lire : limité] au traitement des données dans le cadre des recherches ponctuelles comme réglé dans l'article 27 de la loi.

[...]

La cinquième finalité concerne les infractions douane et accises de l'annexe II de la directive européenne PNR : Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 17-20).

B.50.4. Die in Artikel 8 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecke bilden einen erschöpfenden Rahmen für die zulässigen Verarbeitungen von Passagierdaten.

Wie in B.12 erwähnt, ist Artikel 8 des Gesetzes vom 25. Dezember 2016 außerdem im Lichte des Gesetzes vom 30. Juli 2018 auszulegen.

In den in B.12.2 erwähnten Vorarbeiten zum Gesetz vom 30. Juli 2018 ist angegeben, dass die in Artikel 8 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecke in drei Kategorien unterteilt sind:

- die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Straftaten oder die Strafvollstreckung (Artikel 8 § 1 Nrn. 1, 2, 3 und 5 des Gesetzes vom 25. Dezember 2016); diese Verarbeitungen sind in Titel 2 des Gesetzes vom 30. Juli 2018 geregelt;

- die in den Artikeln 7 und 11 des Gesetzes vom 30. November 1998 erwähnten Aufträge der Nachrichten- und Sicherheitsdienste (Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016); diese Verarbeitungen sind in Titel 3 des Gesetzes vom 30. Juli 2018 geregelt;

- die Verbesserung der Personenkontrolle an den Außengrenzen und die Bekämpfung der illegalen Einwanderung (Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016); diese Verarbeitungen sind in Titel 2 des Gesetzes vom 30. Juli 2018 geregelt.

B.51.1. Aus dem in B.50 Erwähnten geht hervor, dass einige der in Artikel 8 des Gesetzes vom 25. Dezember 2016 erwähnten Verarbeitungszwecke den Straftaten in Anhang II der PNR-Richtlinie gemäß den in der Richtlinie genannten Zielen der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität entsprechen (Artikel 8 § 1 Nr. 1, 2 und 5).

Wie in B.40.1 erwähnt, stellt die Verfolgung dieser Ziele durch die Erhebung und Verarbeitung der PNR-Daten eine dem Gemeinwohl dienende Zielsetzung dar, die eine Einmischung in das Recht auf Achtung des Privatlebens und Schutz personenbezogener Daten rechtfertigen kann.

B.51.2. Die zur Bestimmung dieser Zwecke verwendeten Begriffe sind klar und präzise definiert, da sie auf die in den Bestimmungen des Strafgesetzbuches definierten Straftaten verweisen.

Solche Regeln, in denen die Straftaten, die man verhüten, aufdecken und verfolgen möchte, bestimmt werden, sind gemäß den in B.35 genannten Anforderungen klar und präzise und auf das absolut Notwendige beschränkt.

B.52.1. Jedoch kommen einige Verarbeitungszwecke der PNR-Daten zu denjenigen hinzu, die in der PNR-Richtlinie vorgesehen sind. Dies gilt für:

- die « 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 » (Artikel 8 § 1 Nr. 3);

- 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 » (Artikel 8 § 1 Nr. 4);

- die Verbesserung der Personenkontrolle an den Außengrenzen und die Bekämpfung der illegalen Einwanderung (Artikel 8 § 2).

B.52.2. Es ist zu prüfen, ob diese weiteren Zwecke in klaren, präzisen und auf das absolut Notwendige beschränkten Regeln gemäß den in B.35 genannten Anforderungen zum Ausdruck gebracht wurden.

B.53.1. Was den Zweck der Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung betrifft, der in Artikel 8 § 1 Nr. 3 des Gesetzes vom 25. Dezember 2016 erwähnt ist, wird auf die 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 » (nachstehend: Gesetz vom 5. August 1992) Bezug genommen.

Artikel 44/1 des Gesetzes vom 5. August 1992 sieht vor, dass die Polizeidienste im Rahmen der Erfüllung ihrer Aufträge Informationen und personenbezogene Daten verarbeiten können.

Gemäß Artikel 44/2 des Gesetzes vom 5. August 1992 werden diese personenbezogenen Daten und Informationen in einer operativen polizeilichen Datenbank (1. Allgemeine Nationale Datenbank, 2. Basisdatenbanken oder 3. besondere Datenbanken) gemäß den jeweiligen Zwecken der Kategorien der Datenbanken verarbeitet, wenn die Polizeidienste zur Erfüllung der verwaltungspolizeilichen und gerichtspolizeilichen Aufträge diese so strukturieren müssen, dass sie direkt wieder aufgefunden werden können.

Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 bestimmt:

« Die personenbezogenen Daten, die zu verwaltungspolizeilichen Zwecken in den in Artikel 44/2 § 1 Absatz 2 Nr. 1 und 2 erwähnten Datenbanken verarbeitet werden, sind folgende:

[...]

2. Daten in Bezug auf Personen, die von verwaltungspolizeilichen Phänomenen betroffen sind, das heißt von allen Problemen, die eine Störung der öffentlichen Ordnung darstellen und angepasste verwaltungspolizeiliche Maßnahmen notwendig machen, weil sie gleicher Art sind und wiederkehren, von denselben Personen begangen werden oder gegen dieselben Kategorien von Opfern oder Orten gerichtet sind,

3. Daten in Bezug auf Mitglieder einer nationalen oder internationalen Gruppierung, die die in Artikel 14 erwähnte öffentliche Ordnung stören könnten,

[...]

§ 2. Die Liste der in § 1 Nr. 2 erwähnten Phänomene und der in § 1 Nr. 3 erwähnten Gruppierungen wird mindestens jährlich vom Minister des Innern erstellt, auf der Grundlage eines gemeinsamen Vorschlags der föderalen Polizei, des Koordinierungsorgans für die Bedrohungsanalyse und der Nachrichten- und Sicherheitsdienste ».

B.53.2. In Bezug auf den in Artikel 8 § 1 Nr. 3 erwähnten Zweck heißt es in der Begründung:

« La troisième finalité s'inscrit dans le cadre de l'exercice des missions de police administrative des services de police.

Conformément à la loi sur la fonction de police, les services de police peuvent, dans le cadre de l'exercice de leurs missions de police administrative, traiter les données à caractère personnel pour autant qu'elles soient adéquates, pertinentes et non excessives.

Cette finalité spécifique s'inscrit dans une perspective d'approche globale du phénomène lié à la radicalisation violente ayant une incidence directe sur la protection des intérêts défendus par le présent avant-projet de loi.

La Circulaire GPI 78 du 31 janvier 2014 définit le radicalisme violent comme ' un processus par lequel un individu ou un groupe est influencé de sorte que l'individu ou le groupe en question soit mentalement prêt à commettre des actes extrémistes, ces actes allant jusqu'à être violents ou même terroristes '.

Il est essentiel que dans le cadre du suivi du radicalisme ou de groupements y liés présentant une menace grave pour l'ordre public, les données des passagers puissent également être utilisées d'une manière limitée. On peut penser par exemple à la venue sur notre territoire lors d'événements planifiés ou non de membres d'un groupe prônant des thèses extrémistes opposées aux valeurs et principes démocratiques.

L'information traitée à cette occasion doit uniquement servir à prendre des mesures afin de garantir l'ordre public. Si, par exemple, on apprend qu'une trentaine de membres d'un tel groupement a l'intention de se rendre en Belgique pour un rassemblement, des mesures plus adaptées en matière de maintien de l'ordre public pourront être prises (renforcement du dispositif, moyens spéciaux,...).

Dans cette optique, cette finalité est extrêmement limitée dans son application.

En effet, seul le phénomène de la radicalisation violente et les groupements y liés tels que mentionnés dans une liste fermée, établie annuellement par le ministre de l'Intérieur, après avis de la Police fédérale, l'OCAM, et les services de renseignement et de sécurité, peuvent fonder le traitement. Il ne s'agira dès lors pas de traiter les données des passagers pour n'importe quel événement ou menace de trouble à l'ordre public.

En outre, l'article 24, § 3, en projet limite fortement les modes, les conditions de traitement et exclut l'utilisation de profils de risques de cette finalité. L'article 27 exclut la recherche ponctuelle de cette finalité (*cfr infra*) » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 18-19).

Der Minister der Sicherheit und des Innern hat auch erläutert, dass der Begriff der gewalttätigen Radikalisierung « im Sinne des Rundschreibens verstanden werden » muss (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/003, S. 31).

B.53.3. Aus dem Vorstehenden geht hervor, dass der Zweck der Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung auf eine schwerwiegende Bedrohung für die öffentliche Ordnung, die sich aus der gewalttätigen Radikalisierung im Sinne des ministeriellen Rundschreibens GPI 78 vom 31. Januar 2014 « über die Informationsverarbeitung für eine integrierte Vorgehensweise gegen den Terrorismus und die gewalttätige Radikalisierung durch die Polizei » (nachstehend: ministerielles Rundschreiben) ergibt, beschränkt ist.

B.53.4. Bei diesem Zweck findet im Übrigen im Rahmen der Vorabüberprüfung der Passagiere eine eingeschränktere Verarbeitung als bei den anderen Zwecken zur Verhinderung und Ermittlung der in Artikel 8 § 1 des Gesetzes vom 25. Dezember 2016 erwähnten Straftaten statt.

So sieht Artikel 24 § 3 des Gesetzes vom 25. Dezember 2016 vor, dass im Rahmen der in Artikel 8 § 1 Nr. 3 erwähnten Zwecke « die Vorabüberprüfung der Passagiere auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und den in § 2 Nr. 1 erwähnten Datenbanken [beruht] ». Zudem sieht Artikel 26 § 1 des Gesetzes vom 25. Dezember 2016

vor, dass für den in Artikel 8 § 1 Nr. 3 erwähnten Zweck nur die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten (API-Daten), die sich auf die Person(en) beziehen, für die sich ein Treffer ergeben hat, zugänglich sind. Schließlich schließt es Artikel 27 des Gesetzes vom 25. Dezember 2016 aus, dass gezielte Recherchen zu den in Artikel 8 § 1 Nr. 3 erwähnten Zwecken durchgeführt werden.

In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 heißt es:

« Le § 3 de l'article 24 concerne l'évaluation préalable dans le cadre de la finalité relative au suivi des phénomènes de police administrative et des groupements lié à la radicalisation violente.

Cette finalité est soumise à des conditions beaucoup plus restrictives que les autres finalités. L'évaluation préalable dans ce cadre ne peut se baser que sur une corrélation avec les banques de données des services de police. Aucun critère préétabli ne peut être appliqué. Ces conditions limitatives se justifient par le fait que le traitement est généralement lié à l'éventuelle prise de mesure immédiate pour assurer l'ordre public. Il est par exemple indispensable que les services soient informés de la venue sur notre territoire d'une personne figurant sur la liste d'un groupement à suivre. On rappellera à ce sujet que l'établissement de ces listes est soumis à des conditions strictes et que seules les personnes présentant une menace grave pour l'ordre public en lien avec la radicalisation violente s'y retrouvent. La simple participation à une manifestation par exemple antimondialiste ne constitue pas un critère suffisant » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 30).

B.53.5. Zwar sind die Begriffe « Phänomene » und « Gruppierungen » in Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 definiert, aber dies gilt nicht für den Begriff « gewalttätige Radikalisierung », der nicht gesetzlich definiert ist.

Jedoch definiert Artikel 3 Nr. 15 des Grundlagengesetzes vom 30. November 1998 « über die Nachrichten- und Sicherheitsdienste » (nachstehend: Gesetz vom 30. November 1998) den « Radikalisierungsprozess » als einen « Prozess, bei dem ein Individuum oder eine Gruppe von Individuen so beeinflusst wird, dass dieses Individuum beziehungsweise diese Gruppe von Individuen mental darauf vorbereitet ist oder bereit ist, Terrorakte zu begehen ».

Außerdem ist in Artikel 1 des ministeriellen Rundschreibens die « gewalttätige Radikalisierung » wie folgt definiert:

« La radicalisation violente est un processus par lequel un individu ou un groupe est influencé de sorte que l'individu ou le groupe en question soit mentalement prêt à commettre

des actes extrémistes, ces actes allant jusqu'à être violents ou même terroristes. L'adjectif ' violent ' est dans ce cas utilisé pour établir une distinction claire entre d'une part les idées non punissables et leur expression et, d'autre part, les infractions ou actes qui représentent un danger pour la sécurité publique commis pour réaliser ces idées ou l'intention de commettre ces infractions ou actes.

Par violence extrémiste, on entend la violence contre les personnes ou les biens commise par motivation idéologique, politique ou religieuse sans toutefois répondre à la définition pénale du terrorisme ».

Auch wenn der Begriff « gewalttätige Radikalisierung » nicht gesetzlich definiert ist, deutet seine Definition durch das ministerielle Rundschreiben darauf hin, dass er anhand der Begriffe « Phänomene » und « Gruppierungen », die gesetzlich in Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 definiert sind, zu verstehen ist. Einer solchen Maßnahme mangelt es also nicht an Klarheit und Präzision.

B.53.6. Aus dieser Definition wird außerdem ersichtlich, dass die anhand der « Phänomene » und « Gruppierungen » verstandene gewalttätige Radikalisierung im direkten Zusammenhang mit terroristischen Taten oder schwerer Kriminalität steht, die sowohl durch die PNR-Richtlinie als auch durch das Gesetz vom 25. Dezember 2016 verhütet, aufgedeckt und verfolgt werden sollen.

Eine solche Maßnahme ist somit klar und präzise und in Anbetracht der im vorliegenden Fall verfolgten legitimen Zielsetzung nicht unverhältnismäßig.

B.54.1. Gemäß Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 dient die Verarbeitung der PNR-Daten zur Beaufsichtigung der in den Artikeln 7 Nr. 1 und 3/1 und 11 § 1 Nr. 1 bis 3 und 5 des Gesetzes vom 30. November 1998 erwähnten Aktivitäten.

Artikel 7 des Gesetzes vom 30. November 1998 bestimmt:

« Die Staatssicherheit ist beauftragt:

1. Nachrichten in Bezug auf jegliche Aktivität, die die innere Sicherheit des Staates und den Fortbestand der demokratischen und verfassungsmäßigen Ordnung, die äußere Sicherheit des Staates und die internationalen Beziehungen, das vom Nationalen Sicherheitsrat definierte wissenschaftliche oder wirtschaftliche Potential oder jedes andere vom König auf Vorschlag des Nationalen Sicherheitsrats definierte grundlegende Interesse des Landes gefährdet oder gefährden könnte, zu ermitteln, zu analysieren und zu verarbeiten,

[...]

3/1. Nachrichten in Bezug auf die Aktivitäten der ausländischen Nachrichtendienste auf belgischem Staatsgebiet zu ermitteln, zu analysieren und zu verarbeiten,

[...] ».

Artikel 11 § 1 des Gesetzes vom 30. November 1998 bestimmt:

« Der Allgemeine Nachrichten- und Sicherheitsdienst ist beauftragt:

1. Nachrichten in Bezug auf Faktoren, die die nationale und internationale Sicherheit beeinflussen oder beeinflussen können, sofern die Streitkräfte darin verwickelt sind oder sein könnten, indem sie ihre laufenden oder eventuellen zukünftigen Einsätze mit Informationen unterstützen, sowie Nachrichten in Bezug auf jegliche Aktivität, die Folgendes gefährdet oder gefährden könnte, zu ermitteln, zu analysieren und zu verarbeiten:

a) die Integrität des Staatsgebiets oder die Bevölkerung,

b) die militärischen Verteidigungspläne,

c) das wissenschaftliche und wirtschaftliche Potential in Zusammenhang mit den Akteuren, sowohl natürlichen als auch juristischen Personen, die in den mit der Verteidigung verbundenen wirtschaftlichen und industriellen Sektoren tätig sind und die in einer auf Vorschlag des Ministers der Justiz und des Ministers der Landesverteidigung vom Nationalen Sicherheitsrat gebilligten Liste aufgeführt sind,

d) die Erfüllung der Aufträge der Streitkräfte,

e) die Sicherheit von belgischen Staatsangehörigen im Ausland,

f) jedes andere vom König auf Vorschlag des Nationalen Sicherheitsrats definierte grundlegende Interesse des Landes

und die zuständigen Minister unverzüglich davon in Kenntnis zu setzen sowie der Regierung auf Verlangen Stellungnahmen im Hinblick auf die Bestimmung ihrer internen und auswärtigen Sicherheits- und Verteidigungspolitik abzugeben,

2. für die Gewährleistung der militärischen Sicherheit des Personals, das dem Ministerium der Landesverteidigung untersteht, und von militärischen Anlagen, Waffen und Waffensystemen, Munition, Ausrüstung, Plänen, Schriftstücken, Dokumenten, EDV- und Kommunikationssystemen oder anderen militärischen Gegenstände zu sorgen und im Rahmen der Cyberattacken auf Waffensysteme, militärische EDV- und Kommunikationssysteme oder auf die vom Ministerium der Landesverteidigung verwalteten Systeme die Attacke zu neutralisieren und deren Urheber zu identifizieren, unbeschadet des Rechts, sofort unter Einhaltung der Bestimmungen des Rechts des bewaffneten Konflikts mit einer eigenen Cyberattacke zu reagieren,

3. das Geheimnisse zu wahren, das aufgrund der internationalen Verpflichtungen Belgiens oder zur Wahrung der Integrität des Staatsgebiets und zur Erfüllung der Aufträge der Streitkräfte für militärische Anlagen, Waffen, Munition, Ausrüstung, Pläne, Schriftstücke, Dokumente oder andere militärische Gegenstände, militärische Nachrichten und Kommunikationen sowie militärische EDV- und Kommunikationssysteme oder die vom Ministerium der Landesverteidigung verwalteten Systemen geboten ist,

[...]

5. Nachrichten in Bezug auf die Aktivitäten der ausländischen Nachrichtendienste auf belgischem Staatsgebiet zu ermitteln, zu analysieren und zu verarbeiten ».

B.54.2. In der Begründung ist in Bezug auf diesen Zweck angegeben:

« La quatrième finalité a trait aux compétences des services de renseignement, à savoir, la Sûreté de l'État et le Service général de Renseignement et de Sécurité (SGRS). Afin de mener leurs missions de recherche, d'analyse et de traitement des renseignements relatifs aux activités susceptibles de menacer les intérêts fondamentaux de l'État, ces services doivent être en mesure d'analyser les données des passagers afin de détecter le plus tôt possible des menaces concrètes, suivre les déplacements de personnes précises ou d'établir des analyses de phénomènes ou tendances plus larges. Les missions concernant la recherche, l'analyse et le traitement des renseignements relatifs aux activités des services de renseignement étrangers sur le territoire belge entrent dans cette finalité.

La Sûreté de l'État joue un rôle indispensable dans la détection et la surveillance de *foreign fighters* et mais également dans d'autres activités déstabilisantes telles que celles liées aux organisations criminelles ou extrémistes.

Le SGRS exerce notamment des missions en rapport avec la protection de l'intégrité du territoire national, la protection de nos forces armées en mission à l'étranger et à l'égard de la sécurité des Belges à l'étranger.

Enfin, l'action des services de renseignement participe également dans de nombreux cas, à la réponse policière et judiciaire en aval au regard de la première finalité » (ebenda, SS. 19-20).

B.54.3. Zwar tragen die Aufträge der Nachrichten- und Sicherheitsdienste allgemein zur nationalen und internationalen Sicherheit bei, aber die Verarbeitung der PNR-Daten im Rahmen des in Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecks erscheint sehr vage und allgemein.

Dieser Zweck ist zudem im Rahmen der Vorabüberprüfung der Passagiere Gegenstand derselben Verarbeitung wie die Verarbeitung zu den in den Artikeln 8 § 1 Nr. 1, 2 und 5 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecken (Artikel 24 § 2 und Artikel 26 § 2).

B.54.4. Vor diesem Hintergrund ist folglich dem Gerichtshof der Europäischen Union die im Tenor wiedergegebene fünfte Vorabentscheidungsfrage zu stellen, um zu entscheiden, ob dieser Zweck ausreichend klar und präzise und auf das absolut Notwendige beschränkt ist.

B.55.1. Schließlich gestattet es Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016, die PNR-Daten unter den in Kapitel 11 (Artikel 28 bis 31) des Gesetzes vom 25. Dezember 2016 erwähnten Bedingungen zu verarbeiten, um die Personenkontrolle an den Außengrenzen zu verbessern und insbesondere um die illegale Einwanderung zu bekämpfen.

B.55.2. In der Begründung ist in Bezug auf diesen Zweck angegeben:

« La participation des services de police et de l'Office des étrangers dans la gestion des phénomènes de radicalisation violente, des '*foreign fighters*', des '*returnees*' et dans la lutte contre le terrorisme et la grande criminalité, telle que la traite et le trafic d'êtres humains, est nécessaire et incontournable.

[...]

Il est donc primordial que les services de police et l'Office des étrangers puissent utiliser certaines données de passagers dans le cadre du contrôle aux frontières extérieures et sur le territoire ainsi que dans le cadre des procédures de séjour et d'asile.

Ils auront donc accès à certaines données de passagers et ce, pendant une durée limitée. Le but est que les services de police et l'Office des étrangers soient en mesure d'exercer leurs missions légales correctement, tout en garantissant un niveau de protection des données personnelles suffisant au regard des objectifs poursuivis.

La banque de données des passagers constitue un outil indispensable à leur action. Les données de passagers auxquelles ils auront accès ou qui devront leur être transmises sont de nature à les aider à l'accomplissement de leurs tâches, telles que : l'identification des personnes, la vérification de l'authenticité et de la validité des documents ayant servi à entrer en Belgique, à y séjourner ou à quitter le pays (document d'identité, passeport, visas, document ou titre de séjour, billets de transport, etc.), la vérification des déclarations des personnes concernées, la motivation et l'exécution des décisions prises en la matière.

Elles seront donc utilisées dans les procédures de visa, lors des contrôles effectués aux frontières extérieures et sur le territoire, pour le suivi du séjour ou encore pour l'exécution des mesures d'éloignement. Elles pourront servir également dans les procédures d'asile, pour la détermination de l'État responsable de la demande d'asile et pour la prise de décision, y compris pour le retrait du statut de réfugié ou de la protection subsidiaire » (ebenda, SS. 9-10).

« Le paragraphe 2 autorise le traitement des données des passagers en matière de migration et d'asile.

Les autorités compétentes en la matière pourront donc traiter ces données dans l'exercice des missions qui leur sont attribuées, en particulier dans le but d'améliorer le contrôle des frontières et de lutter contre l'immigration illégale.

Ce traitement aura lieu dans les limites fixées prévues au chapitre XI » (ebenda, S. 20).

« Les finalités du traitement des données de passagers sont identiques à celles de la directive 2004/82/CE. Il ressort clairement de ses considérants et de son dispositif qu'elle vise essentiellement le contrôle des flux migratoires, la lutte contre l'immigration illégale, l'amélioration des contrôles aux frontières extérieures et la protection de l'ordre public et de la sécurité nationale » (ebenda, S. 33).

Die Gesetzgebungsabteilung des Staatsrates hat ebenfalls Folgendes bemerkt:

« Les articles 28 et 29, faisant partie du chapitre XI – Du traitement des données des passagers en vue de l'amélioration du contrôle au(x) frontière(s) et de la lutte contre l'immigration illégale, de l'avant-projet, font usage de la notion de ' frontières extérieures ' de la Belgique. Cette notion de frontières extérieures est définie à l'article 2, b), de la directive 2004/82/CE, que transpose plus spécifiquement le chapitre XI de l'avant-projet » (ebenda, S. 97).

B.55.3. Die Verarbeitung der Passagierdaten im Rahmen des in Artikel 8 § 2 erwähnten Zwecks ist in den Artikeln 28 bis 31 des Gesetzes vom 25. Dezember 2016 geregelt.

Nur die in Artikel 9 § 1 Nr. 18 des Gesetzes vom 25. Dezember 2016 erwähnten Passagierdaten werden an die in Artikel 14 § 1 Nr. 2 Buchstabe a) erwähnten Polizeidienste und an das Ausländeramt übermittelt, damit sie ihre gesetzlichen Aufträge ausführen können (Artikel 29). Es sind nur die Passagiere betroffen, die beabsichtigen, über die Außengrenzen Belgiens ins Hoheitsgebiet zu kommen, oder bereits über die Außengrenzen Belgiens ins Hoheitsgebiet gekommen sind (Artikel 29 § 2 Nr. 1) und die Passagiere, die beabsichtigen, das Hoheitsgebiet über die Außengrenzen Belgiens zu verlassen, oder die das Hoheitsgebiet bereits über die Außengrenzen Belgiens verlassen haben (Artikel 29 § 2 Nr. 2) und die Passagiere, die beabsichtigen, sich in einer in Belgien gelegenen internationalen Transitzone aufzuhalten, sich dort aufhalten oder sich dort aufgehalten haben (Artikel 29 § 2 Nr. 3).

Diese Daten werden unmittelbar nach ihrer Speicherung in der Passagierdatenbank an die in Artikel 14 § 1 Nr. 2 Buchstabe a) erwähnten Polizeidienste und an das Ausländeramt, wenn

es sie für die Ausführung seiner gesetzlichen Aufträge benötigt, übermittelt; diese Daten werden in einer temporären Datei aufbewahrt und innerhalb von vierundzwanzig Stunden nach ihrer Übermittlung vernichtet (Artikel 29 §§ 3 und 4). Das Ausländeramt kann außerdem nach Ablauf dieser Frist eine gebührend mit Gründen versehene Anfrage an die PNR-Zentralstelle richten, um auf diese Daten zuzugreifen (Artikel 29 § 4 Absatz 2). Das Ausländeramt übermittelt dem Ausschuss für den Schutz des Privatlebens, nunmehr die Datenschutzbehörde, monatlich einen Bericht über die Anwendung von Artikel 29 § 4 Absatz 2 (Artikel 29 § 4 Absatz 3).

Ein Protokoll in Bezug auf die technischen Sicherungs-, Zugriffs- und Übermittlungsmodalitäten der Passagierdaten an die mit der Grenzkontrolle beauftragten Polizeidienste und an das Ausländeramt muss in Absprache mit dem Datenschutzbeauftragten und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens (Datenschutzbehörde) zwischen dem leitenden Beamten der PNR-Zentralstelle einerseits und dem Generalkommissar der föderalen Polizei und dem leitenden Beamten des Ausländeramtes andererseits für ihren jeweiligen Bereich abgeschlossen werden (Artikel 30).

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, die sie gemäß Artikel 7 übermitteln (Artikel 31 in der durch das Gesetz vom 15. Juli 2018 abgeänderten Fassung).

B.55.4. Aus dem Vorstehenden ergibt sich, dass nur die in Artikel 9 § 1 Nr. 18 des Gesetzes vom 25. Dezember 2016 erwähnten API-Daten bestimmter Passagierkategorien im Hinblick auf den Zweck im Zusammenhang mit der Bekämpfung der illegalen Einwanderung und der Grenzkontrolle, der in Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016 aufgeführt ist, unter den in Kapitel 11 des Gesetzes vom 25. Dezember 2016 erwähnten Bedingungen verarbeitet werden dürfen.

Wie in den in B.55.2 zitierten Vorarbeiten angegeben ist, erfolgt eine solche Maßnahme im Rahmen der Umsetzung der Richtlinie 2004/82/EG, deren Ziel gemäß ihrem Erwägungsgrund 1 darin besteht, die illegale Einwanderung wirksam zu bekämpfen und die Grenzkontrollen zu verbessern. Insbesondere Kapitel 11 des Gesetzes vom 25. Dezember 2016 übernimmt den angepassten Inhalt des königlichen Erlasses vom 11. Dezember 2006

« über die Verpflichtung von Fluggesellschaften, Angaben über die beförderten Personen zu übermitteln », der vor seiner Aufhebung durch den königlichen Erlass vom 18. Juli 2017 die Richtlinie 2004/82/EG in innerstaatliches Recht umsetzte.

B.55.5. Unter Berücksichtigung der verschiedenen in B.55.3 aufgezählten Einschränkungen für die Verarbeitung der Daten im Rahmen des in Artikel 8 § 2 erwähnten Zwecks ist diese Maßnahme ausreichend klar und präzise und auf das absolut Notwendige beschränkt und ist somit nicht unverhältnismäßig.

*6. Die Verwaltung der Passagierdatenbank und die Verarbeitung der Daten im Rahmen der Vorabüberprüfung der Passagiere und der gezielten Recherchen (Artikel 12 bis 16 und 24 bis 27 und 50 und 51)*

B.56. Die klagende Partei ist der Auffassung, dass die verschiedenen Verarbeitungen und Übermittlungen von personenbezogenen Daten offenkundig unverhältnismäßig seien.

Sie bemängelt einerseits die Schaffung der Passagierdatenbank, die von der innerhalb des FÖD Inneres geschaffenen PNR-Zentralstelle verwaltet werde und die Informationen mit den ausländischen PNR-Zentralstellen und Europol austausche. Sie vertritt die Ansicht, dass die Verarbeitung der Passagierdaten nicht die Schaffung einer Datenbank erfordere.

Andererseits bemängelt sie die Korrelation zwischen den Datenbanken und dem « *Pre-Screening* », das anhand von im Voraus festgelegten Kriterien, die als Indikator für eine Bedrohung dienen, durchgeführt werden müsste.

Schließlich bemängelt sie den Umstand, dass die entsandten Mitglieder der zuständigen Dienste über eine Anfrage auf individuellen Zugriff im Rahmen gezielter Recherchen befinden könnten.

B.57.1. Nach Artikel 4 Absatz 1 der PNR-Richtlinie errichtet oder benennt jeder Mitgliedstaat 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.

Gemäß Artikel 4 Absatz 2 der PNR-Richtlinie ist die PNR-Zentralstelle 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 ».

B.57.2. In Bezug auf die Datenverarbeitung bestimmt Artikel 6 der PNR-Richtlinie:

« 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.

3. Bei der Durchführung der in Absatz 2 Buchstabe a genannten Überprüfungen darf die PNR-Zentralstelle

a) die PNR-Daten mit Datenbanken, die zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität maßgeblich sind, einschließlich Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, unter Einhaltung der für

solche Datenbanken einschlägigen nationalen, internationalen und Unionsvorschriften abgleichen; oder

b) die PNR-Daten anhand im Voraus festgelegter Kriterien abgleichen.

4. Die Überprüfung von Fluggästen vor ihrer planmäßigen Ankunft in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat anhand im Voraus festgelegter Kriterien gemäß Absatz 3 Buchstabe b erfolgt in nichtdiskriminierender Weise. Diese im Voraus festgelegten Kriterien müssen zielgerichtet, verhältnismäßig und bestimmt sein. Die Mitgliedstaaten stellen sicher, dass diese Kriterien von der PNR-Zentralstelle aufgestellt und von ihr in Zusammenarbeit mit den in Artikel 7 genannten zuständigen Behörden regelmäßig überprüft werden. Die rassische oder ethnische Herkunft, die politischen Meinungen, die religiösen oder weltanschaulichen Überzeugungen, die Mitgliedschaft in einer Gewerkschaft, der Gesundheitszustand, das Sexualleben oder die sexuelle Orientierung einer Person dürfen unter keinen Umständen als Grundlage für diese Kriterien dienen.

5. Die Mitgliedstaaten stellen sicher, dass jeder einzelne Treffer bei der automatisierten Verarbeitung von PNR-Daten nach Maßgabe von Absatz 2 Buchstabe a auf andere, nicht-automatisierte Art individuell überprüft wird, um zu klären, ob die zuständige Behörde gemäß Artikel 7 Maßnahmen im Einklang mit dem nationalen Recht ergreifen muss.

6. Die PNR-Zentralstelle eines Mitgliedstaats übermittelt die PNR-Daten von nach Absatz 2 Buchstabe a ermittelten Personen oder die Ergebnisse der Verarbeitung dieser Daten zur weiteren Überprüfung an die zuständigen Behörden gemäß Artikel 7 desselben Mitgliedstaats. Derartige Übermittlungen dürfen nur im Einzelfall erfolgen und im Fall einer automatisierten Verarbeitung der PNR-Daten nur nach einer individuellen Überprüfung auf andere, nicht-automatisierte Art.

7. Die Mitgliedstaaten stellen sicher, dass der Datenschutzbeauftragte Zugang zu sämtlichen von der PNR-Zentralstelle verarbeiteten Daten erhält. Wenn der Datenschutzbeauftragte der Auffassung ist, dass eine Verarbeitung von Daten nicht rechtmäßig war, kann er die Angelegenheit an die nationale Kontrollstelle verweisen.

8. Die Speicherung, Verarbeitung und Auswertung von PNR-Daten durch die PNR-Zentralstelle erfolgt ausschließlich an einem gesicherten Ort bzw. gesicherten Orten im Hoheitsgebiet der Mitgliedstaaten.

9. Das Recht zur Einreise von Personen, die im Hoheitsgebiet des betreffenden Mitgliedstaats gemäß der Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates das Unionsrecht auf freien Personenverkehr genießen, darf von den Auswirkungen der Überprüfungen von Fluggästen gemäß Absatz 2 Buchstabe a dieses Artikels nicht beeinträchtigt werden. Darüber hinaus müssen, wenn Überprüfungen in Bezug auf EU-Flüge zwischen Mitgliedstaaten vorgenommen werden, für die die Verordnung (EG) Nr. 562/2006 des Europäischen Parlaments und des Rates gilt, die Auswirkungen solcher Überprüfungen mit der genannten Verordnung im Einklang stehen ».

*a) Die Verwaltung der Passagierdatenbank durch die PNR-Zentralstelle (Artikel 12 bis 16)*

B.58.1. Nach Artikel 5 des Gesetzes vom 25. Dezember 2016 erhebt und übermittelt jedes Beförderungsunternehmen und Reiseunternehmen die Daten zu den in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet beförderten Passagieren, über die es verfügt, damit sie in der in Artikel 15 erwähnten Passagierdatenbank gespeichert werden. Aufgrund von Artikel 6 des Gesetzes vom 25. Dezember 2016 teilen die Beförderungsunternehmen und Reiseunternehmen den betreffenden Personen mit, dass ihre Daten der PNR-Zentralstelle übermittelt werden und später zu den in Artikel 8 erwähnten Zwecken verarbeitet werden können.

Diese Passagierdatenbank wird von der PNR-Zentralstelle verwaltet, die innerhalb des Föderalen Öffentlichen Dienstes Inneres geschaffen wird (Artikel 12). Die PNR-Zentralstelle ist verantwortlich für die Erhebung, Aufbewahrung und Verarbeitung der Passagierdaten sowie die Verwaltung der Passagierdatenbank und den Austausch der Daten und Ergebnisse ihrer Verarbeitung mit den PNR-Zentralstellen anderer Mitgliedstaaten der Europäischen Union und Europol (Artikel 13). Die PNR-Zentralstelle setzt sich zusammen aus einem leitenden Beamten, dem ein Unterstützungsdienst beisteht, und entsandten Mitgliedern der zuständigen Dienste (Artikel 14).

B.58.2. Gemäß Artikel 15 § 1 des Gesetzes vom 25. Dezember 2016 wird eine vom Föderalen Öffentlichen Dienst Inneres verwaltete Passagierdatenbank geschaffen, in der die Passagierdaten gespeichert werden. Der leitende Beamte der PNR-Zentralstelle ist der für die Verarbeitung Verantwortliche der Passagierdaten im Sinne von Artikel 1 § 4 des Gesetzes vom 8. Dezember 1992 « über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten » (Artikel 15 § 2).

Die aufgrund des vorliegenden Gesetzes vorgenommenen Verarbeitungen der Passagierdaten unterliegen dem vorerwähnten Gesetz vom 8. Dezember 1992 (Artikel 15 § 4).

Im Rahmen der in Artikel 8 § 1 erwähnten Zwecke ist die Passagierdatenbank der PNR-Zentralstelle direkt zugänglich für die in den Artikeln 24 bis 27 erwähnten Verarbeitungen gemäß den Bestimmungen von Kapitel 9 (Artikel 16). In Kapitel 9 des

Gesetzes vom 25. Dezember 2016, das die Artikel 18 bis 23 umfasst, sind die Aufbewahrungsfristen der Passagierdaten vorgesehen.

Ein Vereinbarungsprotokoll, das der Umsetzung der technischen Sicherungs- und Zugriffsmodalitäten dient, wird vom leitenden Beamten der PNR-Zentralstelle und den zuständigen Diensten nach Absprache mit dem Datenschutzbeauftragten und nach Stellungnahme der für die Aufsicht über die Verarbeitung personenbezogener Daten zuständigen Behörde abgeschlossen (Artikel 17, ersetzt durch das Gesetz vom 15. Juli 2018).

B.58.3. In Bezug auf die Schaffung der Passagierdatenbank ist in den Vorarbeiten erläutert:

« Le premier paragraphe prévoit la création d'une Banque de données des passagers. En effet, pour traiter et analyser les données des passagers visées à l'article 9, il est nécessaire de les traiter dans une banque de données spécifique, afin de pouvoir les structurer, les exploiter et les détruire après un délai déterminé.

Étant donné que le but ultime du traitement des données consiste à assurer la sécurité des citoyens, la banque de données est gérée par le SPF Intérieur. Le fonctionnaire dirigeant est désigné comme responsable du traitement de cette banque de données tel que visé à l'article 1er, § 4, de la Loi sur la Protection des données à caractère personnel. Il sera par conséquent responsable, dans le cadre établi par la loi, de la rédaction et du suivi des plans stratégiques pour le traitement des données et déterminera les moyens nécessaires pour atteindre ses objectifs stratégiques » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 24).

B.59.1. Durch die Schaffung einer Passagierdatenbank, mit deren Verwaltung die PNR-Zentralstelle beauftragt ist, regelt das Gesetz vom 25. Dezember 2016 eine zentrale Speicherung der Passagierdaten unter der Verantwortung der PNR-Zentralstelle mit zahlreichen Garantien in Bezug auf die Sicherung, den Zugriff auf und die Speicherung von diesen Daten und indem die Datenverarbeitungen, die von der PNR-Zentralstelle im Rahmen der in Artikel 8 § 1 erwähnten Zwecke vorgenommen werden dürfen, eingeschränkt werden. Durch die präzise Benennung des Speicherortes dieser Daten ermöglicht es die Schaffung einer solchen Datenbank, den Datenfluss zu begrenzen.

Auch wenn sie nicht ausdrücklich durch die PNR-Richtlinie vorgesehen ist, stellt die Schaffung einer Passagierdatenbank, die mit den in B.58 genannten Garantien versehen ist,

ein wesentliches Element des Systems dar, das durch die PNR-Richtlinie, die das Gesetz vom 25. Dezember 2016 umsetzt, eingeführt wurde.

B.59.2. In Anbetracht des Vorstehenden und der verschiedenen in B.58 aufgezählten Garantien, die den Rahmen für die Schaffung und Verwaltung der Passagierdatenbank bilden, ist diese Maßnahme nicht unverhältnismäßig.

*b) Die Verarbeitung von Passagierdaten im Rahmen der Vorabüberprüfung der Passagiere (Artikel 24 bis 26)*

B.60.1. Artikel 16 des Gesetzes vom 25. Dezember 2016 sieht vor, dass die Passagierdaten im Rahmen der in Artikel 8 § 1 erwähnten Zwecke Gegenstand der in den Artikeln 24 bis 27 erwähnten Verarbeitungen sind.

Die Artikel 24 bis 26 betreffen die Verarbeitung von Passagierdaten im Rahmen der Vorabüberprüfung der Passagiere.

B.60.2. Gemäß Artikel 24 § 1 des Gesetzes vom 25. Dezember 2016 werden die Passagierdaten 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 (Artikel 24 § 1).

In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 heißt es:

« L'article 24 concerne l'évaluation (pré-screening) du risque représenté par les passagers. Il s'agit d'évaluer la menace potentielle et de déterminer quels passagers présentent un intérêt pour l'exercice de leurs missions ou par exemple nécessitent une mesure à prendre (exécution d'un mandat d'arrêt, fouille,...).

Cette évaluation préalable s'applique avant l'arrivée, le transit ou le départ du territoire national » (ebenda, S. 28).

B.60.3.1. Die Vorabüberprüfung erfolgt auf zwei Wegen: einerseits die Korrelation der Passagierdaten mit den Datenbanken und andererseits die Korrelation der Daten mit im Voraus festgelegten Kriterien.

Diese Überprüfung beruht auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und:

- den von den zuständigen Diensten verwalteten Datenbanken und den von der PNR-Zentralstelle im Voraus festgelegten Überprüfungskriterien im Rahmen der Zwecke, die in Artikel 8 § 1 Nr. 1, 2, 4 und 5 erwähnt sind oder sich auf Bedrohungen beziehen, die in den Artikeln 8 Nr. 1 Buchstabe *a)*, *b)*, *c)*, *d)*, *f)*, *g)* und 11 § 2 des Gesetzes vom 30. November 1998 aufgeführt sind (Artikel 24 § 2, ersetzt durch das Gesetz vom 15. Juli 2018); für diese Zwecke sind alle in Artikel 9 erwähnten Passagierdaten zugänglich (Artikel 26 § 2, ersetzt durch das Gesetz vom 15. Juli 2018);

- den von den zuständigen Diensten verwalteten Datenbanken im Rahmen der in Artikel 8 § 1 Nr. 3 erwähnten Zwecke (Artikel 24 § 3). Für diesen Zweck sind nur die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, die sich auf die Person(en) beziehen, für die sich ein Treffer ergeben hat, zugänglich (Artikel 26 § 1).

Der Treffer wird innerhalb von vierundzwanzig Stunden nach Eingang der automatisierten Mitteilung des Treffers von der PNR-Zentralstelle validiert (Artikel 24 § 4). Ab dieser Validierung sorgt der zuständige Dienst, von dem der Treffer herkommt, schnellstmöglich für die weitere Bearbeitung (Artikel 24 § 5).

Schließlich wurde Artikel 24 § 2 des Gesetzes vom 25. Dezember 2016 aufgrund von Artikel 5 des Gesetzes vom 2. Mai 2019 durch einen neuen Absatz ergänzt. Mit dieser Abänderung « soll in Artikel 24 § 2 vorgesehen werden, dass die Vorabüberprüfung der Passagiere ebenfalls auf einer Analyse der anderen Passagierdaten im Zusammenhang mit einem Treffer beruht » (*Parl. Dok.*, Kammer, 2018-2019, DOC 54-3652/001, S. 5).

B.60.3.2. Bezüglich der Korrelation mit den Datenbanken heißt es in den Vorarbeiten zum Gesetz vom 25. Dezember 2016:

« Le premier axe consiste en la recherche de correspondances positives par le biais de corrélations des données de passagers avec les données traitées dans les banques de données gérées par les services compétents. Cela permet par exemple d'évaluer si une personne présente un degré élevé de dangerosité, car elle est connue dans une banque de données policière dans le cadre d'un dossier terroriste et pour laquelle il appert de l'analyse de ses données passager, que cette dernière se rend régulièrement dans des pays abritant des camps d'entraînement pour terroristes ou dans des pays de transit vers de tels lieux. Il peut par exemple s'agir également d'une personne à propos de laquelle des renseignements disponibles auprès des services de renseignements indiquent qu'elle préparerait une prise d'otage et qu'elle se rend, sur la base des données de transport, dans un pays dont les services de renseignements savent, sur base des informations reçues, que cette personne pourrait y recruter afin de mettre ses plans à exécution. En outre, plus les correspondances positives découvertes par plusieurs services sont nombreuses pour une seule et même personne, plus la probabilité de menace est réelle.

La correspondance positive peut également requérir la prise d'une mesure sur ordre des autorités judiciaires, telle que l'exécution d'un mandat d'arrêt d'une personne qui s'apprête à quitter la Belgique.

La correspondance positive peut également ressortir d'une corrélation avec des banques de données internationale telles que SIS II, Interpol (SLTD).

L'objectif n'est naturellement pas de lier l'ensemble des banques de données des services avec la banque de données des passagers mais bien de limiter techniquement les corrélations avec les banques de données en relation directe avec les finalités telles que déterminées par la loi.

[...]

Cette corrélation pourra également se faire via des listes de personnes élaborées spécifiquement par les services compétents à cette fin. Conformément à la loi sur la protection de la vie privée et plus particulièrement, à son article 4, § 1er, 4°, ces listes devront être mises à jour régulièrement » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 28-29).

Bezüglich der Korrelation mit den im Voraus festgelegten Kriterien heißt es in den Vorarbeiten zum Gesetz vom 25. Dezember 2016:

« Le deuxième axe consiste en la recherche de correspondances positives par le biais de critères préétablis par l'UIP (un ou plusieurs) appliqués aux données des passagers. Ces critères sont composés d'un ou de plusieurs indicateurs objectifs sur la base desquels il peut être déduit que les personnes qui en font l'objet, présentent un comportement à risque spécifique susceptible de constituer une menace au regard des finalités à l'article 8, § 1er, points 1, 4 et 5, de la loi.

Ces critères peuvent intégrer, par exemple, certains comportements spécifiques en matière de réservation ou de voyage.

Leur utilisation présente l'avantage de pouvoir faire émerger des profils de passagers à risque qui ne sont pas nécessairement connus ou mentionnés dans les banques de données des services.

Ces critères peuvent concerner, par exemple, un pays de destination ou de départ, combiné à certaines informations sur le voyage telles que le mode de paiement et la date de réservation » (ebenda, SS. 29-30).

« L'évaluation préalable réalisée dans le cadre de la finalité relative au suivi des phénomènes de police administrative et des groupements lié à la radicalisation violente est soumise à des conditions beaucoup plus restrictives que les autres finalités :

- elle ne peut se baser que sur une corrélation avec les banques de données des services de police;
- Seules les données visées à l'article 9, § 1er, 18° de la loi sont accessibles.

L'évaluation préalable réalisée dans le cadre des autres finalités se voit autoriser l'accès à toutes les données des passagers énumérées à l'article 9 » (ebenda, S. 31).

« La correspondance positive doit dans tous les cas être validée par l'UIP. En effet, pour assurer le respect total du droit à la protection des données personnelles, et plus précisément de l'article 12*bis* de la loi sur la vie privée et le droit à la non-discrimination, aucune décision aux conséquences juridiques pour une personne ou susceptible de la préjudicier gravement ne peut être prise, sur la simple base du traitement automatisé des données du fichier contenant des informations sur son voyage. C'est pourquoi l'évaluation humaine précédera toujours toute décision contraignante pour la personne concernée.

Cette validation doit intervenir dans les 24 heures afin d'ouvrir le droit d'accès à la banque de données des passagers.

§ 5. Après la validation de la correspondance positive, les services qui sont à l'origine de cette correspondance assurent le suivi utile dans un délai approprié. Un suivi utile pourrait signifier une intervention active (fouille, arrestation ...), mais il peut aussi s'agir de n'entreprendre provisoire aucune intervention active. Cette appréciation opérationnelle appartient pleinement aux services compétents » (ebenda, SS. 30-31).

B.60.4.1. In Bezug auf die im Voraus von der PNR-Zentralstelle festgelegten Überprüfungskriterien sieht Artikel 25 des Gesetzes vom 25. Dezember 2016 vor, dass für diese Kriterien nicht Daten als Grundlage dienen dürfen, 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 (Artikel 25 § 3).

Die Überprüfung der Passagiere vor ihrer Ankunft, ihrer Durchreise oder ihrer Abreise anhand im Voraus festgelegter Kriterien erfolgt in nichtdiskriminierender Weise. Diese Kriterien dürfen nicht darauf abzielen, eine Person zu identifizieren, und müssen zielgerichtet, verhältnismäßig und bestimmt sein (Artikel 25 § 2).

Die Passagierdaten können von der PNR-Zentralstelle zwecks Aktualisierung der Kriterien oder Aufstellung neuer Kriterien benutzt werden, die dazu bestimmt sind, bei den Vorabüberprüfungen der Passagiere Einzelpersonen ins Visier zu nehmen (Artikel 25 § 1).

B.60.4.2. In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 wurde diesbezüglich dargelegt:

« Sur le plan technique, pour toutes les modalités de consultation, un principe uniforme de traitement est applicable : sur la base d'une corrélation avec un profil de risque opérationnel ou avec une banque de données ou sur la base d'une requête ponctuelle introduite par un service compétent, des ' hits ' sont générés à l'égard d'une entrée PNR unique. Ce *hit* est uniquement visible pour le service en question. Chaque hit doit être validé manuellement par le membre détaché issu du service compétent concerné pour être traduit dans un ' match '.

Dès qu'une correspondance positive est validée, un code d'encryptions est automatiquement généré qui sera croisé, aux codes de tous les services compétents. Si les deux codes coïncident, deux ou plusieurs services sont informés que des ' correspondances positives ' existent pour cette unique entrée PNR. Ces services doivent assurer le suivi utile dans un délai approprié » (ebenda, S. 23; siehe ebenfalls *Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/003, S. 7).

« L'Article 25 détermine le troisième mode de traitement des données : l'UIP traite les données des passagers pour mettre à jour ou définir de nouveaux critères qui doivent être utilisés lors des évaluations préalables des passagers afin d'objectiver l'évaluation et, par conséquent, d'opérer une sélection rigoureuse des seuls passagers à risque.

Étant donné que le traitement des données des passagers implique une ingérence dans leur vie privée, la garantie d'une objectivation des critères prédéterminés permettra également de garantir le caractère adéquat, pertinent et non excessif de l'ingérence dans la vie privée.

Les critères préétablis doivent être ciblés, proportionnés et spécifiques. En outre, ils ne peuvent viser l'identification d'un individu en particulier. Par conséquent, il est précisé qu'ils ne sont pas nominatifs.

Il ne peuvent en aucun cas être fondés sur des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance à un syndicat, l'état de santé, la vie sexuelle ou l'orientation sexuelle de l'intéressé » (ebenda, S. 31).

B.60.4.3. In Bezug auf die im Voraus festgelegten Überprüfungskriterien verlangt Artikel 6 Absatz 4 der PNR-Richtlinie, dass diese im Voraus festgelegten Kriterien « zielgerichtet, verhältnismäßig und bestimmt » sein müssen und dass die Mitgliedstaaten sicherstellen, dass diese Kriterien « von der PNR-Zentralstelle aufgestellt und von ihr regelmäßig überprüft werden ».

B.61.1. Das System der Vorabüberprüfung bedeutet, dass die PNR-Daten aller Passagiere mit Datenbanken oder im Voraus festgelegten Kriterien abgeglichen werden, um Treffer festzustellen.

In seiner Stellungnahme vom 19. August 2016 über die datenschutzrechtlichen Auswirkungen der Verarbeitung von Passagierdaten hat der Beratende Ausschuss für das Übereinkommen Nr. 108 des Europarates « zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten » diesbezüglich angemerkt:

« Le traitement des données à caractère personnel peut concerner tous les passagers et pas seulement les individus ciblés soupçonnés d'être impliqués dans une infraction pénale ou de constituer une menace immédiate à la sécurité nationale ou à l'ordre public.

Les données PNR peuvent être comparées (‘ data matching ’) à des bases de données (à savoir, des bases sur les personnes condamnées pour infractions pénales graves, les personnes visées par une enquête pour soupçon d'activités terroristes, les passeports volés ou perdus) tenues par les autorités compétentes conformément à la loi afin d'identifier les suspects ou auteurs d'infractions ainsi que les personnes liées à ces suspects ou auteurs d'infractions potentiels (« graphe social »).

Les données PNR peuvent aussi être traitées dans le but d'identifier (par ‘ data mining ’) quiconque ‘ pourrait ’ être impliqué ou s'engager dans les activités criminelles définies par la loi qui établit le partage des PNR avec les autorités compétentes comme, par exemple, les individus voyageant dans le but de devenir des combattants terroristes étrangers. Cela pourrait être obtenu par l'exploration de données selon des sélecteurs ou des algorithmes prédictifs.

L'évaluation des passagers par la mise en correspondance de données peut soulever la question de la prévisibilité, en particulier lorsqu'elle est effectuée sur la base d'algorithmes prédictifs utilisant des critères dynamiques susceptibles d'évoluer en permanence selon les capacités d'auto-apprentissage.

Le développement d'algorithmes d'exploration de données devrait se fonder sur les résultats d'évaluations régulières de l'impact probable du traitement de données sur les droits et libertés fondamentales des personnes concernées.

La structure de base des analyses devrait se fonder sur des indicateurs de risque prédéfinis ayant été clairement établis au préalable.

La pertinence des résultats individuels de ces évaluations automatiques devrait être examinée avec soin au cas par cas, par une personne et de façon non automatisée » (Stellungnahme vom 19. August 2016, T-PD(2016)18rev, S. 8).

B.61.2. Im vorliegenden Fall sind die in Artikel 24 erwähnten Datenbanken präzise und im direkten Zusammenhang mit den in Artikel 8 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecken definiert. Es handelt sich nämlich um Datenbanken der « zuständigen Dienste », das heißt der Polizeidienste, der Staatssicherheit, des Allgemeinen Nachrichten- und Sicherheitsdienstes und des Zolldienstes.

B.61.3. Zudem garantiert Artikel 24 §§ 4 und 5 des Gesetzes vom 25. Dezember 2016, dass die automatisierte systematische Verarbeitung im Fall eines Treffers Gegenstand einer individuellen Überprüfung auf nicht automatisierte Art ist, um zu klären, ob die zuständige Behörde Maßnahmen im Einklang mit dem nationalen Recht ergreifen muss, wie es Artikel 6 Absatz 5 der PNR-Richtlinie erfordert.

In seinem Gutachten 1/15 vom 26. Juli 2017 hatte der Gerichtshof der Europäischen Union ebenfalls auf die Notwendigkeit einer individuellen Überprüfung mit nicht automatisierten Mitteln, bevor eine individuelle Maßnahme getroffen wird, hingewiesen (EuGH, Große Kammer, 26. Juli 2017, Gutachten 1/15, Randnr. 173).

Die Anforderung eines menschlichen Eingreifens nach einem Treffer stellt eine Garantie dar, mit der sichergestellt werden kann, dass die Vorabüberprüfung nicht nur auf automatisierten Mitteln beruht, was zur Wirksamkeit des Systems beiträgt.

Eine systematische Vorabüberprüfung der Passagiere stellt somit im Prinzip eine sachdienliche Maßnahme im Hinblick auf das Ziel, Bedrohungen für die öffentliche Sicherheit zu erkennen und zu verhindern, dar.

B.61.4. Wie der Gerichtshof jedoch in seinem vorerwähnten Gutachten 1/15 vom 26. Juli 2017 festgestellt hat, können durch die sich aus Vorabüberprüfungen ergebenden Verarbeitungen « weitere Informationen über das Privatleben der Fluggäste erlangt werden » (EuGH, Große Kammer, 26. Juli 2017, Gutachten 1/15, Randnr. 131); « die Analysen werden

zudem durchgeführt, ohne dass konkrete Anhaltspunkte dafür vorliegen, dass von den betreffenden Personen eine Gefahr für die öffentliche Sicherheit ausgehen könnte » (ebenda, Randnr. 132).

Nach der Feststellung, dass die automatisierte Verarbeitung von PNR-Daten, die auf im Voraus festgelegten Modellen und Kriterien beruht, eine erhebliche Fehlerquote aufweist (ebenda, Randnrn. 169-170), war der Gerichtshof jedoch der Auffassung, 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] » (ebenda, Randnr. 172). Um zu gewährleisten, dass diese Überprüfung nicht diskriminierend ist und sich auf das absolut Notwendige beschränkt, war der Gerichtshof schließlich der Ansicht, 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] », das heißt ein Jahr nach dessen Inkrafttreten und danach in regelmäßigen Abständen (ebenda, Randnr. 174).

B.61.5. Im Übrigen erscheint es technisch unmöglich, die im Voraus festgelegten Kriterien, die zur Festlegung von Risikoprofilen dienen, näher zu definieren. Wie in B.61.4 erwähnt, müssen diese Kriterien bestimmt, zuverlässig und nicht diskriminierend sein.

Auch wenn weder die PNR-Richtlinie noch das Gesetz vom 25. Dezember 2016 Angaben dazu enthalten, wie die Kriterien, die der Vorabüberprüfung zugrunde liegen, durch die PNR-Zentralstelle im Voraus festgelegt werden, scheinen die in B.60.4 aufgeführten Garantien, die für die Ausarbeitung dieser Kriterien gelten, ausreichend, damit die angefochtene Maßnahme nicht als unverhältnismäßig anzusehen ist.

B.61.6. Dem Gerichtshof der Europäischen Union ist jedoch die im Tenor wiedergegebene sechste Vorabentscheidungsfrage zu stellen, damit entschieden wird, ob diese

systematische Vorabüberprüfung ausreichend klar und präzise und auf das absolut Notwendige beschränkt ist.

*c) Die gezielten Recherchen (Artikel 27, 50 und 51)*

B.62.1. In Artikel 27 des Gesetzes vom 25. Dezember 2016 in seiner ursprünglichen Fassung wird die Verarbeitung von Passagierdaten gestattet, um gezielte Recherchen zu den in Artikel 8 § 1 Nr. 1, 2, 4 und 5 erwähnten Zwecken und unter den in Artikel 46septies des Strafprozessgesetzbuches oder in Artikel 16/3 des Gesetzes vom 30. November 1998 vorgesehenen Bedingungen durchzuführen, die jeweils durch die Artikel 50 und 51 des Gesetzes vom 25. Dezember 2016 eingefügt wurden.

Gemäß Artikel 20 des Gesetzes vom 25. Dezember 2016 gelten die Anwendungsbedingungen von Artikel 27 ebenfalls für Zugriffsanfragen nach der in Artikel 19 vorgesehenen sechsmonatigen Frist.

B.62.2. Artikel 46septies des Strafprozessgesetzbuches, eingefügt durch Artikel 50 des Gesetzes vom 25. Dezember 2016, bestimmt:

« 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.

Die Begründung spiegelt die Verhältnismäßigkeit unter Berücksichtigung des Privatlebens und die Subsidiarität gegenüber jeder anderen Ermittlungsaufgabe wider.

Die Maßnahme kann eine Gesamtheit von Daten in Bezug auf eine spezifische Ermittlung betreffen. In diesem Fall bestimmt der Prokurator des Königs die Dauer der Maßnahme, die einen Monat ab dem Beschluss nicht überschreiten darf, unbeschadet einer Erneuerung.

In Fällen äußerster Dringlichkeit kann jeder Gerichtspolizeioffizier mit der mündlichen und vorherigen Zustimmung des Prokurators des Königs durch einen mit Gründen versehenen schriftlichen Beschluss den leitenden Beamten der PNR-Zentralstelle auffordern, die Passagierdaten mitzuteilen. Der Gerichtspolizeioffizier teilt dem Prokurator des Königs

diesen mit Gründen versehenen schriftlichen Beschluss sowie die erhaltenen Informationen binnen vierundzwanzig Stunden mit und begründet außerdem die äußerste Dringlichkeit ».

Diese Bestimmung betrifft also gezielte Recherchen im Rahmen des in Artikel 8 § 1 Nr. 1, 2, und 5 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecks. Diese Maßnahme ist mit mehreren Garantien versehen, darunter die vorherige Zustimmung des Prokurators des Königs.

B.62.3. Artikel 16/3 des Gesetzes vom 30. November 1998, eingefügt durch Artikel 51 des Gesetzes vom 25. Dezember 2016, bestimmt:

« § 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.

§ 2. Der in § 1 erwähnte Beschluss wird von einem Dienstleiter gefasst und der in Kapitel 7 des vorerwähnten Gesetzes erwähnten PNR-Zentralstelle schriftlich übermittelt. Der Beschluss wird zusammen mit seiner Begründung dem Ständigen Ausschuss N notifiziert.

Der Ständige Ausschuss N verbietet den Nachrichten- und Sicherheitsdiensten, die gesammelten Daten unter Bedingungen zu benutzen, die die gesetzlichen Bedingungen nicht einhalten.

Der Beschluss kann eine Gesamtheit von Daten in Bezug auf eine spezifische nachrichtendienstliche Untersuchung betreffen. In diesem Fall wird dem Ständigen Ausschuss N einmal pro Monat die Liste der Abfragen der Passagierdaten übermittelt ».

Diese Bestimmung betrifft also gezielte Recherchen im Rahmen des in Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecks. Diese Maßnahme ist mit mehreren Garantien versehen, darunter die Information und Kontrolle des Ständigen Ausschusses N.

B.62.4. In Bezug auf die gezielten Recherchen heißt es in den Vorarbeiten zum Gesetz vom 25. Dezember 2016:

« L'article 27 détermine le mode de traitement qui consiste pour l'UIP à réagir au cas par cas aux demandes dûment motivées d'autorités compétentes visant à obtenir des données de passagers et le traitement de celles-ci dans des cas spécifiques. Ce mode de traitement est limité à quatre finalités et exclut celle liée au suivi des phénomènes de police administrative et des membres d'un groupement telle que prévue à l'article 8, § 1er, point 3.

L'hypothèse implique, selon les services, qu'un dossier d'enquête ou de renseignement est ouvert à la suite d'une évaluation préalable positive ou sur la base d'autres éléments concrets indépendants des données des passagers.

Par exemple, sur le plan policier, une enquête pénale est ouverte suite à une fouille positive d'un passager en possession de stupéfiants résultant d'une évaluation préalable ou suite à un contrôle de véhicule ou de personne sur la voie publique. Dans les deux cas, il peut s'avérer nécessaire de consulter les données des passagers ' rétroactivement ' pour les besoins de l'enquête afin de retracer les éventuels déplacements du suspect.

La consultation de la banque de données des passagers ne se fera plus ici à proprement parler sur la base des critères préétablis ou d'une corrélation automatique mais sur la base de recherches à l'aide d'éléments issus du dossier. Par exemple, un nom, le n° de passeport du suspect, n° de GSM, destination,...

Dans ce cadre, la nécessité de pouvoir remonter à un historique des données des passagers est plus cruciale encore compte tenu de la durée et complexité de certaines enquêtes, voire de la découverte d'infractions bien plus tard après les déplacements. C'est pour cette raison que les données doivent être accessibles sur une période de 5 ans afin de recueillir des preuves, de trouver d'éventuels co-auteurs ou complices et de démanteler des réseaux criminels.

Exemple : suite à de nouveaux éléments dans une enquête terrorisme, le magistrat traitant estime devoir consulter certaines données de voyage de suspects identifiés.

L'autorisation du procureur du Roi sera nécessaire à tout moment pour accéder à toutes les informations, y compris celles qui ont été masquées en ce qui concerne les finalités de l'article 8, § 1er, 1°, 2° et 5°. En ce qui concerne la finalité de l'article 8, § 1er, 4°, l'autorisation par le dirigeant du service comme requise dans l'article 51 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 32-33).

« Les articles 50 et 51 concernent les dispositions modifiant le Code d'instruction criminelle et la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et relatives aux modalités d'accès aux données des passagers dans le cadre de l'analyse a posteriori » (ebenda, S. 43).

B.63.1. Die klagende Partei führt an, dass die entsandten Mitglieder der Polizeidienste, die der PNR-Zentralstelle angehören, nicht ausreichend unabhängig seien, um auf die Zugriffsanfragen im Rahmen dieser gezielten Recherchen zu antworten.

B.63.2. Nach Artikel 14 § 1 des Gesetzes vom 25. Dezember 2016 setzt sich die PNR-Zentralstelle zusammen aus einem leitenden Beamten, dem ein Unterstützungsdienst beisteht, (Artikel 14 § 1 Nr. 1) sowie aus entsandten Mitgliedern, die aus den Polizeidiensten, der Staatssicherheit, dem Allgemeinen Nachrichten- und Sicherheitsdienst und der Verwaltung Ermittlung und Fahndung und den Enquetendiensten, Ermittlungsdiensten und

Diensten der Generalverwaltung Zoll und Akzisen, die mit der Aufsicht, Kontrolle und Feststellung beauftragt sind, stammen (Artikel 14 § 1 Nr. 2, ersetzt durch das Gesetz vom 15. Juli 2018).

In Bezug auf die Zusammensetzung der PNR-Zentralstelle heißt es in den Vorarbeiten:

« Le modèle belge repose sur un concept d'unité multidisciplinaire composée d'un fonctionnaire dirigeant assurant une mission de direction, de membres administratifs et de membres détachés issus des services compétents.

L'UIP sera composé :

- d'un fonctionnaire dirigeant, assisté par un service d'appui, qui au sein du SPF Intérieur sera responsable notamment de la gestion de la banque de données, du respect des obligations des transporteurs et opérateurs de voyage, du rapportage, de la conclusion de protocoles avec les services compétents et du respect des conditions de traitement. Le service d'appui sera notamment composé d'analystes, juristes, experts ICT et du délégué à la protection des données, qui disposeront des habilitations de sécurité nécessaires.

- de membres détachés issus des services compétents limitativement énumérés par le point 2 du § 1er, à savoir : les services de police, les services de renseignement et la Douane. Les finalités précises constituent en tant que telles la première limitation. Par exemple, au niveau des services de la police intégrée, il est évident qu'un agent de quartier au sein d'une police locale ne pourra jamais prendre connaissance des données des passagers dès lors que les finalités ne rentrent pas dans ses missions.

Le détachement des services compétents a pour objectif de garantir un certain degré d'expertise mais n'exclut d'aucune façon des accords entre ceux-ci afin de mutualiser les détachements » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 22).

Der Minister der Sicherheit und des Innern hat ebenfalls erläutert:

« Au total, quinze personnes auront accès à ces données. Les quatre services compétents détacheront chacun deux personnes. Celles-ci viendront s'ajouter aux sept membres du personnel de l'UIP. Il sera également désigné un *data protection officer* chargé de faire rapport à la Commission de la protection de la vie privée » (*Parl. Dok.*, Kammer, 2016-2017, DOC 54-2069/003, S. 24).

B.63.3. In Ausführung von Artikel 14 § 4 des Gesetzes vom 25. Dezember 2016 bestimmt der königliche Erlass vom 21. Dezember 2017 « zur Ausführung des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten und zur Festlegung verschiedener Bestimmungen in Bezug auf die PNR-Zentralstelle und den

Datenschutzbeauftragten » die Modalitäten der Zusammensetzung und Organisation der PNR-Zentralstelle.

Im Bericht an den König, der diesem königlichen Erlass vorausging, heißt es diesbezüglich:

« La banque de données ne peut donc être consultée qu’au sein de l’UIP, et uniquement par les membres de l’UIP, dans le cadre de leurs missions, ainsi que par le délégué à la protection des données » (*Belgisches Staatsblatt* vom 29. Dezember 2017, zweite Ausgabe, S. 116833).

Das Entsendeverfahren ist in den Artikeln 12 bis 21 des vorgenannten königlichen Erlasses vom 21. Dezember 2017 geregelt.

B.63.4. Durch den Umstand, dass die entsandten Mitglieder der zuständigen Dienste an der Arbeitsweise der PNR-Zentralstelle beteiligt sind, soll gewährleistet werden, dass sich diese PNR-Zentralstelle aus Personen zusammensetzt, die über ein gewisses Fachwissen verfügen, um so die Effizienz der PNR-Zentralstelle zu verstärken.

Diese Möglichkeit der Entsendung ist außerdem ausdrücklich in Artikel 4 Absatz 3 der PNR-Richtlinie vorgesehen, der bestimmt:

« Das Personal der PNR-Zentralstelle kann aus Mitarbeitern zuständiger Behörden bestehen, die zu diesem Zweck abgeordnet wurden. [...] ».

Nichts deutet darauf hin, dass diese Personen, auch wenn sie das Statut ihres ursprünglichen Dienstes behalten, ihre Aufgaben innerhalb der PNR-Zentralstelle nicht unabhängig ausüben. Artikel 14 § 1 Absatz 2 des Gesetzes vom 25. Dezember 2016 präzisiert außerdem, dass « die Mitglieder der zuständigen Dienste [während der Entsendung] der funktionellen und hierarchischen Amtsgewalt des leitenden Beamten der PNR-Zentralstelle [unterliegen] ».

Die Mitglieder der PNR-Zentralstelle machen sich zudem strafbar, wenn sie gegen die Schweigepflicht verstoßen oder wissentlich und willentlich Informationen, Daten und Auskünfte zurückhalten, wodurch die in Artikel 8 vorgesehenen Zwecke behindert werden (Artikel 48 und 49).

B.63.5. In Bezug auf den Zugriff auf die PNR-Daten im Rahmen von gezielten Recherchen nach einer sechsmonatigen Frist war der Gerichtshof der Europäischen Union in seinem vorerwähnten Gutachten 1/15 vom 26. Juli 2017 der Auffassung, dass sich die Verwendung der so 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 » (ebenda, Randnr. 208).

Artikel 12 Absatz 3 der PNR-Richtlinie bestimmt diesbezüglich:

« 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 ».

B.63.6. Um zu prüfen, ob die PNR-Zentralstelle als diese « andere nationale Behörde, die [...] zuständig ist » im Sinne von Artikel 12 Absatz 3 der PNR-Richtlinie anzusehen ist, ist folglich vor der Urteilsfällung dem Gerichtshof der Europäischen Union die im Tenor wiedergegebene siebte Vorabentscheidungsfrage zu stellen.

## 7. Die Aufbewahrungsdauer der PNR-Daten (Artikel 18)

B.64. Die klagende Partei übt Kritik an Artikel 18 des Gesetzes vom 25. Dezember 2016, insofern die Frist von fünf Jahren, während der die PNR-Daten aufbewahrt werden, unverhältnismäßig sei.

B.65.1. Artikel 12 der PNR-Richtlinie mit der Überschrift « Speicherfrist und Depersonalisierung » 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 ».

Der Erwägungsgrund 25 der PNR-Richtlinie bestimmt:

« 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 ».

B.65.2.1. Nach der Rechtsprechung des Gerichtshofes muss die Aufbewahrungsdauer der Daten « stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen » (EuGH, 6. Oktober 2015, C-362/14, *Schrems*, Randnr. 93; Große Kammer, 21. Dezember 2016, C-203/15 und C-698/15, *Tele2 Sverige und Watson u.a.*, Randnr. 110; Große Kammer, 26. Juli 2017, Gutachten 1/15, Randnr. 156).

B.65.2.2. Was insbesondere die PNR-Daten betrifft, hat der Gerichtshof in seinem vorerwähnten Gutachten 1/15 vom 26. Juli 2017 festgestellt, dass die Dauer von fünf Jahren « nicht über das hinausgeht, was zur Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität absolut notwendig ist » (Große Kammer, 26. Juli 2017, Gutachten 1/15, Randnr. 209), unter 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 [würde] » (vgl. entsprechend Urteil vom 21. Dezember 2016, *Tele2 Sverige und Watson u. a.*, C-203/15 und C-698/15, EU:C:2016:970, Randnr. 119) » (ebenda, Randnr. 205).

B.66.1. Artikel 18 des Gesetzes vom 25. Dezember 2016 sieht vor, dass die Passagierdaten höchstens fünf Jahre ab ihrer Speicherung in der Passagierdatenbank aufbewahrt werden und dass sie am Ende dieser Frist vernichtet werden.

Gemäß Artikel 21 § 1 des Gesetzes vom 25. Dezember 2016 stellt die PNR-Zentralstelle sicher, dass die Passagierdaten am Ende des in Artikel 18 erwähnten Zeitraums dauerhaft aus ihrer Datenbank gelöscht werden.

B.66.2. In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 heißt es:

« L'article 18 précise le délai de conservation des données dans la banque de données passagers.

Conformément à l'article 4, 4° de la loi du 8 décembre 1992 relative à la protection de la vie privée eu égard au traitement des données à caractère personnel, les données à caractère personnel sont conservées sous une forme qui permet d'identifier les personnes concernées pendant un délai qui n'excède pas celui qui est nécessaire pour concrétiser les objectifs pour lesquels ils ont été collectés ou pour lesquels ils seront ultérieurement traités.

C'est pourquoi les données du fichier des données de voyage telles que visées à l'article 9 sont conservées pendant un délai maximal de 5 ans pour la prévention, la recherche, l'examen et la poursuite des infractions terroristes et de la criminalité grave ainsi que pour la protection

des intérêts fondamentaux de l'État et ensuite définitivement supprimées de la Banque de données passagers. À l'issue de ce délai, elles sont détruites.

Ce délai de 5 ans maximum doit permettre d'exécuter les analyses et vérifications nécessaires en vue de la découverte de nouveaux phénomènes ou de la recherche de nouvelles tendances liées aux finalités, d'adapter ou de déterminer de nouveaux profils de risque et, le cas échéant, de recueillir des preuves, de trouver d'éventuels co-auteurs ou complices et de démanteler des réseaux criminels » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 25-26).

B.66.3.1. Die in Artikel 18 des Gesetzes vom 25. Dezember 2016 vorgesehene Frist von fünf Jahren ist jedoch in Verbindung mit den Artikeln 19 ff. desselben Gesetzes zu betrachten, die ebenfalls die Modalitäten zur Aufbewahrung der Daten regeln.

B.66.3.2. Artikel 19 des Gesetzes vom 25. Dezember 2016 bestimmt:

« Nach Ablauf einer sechsmonatigen Frist ab der Speicherung der Passagierdaten in der Passagierdatenbank werden alle Passagierdaten durch Unkenntlichmachung folgender Datenelemente, mit denen die Identität des Passagiers, auf den sich die Daten beziehen, unmittelbar festgestellt werden könnte, depersonalisiert:

1. Name(n), auch die Namen anderer Passagiere, sowie Anzahl der mitreisenden Personen,
2. Anschrift und Kontaktangaben,
3. alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift, die zur unmittelbaren Feststellung der Identität des Passagiers oder jeglicher anderen Person beitragen könnten,
4. Informationen in Bezug auf Vielreisende,
5. allgemeine Hinweise, die zur unmittelbaren Feststellung der Identität des Passagiers beitragen könnten,
6. alle in Artikel 9 § 1 Nr. 18 erwähnten Daten ».

Diese Bestimmung ist in Verbindung mit Artikel 4 Nr. 14 des Gesetzes vom 25. Dezember 2016 zu betrachten, der die « Depersonalisierung durch Unkenntlichmachung von Datenelementen » als « die in Artikel 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.

B.66.3.3. Artikel 20 des Gesetzes vom 25. Dezember 2016 sieht vor, dass nach Ablauf des in Artikel 19 erwähnten sechsmonatigen Zeitraums die Mitteilung der vollständigen Passagierdaten nur für die durch Artikel 27 vorgeschriebene Datenverarbeitung zugelassen ist, und auch nur unter den in dieser Bestimmung festgelegten Bedingungen.

Außerdem wird das in Artikel 24 erwähnte Ergebnis der Verarbeitung von der PNR-Zentralstelle nur solange aufbewahrt, wie dies erforderlich ist, um die zuständigen Behörden und gemäß Artikel 36 die PNR-Zentralstellen anderer Mitgliedstaaten der Europäischen Union über einen Treffer zu informieren (Artikel 21 § 3 Absatz 1).

B.66.3.4. Artikel 22 des Gesetzes vom 25. Dezember 2016 gewährleistet, dass der leitende Beamte und der Datenschutzbeauftragte nur Zugriff auf alle im Rahmen der Ausführung ihrer Aufträge relevanten Daten haben.

Schließlich wird die Datenverarbeitung protokolliert und hängt sie in direktem Zusammenhang mit den in Artikel 8 vorgesehenen Zwecken (Artikel 23 § 1). Die PNR-Zentralstelle sorgt für die Protokollierung, indem sie alle ihrer Zuständigkeit unterliegenden Verarbeitungssysteme und -verfahren während fünf Jahren dokumentiert (Artikel 23 § 2 Absatz 1).

B.66.4. Bei der Aufbewahrungsdauer der Passagierdaten müssen die Verarbeitungszwecke dieser Daten im direkten Zusammenhang mit den Zielen der Verhütung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität berücksichtigt werden.

B.67.1. Der Ausschuss für den Schutz des Privatlebens hatte jedoch festgestellt, dass bei einer langen Aufbewahrungsfrist der Daten und einer massenhaften Speicherung der Daten « das Risiko der Profilerstellung der betroffenen Personen zunimmt, ebenso wie das Risiko der Zweckentfremdung (*'function creep'*), das heißt die potenzielle missbräuchliche Verwendung der Daten für andere Straftaten, für die es ursprünglich keine (politische) Vereinbarung über den Datenaustausch gab » (Ausschuss für den Schutz des Privatlebens, Initiativstellungnahme Nr. 01/2010 vom 13. Januar 2010 « zum Gesetzesentwurf zur Zustimmung zu dem 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), geschehen zu Brüssel am 23. Juli 2007 und zu Washington am 26. Juli 2007 », Nummer 3.3, SS. 17-18).

In seiner Stellungnahme Nr. 55/2015 vom 16. Dezember 2015 zu dem Vorentwurf des Gesetzes, der dem Gesetz vom 25. Dezember 2016 zugrunde lag, war der Ausschuss für den Schutz des Privatlebens ebenfalls der Meinung, dass die Notwendigkeit der fünf Jahre langen Aufbewahrungsfrist für die Daten präziser und ausführlicher begründet werden müsste (Nummer 32).

In seiner Stellungnahme vom 19. August 2016 über die datenschutzrechtlichen Auswirkungen der Verarbeitung von Passagierdaten hat der Beratende Ausschuss für das Übereinkommen Nr. 108 des Europarates « zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten » ebenfalls angemerkt, dass « unkenntlich gemachte Daten es immer noch ermöglichen, die Personen zu identifizieren, und deshalb personenbezogene Daten bleiben, und dass ihre Speicherung auch zeitlich begrenzt werden müsste, um einer allgemeinen permanenten Überwachung vorzubeugen » (Stellungnahme vom 19. August 2016, T-PD(2016)18rev, S. 9).

B.67.2. Um zu überprüfen, ob diese Speicherfrist von fünf Jahren, die nach der PNR-Richtlinie zulässig ist, in Anbetracht des Vorstehenden und der verschiedenen in B.66 aufgezählten Garantien mit den in B.65.2.2. erwähnten Anmerkungen des Gerichtshofes vereinbar ist, da keinerlei Unterscheidung danach vorgenommen wird, ob sich im Rahmen der Vorabüberprüfung herausstellt, dass die betroffenen Passagiere ein Risiko für die öffentliche Sicherheit darstellen können oder nicht, ist folglich vor der Urteilsfällung zur Sache dem Gerichtshof der Europäischen Union die im Tenor wiedergegebene achte Vorabentscheidungsfrage zu stellen.

#### *In Bezug auf den zweiten Klagegrund*

B.68. Der zweite, hilfsweise vorgebrachte Klagegrund ist aus einem Verstoß abgeleitet gegen Artikel 22 der Verfassung in Verbindung mit Artikel 3 Absatz 2 des Vertrags über die Europäische Union und Artikel 45 der Charta der Grundrechte der Europäischen Union.

Dieser Klagegrund richtet sich gegen Artikel 3 § 1, Artikel 8 § 2 und Kapitel 11, das die Artikel 28 bis 31 umfasst, des Gesetzes vom 25. Dezember 2016.

Die klagende Partei ist der Ansicht, dass mit den angefochtenen Bestimmungen durch die Ausweitung des PNR-Systems auf Flüge innerhalb der EU mittelbar wieder Grenzkontrollen eingeführt würden, die gegen die Freizügigkeit verstoßen würden.

B.69.1. Artikel 3 § 1 des Gesetzes vom 25. Dezember 2016 bestimmt :

« 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 ».

Der Inhalt der Artikel 8 § 2 und 28 bis 31 des Gesetzes vom 25. Dezember 2016 ist in B.55 aufgeführt.

B.69.2. In Bezug auf den Anwendungsbereich des Gesetzes vom 25. Dezember 2016 heißt es in den Vorarbeiten:

« L'inclusion intra-UE dans la collecte des données permettra d'obtenir un tableau plus complet des déplacements des passagers qui constituent une menace potentielle pour la sécurité intracommunautaire et nationale. La pratique a déjà démontré que certains ' *returnees* ' (aussi appelés ' *foreign fighters* ' qui rentrent en Europe) embarquent à bord de différents vols avant de rallier leur destination finale.

La Directive UE PNR prévoit expressément la possibilité pour les États membres de traiter les données des passagers de l'UE pour le trafic international au sein de l'Union européenne. En outre, tous les États membres ont approuvé, le 21 avril 2016 au Conseil des ministres de l'Intérieur et de la Justice, une déclaration visant à transposer la directive UE PNR dans les droits nationaux aussi pour le trafic intra-Union européenne » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 7).

B.69.3. Wie in B.55 erwähnt, sind die Passagiere, auf die sich Kapitel 11 des Gesetzes vom 25. Dezember 2016 bezieht, ebenso wie die betreffenden Daten und die Aufbewahrungsdauer beschränkt.

In den Vorarbeiten heißt es:

« Par conséquent, seuls sont concernés les passagers qui souhaitent franchir ou ont franchi les frontières extérieures de la Belgique pour y entrer ou en sortir et ce, indépendamment du type de transport utilisé (maritime, ferroviaire, terrestre, aérien). Seules les données de ces passagers seront donc traitées par les services de police chargés du contrôle aux frontières et l'Office des étrangers.

Les passagers qui envisagent de transiter par la zone internationale de transit par exemple d'un aéroport situé en Belgique sont également visés dans la mesure où les règles sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers s'appliquent également à eux. Ainsi, ces personnes doivent disposer des documents de voyage requis. Certaines personnes sont soumises à l'obligation de visa de transit aéroportuaire; des contrôles dans ces zones sont autorisés et peuvent, dans certains cas, conduire à une mesure de refoulement.

Comme déjà mentionné, seules les données de passagers dites ' API ' seront transmises aux services de police et à l'Office des étrangers en vertu du présent chapitre. Ces données sont énumérées à l'article 9, § 2, de l'avant-projet de loi.

Elles correspondent en substance à celles que les transporteurs aériens doivent déjà transmettre en vertu de l'arrêté royal du 11 décembre 2006.

[...]

L'utilisation des données est également limitée à vingt-quatre heures. Au-delà, si l'accès aux données des passagers est nécessaire dans le cadre de l'exercice de ses missions légales, l'Office des étrangers adresse une requête motivée à l'UIP » (ebenda, SS. 34-35).

B.70.1. Wie bereits erwähnt, ist die Ausweitung des PNR-Systems auf EU-Flüge nach dem Erwägungsgrund 10 der PNR-Richtlinie zulässig. Artikel 2 der PNR-Richtlinie regelt das Verfahren, um den Anwendungsbereich auszudehnen.

Wie in B.55.4 erwähnt, betrifft der Zweck der Bekämpfung der illegalen Einwanderung und der Verbesserung der Grenzkontrolle nur die in Artikel 29 § 2 des Gesetzes vom 25. Dezember 2016 aufgezählten Kategorien von Passagieren und beschränkt sich auf die in Artikel 9 § 1 Nr. 18 des Gesetzes vom 25. Dezember 2016 erwähnten API-Daten. Die Verarbeitungen im Rahmen dieses Zwecks sind ebenfalls beschränkt. Die angefochtenen Bestimmungen sind Bestandteil der Umsetzung der API-Richtlinie, die als Ziele ebenfalls die Bekämpfung der illegalen Einwanderung und die Verbesserung der Grenzkontrolle verfolgt.

B.70.2. In seiner Stellungnahme Nr. 55/2015 vom 16. Dezember 2015 zu dem Vorentwurf des Gesetzes, der dem Gesetz vom 25. Dezember 2016 zugrunde lag, hat sich der Ausschuss für den Schutz des Privatlebens jedoch die Frage nach der Vereinbarkeit des eingeführten PNR-Systems, das « sowohl auf Beförderungen in den und aus dem Schengener

Raum (extra-Schengen) als auch aus dem Schengener Raum ein- und ausgehende Beförderungen (intra-Schengen) » abzielt, was « indirekt zu einer Wiedereinführung von Kontrollen an den Binnengrenzen » führen könnte, mit dem Grundsatz der Freizügigkeit gestellt (Nummern 21-25).

B.70.3. Um somit zu prüfen, ob diese Maßnahmen mit der Freizügigkeit vereinbar sind, ist folglich vor der Urteilsfällung zur Sache dem Gerichtshof der Europäischen Union die im Tenor wiedergegebene neunte Vorabentscheidungsfrage zu stellen.

Aus diesen Gründen:

Der Gerichtshof

stellt vor der Urteilsfällung zur Sache dem Gerichtshof der Europäischen Union folgende Vorabentscheidungsfragen:

1. Ist Artikel 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 - DSGVO) in Verbindung mit Artikel 2 Absatz 2 Buchstabe 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 Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union in dem Sinne vereinbar, dass die darin aufgeführten Daten sehr weitgehend sind – insbesondere die in Nummer 18 von Anhang I der Richtlinie (EU) 2016/681 erwähnten Daten, die über die in Artikel 3 Absatz 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 Nummern 12 und 18 von Anhang I der Richtlinie (EU) 2016/681 mit den Artikeln 7, 8 und 52 Absatz 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 Artikel 3 Nummer 4 der Richtlinie (EU) 2016/681 und Anhang I derselben Richtlinie mit den Artikeln 7, 8 und 52 Absatz 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 Artikel 6 der Richtlinie (EU) 2016/681 in Verbindung mit den Artikeln 7, 8 und 52 Absatz 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 Artikel 6 der Richtlinie (EU) 2016/681 mit den Artikeln 7, 8 und 52 Absatz 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 Artikel 12 Absatz 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 Artikel 12 der Richtlinie (EU) 2016/681 in Verbindung mit den Artikeln 7, 8 und 52 Absatz 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 Artikel 3 Absatz 2 des Vertrags über die Europäische Union und Artikel 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 Artikel 3 Absatz 2 des Vertrags über die Europäische Union und Artikel 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?

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 17. Oktober 2019.

Der Kanzler,

Der Präsident,

F. Meersschaut

F. Daoût