Gericht:	VG Wiesbaden 6. Kammer
Entscheidungsdatum:	13.05.2020
Aktenzeichen:	6 K 805/19.WI
ECLI:	ECLI:DE:VGWIESB:2020:0513.6K805.19.WI.00
Dokumenttyp:	Beschluss
Quelle:	HESSEN
Normen:	Art 13 DS-GVO, Art 14 DS-GVO, Art 52 GRCh, Art 7 GRCh, Art 8 GRCh ... mehr

---

Datenschutzrecht

Leitsatz

1. Es bestehen erhebliche Zweifel, ob die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität mit der Charta der Grundrechte der Europäischen Union, insbesondere mit Art. 7 und Art. 8 GRCh, vereinbar ist.

2. Die durch die Richtlinie (EU) 2016/681 vorgeschriebene anlasslose und massenhafte Verarbeitung von Fluggastdaten ist mit der Vorratsdatenspeicherung von Telekommunikationsdaten vergleichbar.

3. Der automatisierte Abgleich personenbezogener Daten mit sogenannten Mustern und die 5-jährige Speicherung personenbezogener Daten stellen tiefgreifende Grundrechtseingriffe dar. Sie können deshalb allenfalls zur Bekämpfung von Terrorismus und besonders schwerer Kriminalität, nicht aber zur Verfolgung weniger schwerwiegender Delikte (sogenannter Beifang), als angemessene Mittel betrachtet werden.

4. Es ist zweifelhaft, ob es mit dem Gesetzesvorbehalt des Art. 52 Abs. 1 GRCh vereinbar ist, die Ausgestaltung der Muster, mit denen die Fluggastdaten automatisiert abgeglichen werden, vollständig der jeweiligen Exekutive der einzelnen Mitgliedstaaten der Europäischen Union zu überlassen.

5. Eine Pseudonymisierung gespeicherter personenbezogener Daten verringert den mit ihrer Speicherung verbundenen Grundrechtseingriff, anders als eine Anonymisierung, nicht.

6. Die Übermittlung personenbezogener Daten nach der Richtlinie (EU) 2016/681 aus der Europäischen Union an Drittstaaten ist nur zulässig, wenn der jeweilige Drittstaat ein angemessenes Datenschutzniveau garantieren kann.

7. Gemäß Art. 13 und 14 DS-GVO spricht viel dafür, dass die Luftfahrtunternehmen dazu verpflichtet sind, die Fluggäste umfassend über die Fluggastdatenverarbeitung nach der Richtlinie (EU) 2016/681 zu informieren.

Tenor

I. Das Verfahren wird ausgesetzt.

II. Das Verfahren wird gemäß Art. 267 AEUV zur Vorabentscheidung dem
Gerichtshof der Europäischen Union hinsichtlich der folgenden Fragen vorgelegt:

1. Ist die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (ABl. EU vom 4. Mai 2016, L 119 S. 132; im Folgenden als PNR-Richtlinie bezeichnet), nach der Luftfahrtunternehmen umfangreiche Datensätze hinsichtlich ausnahmslos aller Fluggäste an von den Mitgliedstaaten eingerichtete PNR-Zentralstellen übermitteln und die Datensätze dort anlasslos für den automatisierten Abgleich mit Datenbanken und Mustern verwendet und anschließend fünf Jahre lang gespeichert werden unter Berücksichtigung des durch die PNR-Richtlinie angestrebten Zwecks und der Erfordernisse der Bestimmtheit und Verhältnismäßigkeit mit der Charta der Grundrechte, insbesondere mit Art. 7, Art. 8 und Art. 52 GRCh vereinbar?

2. Insbesondere:

a) Ist Art. 3 Nr. 9 PNR-Richtlinie in Verbindung mit Anhang II zur PNR-Richtlinie, soweit hierin geregelt wird, dass der Begriff „schwere Kriminalität“ im Sinne der PNR-Richtlinie strafbare Handlungen bezeichnet, die im Anhang II zur PNR-Richtlinie aufgeführt werden und die nach dem nationalem Recht eines Mitgliedstaates mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind, unter dem Gesichtspunkt der hinreichenden Bestimmtheit und dem Erfordernis der Verhältnismäßigkeit mit Art. 7 und Art. 8 GRCh vereinbar?

b) Sind die zu übermittelnden Fluggastdatensätze (im Folgenden: PNR-Daten), soweit sie die Übermittlung der Namen (Art. 8 Abs. 1 Satz 1 i.V.m. Anhang I Nr. 4 PNR-Richtlinie), des Vielflieger-Eintrages (Art. 8 Abs. 1 Satz 1 i.V.m. Anhang I Nr. 8 PNR-Richtlinie) und des Eintragens eines Freitextfeldes mit allgemeinen Hinweisen (Art. 8 Abs. 1 Satz 1 i.V.m. Anhang I Nr. 12 PNR-Richtlinie) verlangen, hinreichend bestimmt, um einen Eingriff in Art. 7 und Art. 8 GRCh rechtfertigen zu können?

c) Ist es mit Art. 7 und Art. 8 GRCh und der Zweckrichtung der PNR-Richtlinie vereinbar, dass über die Daten von Fluggästen hinaus auch die Daten von Dritten, wie Reisebüro/Sachbearbeiter (Anhang I Nr. 9 PNR-Richtlinie), Begleitpersonen von Minderjährigen (Anhang I Nr. 12 PNR-Richtlinie) und Mitreisenden (Anhang I Nr. 17 PNR-Richtlinie) erfasst werden?

d) Ist die PNR-Richtlinie, soweit nach ihr PNR-Daten minderjähriger Flugreisender übermittelt, verarbeitet und gespeichert werden, mit Art. 7, Art. 8 und Art. 24 GRCh vereinbar?

e) Ist Art. 8 Abs. 2 PNR-Richtlinie in Verbindung mit Anhang I Nr. 18 PNR-Richtlinie, wonach API-Daten, auch soweit sie mit PNR-Daten identisch sind, durch die Luftfahrtunternehmen an die PNR-Zentralstellen der Mitgliedstaaten übermittelt werden, unter Berücksichtigung des Grundsatzes der Datensparsamkeit mit Art. 8 und Art. 52 GRCh vereinbar?

f) Ist Art. 6 Abs. 4 PNR-Richtlinie als Rechtsgrundlage zur Bestimmung der Kriterien, mit denen die Datensätze abgeglichen werden (sog. Muster), eine ausreichende gesetzlich geregelte legitime Grundlage im Sinne von Art. 8 Abs. 2 und Art. 52 GRCh sowie Art. 16 Abs. 2 AEUV?

g) Beschränkt Art. 12 PNR-Richtlinie den Eingriff in Art. 7 und Art. 8 GRCh noch auf das absolut notwendige Maß, wenn die übermittelten Daten bei den PNR-Zentralstellen der Mitgliedstaaten fünf Jahre lang gespeichert werden?

h) Führt die Depersonalisierung nach Art. 12 Abs. 2 PNR-Richtlinie zu einer Reduzierung der personenbezogenen Daten auf das nach Art. 8 und Art. 52 GRCh notwendige Maß, wenn es sich dabei um nichts anderes als eine jederzeit wieder umkehrbare Pseudonymisierung handelt?

i) Sind Art. 7, Art. 8 und Art. 47 GRCh dahingehend auszulegen, dass sie es erforderlich machen, dass Fluggäste, deren Daten im Rahmen der Fluggastdatenverarbeitung de-depersonalisiert werden (Art. 12 Abs. 3 PNR-Richtlinie), hierüber benachrichtigt werden und ihnen so die Möglichkeit einer gerichtlichen Überprüfung eröffnet wird?

3. Ist Art. 11 PNR-Richtlinie, soweit er die Übermittlung von PNR-Daten an Drittstaaten erlaubt, die über kein angemessenes Datenschutzniveau verfügen, mit Art. 7 und Art. 8 GRCh vereinbar?

4. Bietet Art. 6 Abs. 4 Satz 4 PNR-Richtlinie hinreichenden Schutz vor der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 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 (ABl. EU vom 4. Mai 2016, L 119 S.1; im Folgenden als DS-GVO bezeichnet) und Art. 10 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung von personenbezogenen Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU vom 4. Mai 2016, L 119 S. 89; im Folgenden als Richtlinie (EU) 2016/680 bezeichnet), wenn im Rahmen des Freitextfeldes „allgemeine

Hinweise“ (Anhang I Nr. 12 PNR-Richtlinie) beispielsweise Essenswünsche übermittelt werden können, die Rückschlüsse auf solche besonderen Kategorien personenbezogener Daten zulassen?

5. Ist es mit Art. 13 DS-GVO vereinbar, wenn Fluggäste durch die Luftfahrtunternehmen auf ihrer Webseite lediglich auf das nationale Umsetzungsgesetz (hier: Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG -) vom 6. Juni 2017, BGBl. I S. 1484, im Folgenden als FlugDaG bezeichnet) hingewiesen werden?

Gründe

I.

1 Gegenstand des Verfahrens ist eine Klage gegen die Bundesrepublik Deutschland, vertreten durch das C. Der Kläger flog mit dem Luftfahrtunternehmen E. am 28. April 2019 von Frankfurt am Main, Deutschland nach Bogota, Kolumbien und am 7. Mai 2019 von Rio de Janeiro, Brasilien zurück nach Frankfurt am Main. Hinsichtlich dieser Flüge begehrt er die Löschung seiner Daten bei der Beklagten.

2 Am 10. Juni 2017 trat das FlugDaG in Kraft. Das Gesetz dient der Umsetzung der PNR-Richtlinie. Diese Richtlinie regelt verbindlich die Übermittlung von PNR-Daten bei Flügen von Mitgliedstaaten der Europäischen Union in Drittstaaten und von Drittstaaten in Mitgliedstaaten der Europäischen Union und die Verarbeitung dieser Daten. Zweck der Richtlinie ist gemäß Art. 1 Abs. 2 PNR-Richtlinie die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Die Richtlinie verpflichtet die Mitgliedstaaten zur Einrichtung sog. PNR-Zentralstellen (Art. 4 Abs. 1 PNR-Richtlinie), die zur Erreichung des Zwecks der Richtlinie für die Erhebung von PNR-Daten bei Fluggesellschaften, für die Speicherung, Verarbeitung und Übermittlung dieser Daten an die zuständigen Behörden sowie für den Austausch der PNR-Daten selbst wie auch der Ergebnisse von deren Verarbeitung zuständig sind. Gemäß Art. 8 PNR-Richtlinie i.V.m. Anhang I PNR-Richtlinie haben die Mitgliedstaaten alle Fluggesellschaften zu verpflichten, einen definierten Satz von PNR-Daten an die PNR-Zentralstellen desjenigen Mitgliedstaates zu übermitteln, in dessen Hoheitsgebiet die betreffenden Flüge ankommen oder von dem sie ausgehen. Gemäß Art. 9 PNR-Richtlinie können Mitgliedstaaten die PNR-Daten untereinander anfordern und aneinander übermitteln. Unter den Voraussetzungen von Art. 11 PNR-Richtlinie ist auch eine Übermittlung der Datensätze an Drittstaaten möglich. Gemäß Art. 12 Abs. 2 PNR-Richtlinie sollen die gespeicherten Fluggastdaten, die fünf Jahre lang gespeichert werden sollen, nach Ablauf von sechs Monaten „depersonalisiert“, das heißt die Datenelemente, mit denen die Identität des Fluggastes unmittelbar festgestellt werden könnte, unkenntlich gemacht werden. Jedoch ist eine De-Depersonalisierung dieser Datenelemente unter den Voraussetzungen des Art. 12 Abs. 3 PNR-Richtlinie möglich. Art. 6 PNR-Richtlinie regelt die Verarbeitung der Daten, die insbesondere durch den automatisierten Abgleich derselben mit Datenbanken und sogenannten Mustern erfolgen soll. Die PNR-Richtlinie enthält für die nationalen Gesetzgeber eine Öffnungsklausel dahingehend, dass auch Flüge innerhalb des EU-Mitgliedstaates bzw. zwischen EU-Mitgliedstaaten erfasst werden können. Das FlugDaG setzt diese Richtlinie in deutsches Recht um. Es erweitert, wie durch Art. 2 Abs. 1 PNR-Richtlinie ausdrücklich zugelassen, die Übermittlungspflicht auf alle zivilen Flüge, die in Deutschland starten und in einem anderen Land landen oder von einem anderen Land aus starten und in

Deutschland landen, also auch auf Flüge innerhalb der Mitgliedstaaten der Europäischen Union, § 2 Abs. 3 FlugDaG.

II.

3 Die **Charta der Grundrechte** der Europäischen Union - **GRCh** - (ABl. EU 2016 Nr. C 202 vom 7. Juni 2016, S. 389) regelt:

4 **Art. 7** GRCh - Achtung des Privat- und Familienlebens

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

5 **Art. 8** GRCh - Schutz personenbezogener Daten

(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.

6 **Art. 24** GRCh - Rechte des Kindes

(1) Kinder haben Anspruch auf den Schutz und die Fürsorge, die für ihr Wohlergehen notwendig sind. Sie können ihre Meinung frei äußern. Ihre Meinung wird in den Angelegenheiten, die sie betreffen, in einer ihrem Alter und ihrem Reifegrad entsprechenden Weise berücksichtigt.

(2) Bei allen Kinder betreffenden Maßnahmen öffentlicher Stellen oder privater Einrichtungen muss das Wohl des Kindes eine vorrangige Erwägung sein.

[...]

7 **Art. 47** GRCh - Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht

(1) Jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, hat das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen.

(2) Jede Person hat ein Recht darauf, dass ihre Sache von einem unabhängigen, unparteiischen und zuvor durch Gesetz errichteten Gericht in einem fairen Verfahren, öffentlich und innerhalb angemessener Frist verhandelt wird. Jede Person kann sich beraten, verteidigen und vertreten lassen.

[...]

8 **Art. 52** GRCh - Tragweite und Auslegung der Rechte und Grundsätze

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

[...]

9 **Art. 16** des **Vertrags über die Arbeitsweise der Europäischen Union** - **AEUV** - (in der bereinigten Fassung vom 07. Juni 2016, ABl. Nr. C 202 S. 1, 47) lautet:

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

(2) Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht. Die auf der Grundlage dieses Artikels erlassenen Vorschriften lassen die spezifischen Bestimmungen des Artikels 39 des Vertrags über die Europäische Union unberührt.

10 Die **PNR-Richtlinie** (ABl. EU vom 4. Mai 2016, L 119 S. 132) regelt:

11 **Art. 1** PNR-Richtlinie - Gegenstand und Anwendungsbereich

(1) Diese Richtlinie regelt

> *a) die Übermittlung von Fluggastdatensätzen (PNR-Daten) zu Fluggästen von Drittstaatsflügen durch Fluggesellschaften;*
>
> *b) die Verarbeitung von Daten gemäß Buchstabe a, unter anderem ihre Erhebung, Verwendung und Speicherung durch Mitgliedstaaten sowie den Austausch dieser Daten zwischen Mitgliedstaaten.*

(2) 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 Abs. 2 Buchstaben a, b und c verarbeitet werden.

12 **Art. 2** PNR-Richtlinie - Anwendung dieser Richtlinie auf EU-Flüge

(1) Ein Mitgliedstaat, der entscheidet, diese Richtlinie auf Flüge innerhalb der Europäischen Union (EU-Flüge) anzuwenden, teilt dies der Kommission schriftlich mit. Ein Mitgliedstaat kann eine solche Mitteilung jederzeit machen oder widerrufen. Die Kommission veröffentlicht diese Mitteilung und eventuelle Widerrufe derselben im Amtsblatt der Europäischen Union.

(2) Im Falle einer Mitteilung gemäß Absatz 1 gelten alle Bestimmungen dieser Richtlinie für EU-Flüge so, als handele es sich um Drittstaatsflüge, und für PNR-Daten zu EU-Flügen so, als handele es sich um PNR-Daten zu Drittstaatsflügen.

(3) Ein Mitgliedstaat kann beschließen, diese Richtlinie nur auf ausgewählte EU-Flüge anzuwenden. Der Mitgliedstaat wählt dabei diejenigen Flüge aus, die er für die Verfolgung der Ziele dieser Richtlinie für erforderlich hält. Der Mitgliedstaat kann jederzeit eine Änderung der von ihm ausgewählten EU-Flüge beschließen.

13 **Art. 3** PNR-Richtlinie - Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

> *1. „Fluggesellschaft“ ein Luftfahrtunternehmen mit einer gültigen Betriebsgenehmigung oder einer gleichwertigen Genehmigung, die es ihm gestattet, Fluggäste auf dem Luftweg zu befördern;*
>
> *[…]*
>
> *4. „Fluggast“ jede Person, einschließlich Transfer- oder Transitfluggästen, mit Ausnahme der Besatzungsmitglieder, die mit Zustimmung der Fluggesellschaft in einem Luftfahrzeug befördert wird oder befördert werden soll, wobei diese Zustimmung durch die Eintragung der Person in die Fluggastliste belegt wird;*
>
> *[…]*
>
> *9. „schwere Kriminalität“ 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;*
>
> *10. „Depersonalisierung durch Unkenntlichmachung von Datenelementen“ die Vorgehensweise, mit der diejenigen Datenelemente, mit denen die Identität des Fluggastes unmittelbar festgestellt werden könnte, für einen Nutzer unsichtbar gemacht werden.*

14 **Art. 4** PNR-Richtlinie - PNR-Zentralstelle

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

(2) Die PNR-Zentralstelle ist verantwortlich für

> *a) die Erhebung der PNR-Daten bei Fluggesellschaften, für die Speicherung und Verarbeitung dieser Daten sowie die Übermittlung dieser Daten oder der Ergebnisse ihrer Verarbeitung an die zuständigen Behörden nach Artikel 7;*
>
> *b) den Austausch sowohl von PNR-Daten als auch der Ergebnisse der Verarbeitung dieser Daten mit den PNR-Zentralstellen anderer Mitgliedstaaten und mit Europol gemäß den Artikeln 9 und 10.*

[…]

(4) Zwei oder mehr Mitgliedstaaten (die beteiligten Mitgliedstaaten) können gemeinsam eine einzige Behörde errichten oder benennen, die als ihre PNR-Zentralstelle handelt. Diese PNR-Zentralstelle hat ihren Sitz in einem der beteiligten Mitgliedstaaten und gilt als nationale PNR-Zentralstelle aller beteiligten Mitgliedstaaten. Die beteiligten Mitgliedstaaten einigen sich gemeinsam unter Beachtung der Anforderungen dieser Richtlinie über die genauen Modalitäten, unter denen die PNR-Zentralstelle ihrer Tätigkeit nachgeht.

[…]

15 **Art. 5** PNR-Richtlinie - Datenschutzbeauftragter der PNR-Zentralstelle

(1) Die PNR-Zentralstelle ernennt einen Datenschutzbeauftragten, der für die Überwachung der Verarbeitung der PNR-Daten und die Umsetzung der maßgeblichen Sicherheitsvorkehrungen zuständig ist.

(2) Die Mitgliedstaaten stellen den Datenschutzbeauftragten die Mittel zur Verfügung, damit sie ihre Pflichten und Aufgaben gemäß diesem Artikel wirksam und unabhängig wahrnehmen können.

(3) Die Mitgliedstaaten sorgen dafür, dass eine betroffene Person das Recht hat, den Datenschutzbeauftragten als zentrale Kontaktstelle im Zusammenhang mit allen Fragen bezüglich der Verarbeitung der PNR-Daten der betroffenen Person zu kontaktieren.

16 **Art. 6** PNR-Richtlinie - Verarbeitung der PNR-Daten

(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, nichtautomatisierte Art individuell überprüft wird, um zu klären, ob die zuständige Behörde gemäß Artikel 7 Maßnahmen im Einklang mit dem nationalen Recht ergreifen muss.

[…]

17 **Art. 8** PNR-Richtlinie - Datenübermittlungspflichten der Fluggesellschaften

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Fluggesellschaften mittels der „Push-Methode“ die in Anhang I aufgelisteten PNR-Daten an die Datenbank der PNR-Zentralstelle des Mitgliedstaats übermitteln, in dessen Hoheitsgebiet der betreffende Flug ankommt oder von dem er abgeht, soweit sie solche Daten im Rahmen ihrer normalen Geschäftstätigkeit bereits erhoben haben. Bei Flügen mit Code-Sharing zwischen mehreren Fluggesellschaften liegt die Pflicht zur Übermittlung der PNR-Daten aller Fluggäste des Fluges bei der Fluggesellschaft, die den Flug durchführt. Erfolgen auf einem Drittstaatsflug eine oder mehrere Zwischenlandungen auf Flughäfen der Mitgliedstaaten, so übermitteln die Fluggesellschaften die PNR-Daten aller Fluggäste an die PNR-Zentralstellen aller betreffenden Mitgliedstaaten. Dies gilt auch, wenn bei einem EU-Flug eine oder mehrere Zwischenlandungen auf den Flughäfen verschiedener Mitgliedstaaten erfolgen, jedoch nur in Bezug auf Mitgliedstaaten, die PNR-Daten zu EU-Flügen erheben.

(2) Falls die Fluggesellschaften in Anhang I Nummer 18 aufgelistete erweiterte Fluggastdaten (API-Daten) erhoben haben, diese aber nicht auf die gleiche technische Weise wie

andere PNR-Daten vorhalten, treffen die Mitgliedstaaten die erforderlichen Maßnahmen, um sicherzustellen, dass die Fluggesellschaften mittels der „Push-Methode“ auch diese Daten der PNR-Zentralstelle des in Absatz 1 genannten Mitgliedstaats übermitteln. Im Fall einer solchen Übermittlung gelten sämtliche Bestimmungen dieser Richtlinie in Bezug auf diese API-Daten.

[...]

18 **Art. 9** PNR-Richtlinie - Informationsaustausch zwischen den Mitgliedstaaten

(1) Die Mitgliedstaaten stellen sicher, dass alle relevanten und erforderlichen PNR-Daten oder die Ergebnisse der Verarbeitung dieser Daten von Personen, die von einer PNR-Zentralstelle nach Artikel 6 Absatz 2 ermittelt wurden, von dieser PNR-Zentralstelle den entsprechenden PNR-Zentralstellen der anderen Mitgliedstaaten übermittelt werden. Die PNR-Zentralstellen der Empfängermitgliedstaaten leiten gemäß Artikel 6 Absatz 6 die erhaltenen Daten an ihre zuständigen Behörden weiter.

(2) Die PNR-Zentralstelle eines Mitgliedstaats ist berechtigt, im Bedarfsfall bei der PNR-Zentralstelle jedes anderen Mitgliedstaats PNR-Daten, die in deren Datenbank vorgehalten werden und noch nicht gemäß Artikel 12 Absatz 2 durch Unkenntlichmachung von Datenelementen depersonalisiert wurden, sowie erforderlichenfalls auch die Ergebnisse jeglicher Verarbeitung dieser Daten, wenn dies bereits gemäß Artikel 6 Absatz 6 Buchstabe a erfolgt ist, anzufordern. Eine solche Anfrage ist gebührend zu begründen. Sie kann ein beliebiges Datenelement oder eine Kombination von Datenelementen betreffen, je nachdem, was die anfordernde PNR-Zentralstelle in dem konkreten Fall im Hinblick auf die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität für erforderlich erachtet. Die PNR-Zentralstellen übermitteln die angeforderten Informationen so rasch wie möglich. Falls die angeforderten Daten gemäß Artikel 12 Absatz 2 durch Unkenntlichmachung von Datenelementen depersonalisiert worden sind, stellt die PNR-Zentralstelle die vollständigen PNR-Daten nur bereit, wenn berechtigter Grund zu der Annahme besteht, dass dies für die Zwecke des Artikels 6 Absatz 2 Buchstabe b erforderlich ist, und nur, wenn sie durch eine in Artikel 12 Absatz 3 Buchstabe b genannte Behörde dazu ermächtigt ist.

[...]

19 **Art. 11** PNR-Richtlinie - Übermittlungen von Daten an Drittstaaten

(1) Die Mitgliedstaaten dürfen die PNR-Daten und die Ergebnisse der Verarbeitung dieser Daten, die durch die PNR-Zentralstelle nach Artikel 12 gespeichert werden, nur im Einzelfall und nur dann an einen Drittstaat übermitteln, wenn

a) die Bedingungen des Artikels 13 des Rahmenbeschlusses 2008/977/JI erfüllt sind;

b) die Übermittlung für die in Artikel 1 Absatz 2 genannten Zwecke dieser Richtlinie erforderlich ist;

c) der Drittstaat sich bereit erklärt, die Daten nur dann an einen anderen Drittstaat zu übermitteln, wenn dies für die in Artikel 1 Absatz 2 genannten Zwecke

dieser Richtlinie unbedingt notwendig ist und nur wenn der jeweilige Mitgliedstaat ausdrücklich zustimmt, und

d) die gleichen Bedingungen wie in Artikel 9 Absatz 2 erfüllt sind.

(2) Ungeachtet des Artikels 13 Absatz 2 des Rahmenbeschlusses 2008/977/JI sind Übermittlungen von PNR-Daten ohne vorherige Zustimmung des Mitgliedstaats, von dem die Daten eingeholt wurden, nur unter außergewöhnlichen Umständen und nur dann zulässig, wenn

a) eine solche Übermittlung unerlässlich ist, um eine bestimmte und gegenwärtige Bedrohung durch terroristische Straftaten oder schwere Kriminalität in einem Mitgliedstaat oder einem Drittstaat abzuwehren, und

b) die vorherige Zustimmung nicht rechtzeitig eingeholt werden kann.

Die für die Erteilung der Zustimmung zuständige Behörde wird unverzüglich unterrichtet und die Übermittlung wird ordnungsgemäß aufgezeichnet und einer Ex-Post-Überprüfung unterzogen.

[…]

20 **Art. 12** PNR-Richtlinie - Speicherfrist und Depersonalisierung

(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.

21 **Art. 13** PNR-Richtlinie - Schutz personenbezogener Daten

(1) Jeder Mitgliedstaat sorgt im Zusammenhang mit der Verarbeitung personenbezogener Daten nach dieser Richtlinie dafür, dass die Rechte jedes Fluggasts in Bezug auf Schutz personenbezogener Daten, Zugang, Berichtigung, Löschung und Einschränkung der Verarbeitung sowie Schadenersatz und Rechtsbehelfe den Rechten entsprechen, die nach Unionsrecht und nationalem Recht sowie zur Umsetzung der Artikel 17, 18, 19 und 20 des Rahmenbeschlusses 2008/977/JI festgelegt sind. Diesbezüglich gelten daher jene Artikel.

(2) Jeder Mitgliedstaat sorgt dafür, dass die nach nationalem Recht erlassenen Bestimmungen zur Umsetzung der Artikel 21 und 22 des Rahmenbeschlusses 2008/977/JI betreffend die Vertraulichkeit der Verarbeitung und die Datensicherheit ebenfalls auf jede Verarbeitung personenbezogener Daten nach dieser Richtlinie Anwendung finden.

(3) Diese Richtlinie berührt nicht die Anwendbarkeit der Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates auf die Verarbeitung personenbezogener Daten durch Fluggesellschaften, insbesondere deren Pflichten, geeignete technische und organisatorische Maßnahmen zum Schutz der Sicherheit und Vertraulichkeit der personenbezogenen Daten zu treffen.

(4) Die Mitgliedstaaten untersagen die Verarbeitung von PNR-Daten, die die rassische oder ethnische Herkunft einer Person, ihre politischen Meinungen, ihre religiösen oder weltanschaulichen Überzeugungen, ihre Mitgliedschaft in einer Gewerkschaft, ihren Gesundheitszustand oder ihr Sexualleben oder ihre sexuelle Orientierung erkennen lassen. Bei der PNR-Zentralstelle eingehende PNR-Daten, aus denen derartige Informationen hervorgehen, werden umgehend gelöscht.

[...]

22 **Anhang I** PNR-Richtlinie - Von Fluggesellschaften erhobene PNR-Daten

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.

23 **Anhang II** PNR-Richtlinie - Liste der strafbaren Handlungen gemäß Artikel 3 Nummer 9

[…]

6. Korruption

7. Betrugsdelikte, einschließlich Betrug zum Nachteil der finanziellen Interessen der Union

[…]

9. Computerstraftaten/Cyberkriminalität

10. Umweltkriminalität, einschließlich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten

[…]

24 Die **Richtlinie (EU) 2016/680** (ABl. EU vom 4. Mai 2016, L 119 S. 89) regelt:

25 **Art. 1** Richtlinie (EU) 2016/680 - Gegenstand und Ziele

(1) 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.

[…]

26 **Art. 3** Richtlinie (EU) 2016/680 **–** Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck:

[…]

5. „Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

[…]

27 **Art. 4** Richtlinie (EU) 2016/680 - Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten

a) auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,

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

c) dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind,

d) sachlich *richtig und erforderlichenfalls auf dem neuesten Stand sind; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,*

e) nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht,

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

[…]

28 **Art. 6** Richtlinie (EU) 2016/680 - Unterscheidung verschiedener Kategorien betroffener Personen

Die Mitgliedstaaten sehen vor, dass der Verantwortliche gegebenenfalls und so weit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen klar unterscheidet, darunter:

a) Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden,

b) verurteilte Straftäter,

c) Opfer einer Straftat oder Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und

d) andere Parteien im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den unter den Buchstaben a und b genannten Personen in Kontakt oder in Verbindung stehen.

29 **Art. 10** Richtlinie (EU) 2016/680 - Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung ist nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und

> *a) wenn sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist*
>
> *b) der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder*
>
> *c) wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.*

30 **Art. 20** Richtlinie (EU) 2016/680 - Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene technische und organisatorische Maßnahmen – wie z.B. Pseudonymisierung – trifft, die dafür ausgelegt sind, Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Richtlinie zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Die Mitgliedstaaten sehen vor, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen trifft, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. [3]Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

31 **Art. 35** Richtlinie (EU) 2016/680 - Allgemeine Grundsätze für die Übermittlung personenbezogener Daten

(1) Die Mitgliedstaaten sehen vor, dass jedwede von einer zuständigen Behörde vorgenommene Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation ver-

arbeitet werden sollen, einschließlich der Weiterübermittlung an ein anderes Drittland oder eine andere internationale Organisation, nur unter Einhaltung der nach Maßgabe anderer Bestimmungen dieser Richtlinie erlassenen nationalen Bestimmungen, zulässig ist, wenn die in diesem Kapitel festgelegten Bedingungen eingehalten werden, nämlich

a) die Übermittlung für die in Artikel 1 Absatz 1 genannten Zwecke erforderlich ist;

b) die personenbezogenen Daten an einen Verantwortlichen in einem Drittland oder einer internationalen Organisation, die eine für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde ist, übermittelt werden;

c) in Fällen, in denen personenbezogene Daten aus einem anderen Mitgliedstaat übermittelt oder zur Verfügung gestellt werden, dieser Mitgliedstaat die Übermittlung zuvor in Einklang mit seinem nationalen Recht genehmigt hat;

d) die Kommission gemäß Artikel 36 einen Angemessenheitsbeschluss gefasst hat oder, wenn kein solcher Beschluss vorliegt, geeignete Garantien im Sinne des Artikels 37 erbracht wurden oder bestehen oder, wenn kein Angemessenheitsbeschluss gemäß Artikel 36 vorliegt und keine geeigneten Garantien im Sinne des Artikels 37 vorhanden sind, Ausnahmen für bestimmte Fälle gemäß Artikel 38 anwendbar sind und

e) im Fall der Weiterübermittlung an ein anderes Drittland oder eine andere internationale Organisation die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, oder eine andere zuständige Behörde des gleichen Mitgliedstaats die Weiterübermittlung genehmigt nach gebührender Berücksichtigung sämtlicher maßgeblicher Faktoren, einschließlich der Schwere der Straftat, des Zwecks der ursprünglichen Übermittlung personenbezogener Daten und des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die personenbezogene Daten weiterübermittelt werden.

(2) Die Mitgliedstaaten sehen vor, dass Übermittlungen ohne vorherige Genehmigung durch einen anderen Mitgliedstaat gemäß Absatz 1 Buchstabe c nur dann zulässig sind, wenn die Übermittlung der personenbezogenen Daten erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Die Behörde, die für die Erteilung der vorherigen Genehmigung zuständig ist, wird unverzüglich unterrichtet.

(3) Sämtliche Bestimmungen dieses Kapitels werden angewendet, um sicherzustellen, dass das durch diese Richtlinie gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

32 **Art. 36** Richtlinie (EU) 2016/680 - Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt werden dürfen, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifi-

sche Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlungen bedarf keiner besonderen Genehmigung.

[…]

33 **Art. 37** Richtlinie (EU) 2016/680 - Datenübermittlung vorbehaltlich geeigneter Garantien

(1) Liegt kein Beschluss nach Artikel 36 Absatz 3 vor, so sehen die Mitgliedstaaten vor, dass eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgen darf, wenn

a) in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder

b) der Verantwortliche alle Umstände beurteilt hat, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, und zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen.

[…]

34 **Art. 38** Richtlinie (EU) 2016/680 - Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 36 vorliegt noch geeignete Garantien nach Artikel 37 bestehen, sehen die Mitgliedstaaten vor, dass eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur zulässig ist, wenn die Übermittlung aus einem der folgenden Gründe erforderlich ist

> *a) zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person,*
>
> *b) zur Wahrung berechtigter Interessen der betroffenen Person, wenn dies im Recht des Mitgliedstaats, aus dem die personenbezogenen Daten übermittelt werden, vorgesehen ist,*
>
> *c) zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes,*
>
> *d) im Einzelfall für die in Artikel 1 Absatz 1 genannten Zwecke, oder*
>
> *e) im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in Artikel 1 Absatz 1 genannten Zwecken.*

(2) Personenbezogene Daten dürfen nicht übermittelt werden, wenn die übermittelnde zuständige Behörde feststellt, dass Grundrechte und Grundfreiheiten der betroffenen Person das öffentliche Interesse an der Übermittlung im Sinne des Absatzes 1 Buchstaben d und e überwiegen.

[…]

35 **Art. 59** Richtlinie (EU) 2016/680 - Aufhebung des Rahmenbeschlusses 2008/977/JI

(1) Der Rahmenbeschluss 2008/977/JI wird mit Wirkung vom 6. Mai 2018 aufgehoben.

(2) Verweise auf den in Absatz 1 genannten aufgehobenen Beschluss gelten als Verweise auf diese Richtlinie.

36 Die **DS-GVO** (ABl. EU vom 4. Mai 2016, L 119 S.1) regelt:

37 **Art. 4** DS-GVO - Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

> *1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;*
>
> *[...]*

38 **Art. 9** DS-GVO **-** Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

[...]

39 **Art. 13** DS-GVO - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

> *a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;*
>
> *b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;*
>
> *c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;*
>
> *d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;*

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) *Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.*

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

40 Das **FlugDaG** (BGBl. I S. 1484) regelt:

41 **§ 2** FlugDaG - Datenübermittlung durch Luftfahrtunternehmen

[…]

(2) Fluggastdaten sind folgende Daten:

1. Familienname, Geburtsname, Vornamen und Doktorgrad des Fluggastes,

[…]

9. sonstige Namensangaben,

[…]

(3) Fluggastdaten sind für alle Flüge des Linien-, Charter- und Taxiverkehrs zu übermitteln, die nicht militärischen Zwecken dienen und die

1. von der Bundesrepublik Deutschland aus starten und in einem anderen Staat landen oder

2. von einem anderen Staat aus starten und in der Bundesrepublik Deutschland landen oder zwischenlanden.

42 **§ 17** FlugDaG - Gerichtliche Zuständigkeit, Verfahren

Für gerichtliche Entscheidungen nach diesem Gesetz ist das Amtsgericht zuständig, in dessen Bezirk das Bundeskriminalamt seinen Sitz hat. Für das Verfahren gelten die Bestimmungen des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.

III.

43 Das vorlegende Gericht ist für die Entscheidung des Verwaltungsstreitverfahrens und mithin auch für das vorliegende Vorabentscheidungsersuchen an den Europäischen Gerichtshof zuständig. Dem steht insbesondere nicht § 17 FlugDaG entgegen, wonach für gerichtliche Entscheidungen nach diesem Gesetz das Amtsgericht zuständig ist, in dessen Bezirk das Bundeskriminalamt seinen Sitz hat. „Entscheidungen nach diesem Gesetz“ sind nämlich nur solche nach § 5 Abs. 2 FlugDaG. Vorliegend ist nicht „eine Entscheidung *nach* diesem Gesetz“, sondern eine Entscheidung *über* dieses Gesetz zu treffen.

44 Vorliegend kommt es zur Entscheidung in dem hier vorgelegten Fall darauf an, ob die PNR-Richtlinie oder Teile davon gegen die Grundrechtecharta verstoßen. In diesem Fall wäre das FlugDaG als Umsetzungsgesetz nicht anwendbar, sodass die die Datenverarbeitung insgesamt unzulässig wäre und der Löschungsanspruch bestünde.

Zu Frage 1

45 Die verschiedenen durch die Richtlinie und das Umsetzungsgesetz vorgesehen Verarbeitungen von PNR-Daten greifen in den Schutzbereich des Grundrechts auf Achtung des Privatlebens, das in Art. 7 GRCh garantiert ist, ein. Denn dieses Recht erstreckt sich auf jede Information, die eine bestimmte oder bestimmbare natürliche Person betrifft (vgl. nur EuGH, Urteil vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 52), mithin auch auf die in Anhang I der PNR-Richtlinie genannten Informationen über von der PNR-Daten-Verarbeitung betroffenen Personen. Die in der PNR-Richtlinie vorgesehenen Verarbeitungen der PNR-Daten fallen zudem unter Art. 8 GRCh, weil sie Verarbeitungen personenbezogener Daten im Sinne dieses Artikels darstellen und deshalb zwangsläufig die dort vorgesehenen Erfordernisse des Datenschutzes erfüllen müssen (vgl. nur EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 123).

46 Nach der Rechtsprechung des Europäischen Gerichtshofes stellt die Weitergabe personenbezogener Daten an einen Dritten, etwa eine Behörde, unabhängig von der späteren Verwendung der übermittelten Informationen einen Eingriff in das in Art. 7 GRCh verankerte Grundrecht dar. Dasselbe gilt für die Speicherung personenbezogener Daten und den Zugang zu den Daten zu ihrer Verwendung durch die Behörden. Für die Feststellung eines solchen Eingriffs kommt es nicht darauf an, ob die übermittelten Informationen als sensibel anzusehen sind oder ob die Betroffenen durch den Vorgang irgendwelche Nachteile erlitten haben (vgl. EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 124). Entsprechendes gilt auch für Art. 8 GRCh, soweit es um die Verarbeitung personenbezogener Daten geht. (vgl. EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 126).

47 Zwar können die in den Art. 7 und Art. 8 GRCh niedergelegten Rechte keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden (vgl. EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 136). Eine Einschränkung dieser Rechte kann zur Erreichung von Gemeinwohlzwecken, zu denen die Bekämpfung von terroristischen Straftaten und schwerer Kriminalität zählen (vgl. EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 149), durchaus zulässig sein. Die Eingriffe in die Grundrechte müssen jedoch geeignet und erforderlich zur Erreichung dieser Ziele sein und dürfen sich nicht als unverhältnismäßig im engeren Sinne erweisen. Überdies muss nach Art. 52 Abs. 1 GRCh jede Einschränkung der Ausübung der Unionsgrundrechte und -freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (vgl. EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 138).

48 Der Grundsatz der Verhältnismäßigkeit verlangt nach ständiger Rechtsprechung des Europäischen Gerichtshofes, dass die Handlungen der Unionsorgane geeignet sind, die **mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen**, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist (EuGH, Urteil vom 8. April 2014, Digital Rights Ireland u.a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 46). In Bezug auf das Grundrecht auf Achtung des Privatlebens ist nach der Rechtsprechung des EuGH zu verlangen, dass sich die Ausnahmen

und Einschränkungen in Bezug auf den Schutz personenbezogener Daten **auf das absolut Notwendige beschränken** (EuGH, Urteil vom 8. April 2014, Digital Rights Ireland u.a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 52).

49 Um diesem Erfordernis zu genügen, muss die Regelung, die den Eingriff enthält, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen. Die Personen, deren Daten übermittelt wurden, müssen über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Die Regelung 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 (EuGH, Urteil vom 8. April 2014, Digital Rights Ireland u.a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 54 f.). Es bestehen ernsthafte Zweifel, ob die PNR-Richtlinie diesen Anforderungen in jeder Hinsicht gerecht wird.

50 Nach den Bestimmungen der PNR-Richtlinie sind die Luftfahrtunternehmen dazu verpflichtet, bei jedem einzelnen Flug die PNR-Daten ausnahmslos aller Fluggäste an die PNR-Zentralstellen der Mitgliedstaaten zu übermitteln, bei denen diese Daten automatisiert verarbeitet und dauerhaft gespeichert werden. Eines bestimmten Anlasses, beispielweise konkreter Anhaltspunkte für eine Verbindung zum internationalen Terrorismus oder zu organisierter Kriminalität, bedarf es dabei nicht. Dies führt dazu, dass innerhalb kurzer Zeiträume hunderte Billionen Datensätze verarbeitet und gespeichert werden. Die „Vorratsdatenspeicherung“ von Fluggastdaten betrifft daher die Grundrechte eines sehr weiten Teils der gesamten europäischen Bevölkerung in evidenter Weise (siehe allein das touristische Flugaufkommen vor der sogenannten Corona-Krise; schon 226.764.086 beförderte Personen im Luftverkehr 2019 in Deutschland, 47 Millionen weltweite Flüge im Jahr 2019; innerhalb der Europäischen Union 928.634.652 Passagiere im Jahr 2019, wobei ein jeder Flug zur Erfassung führt – bei 513,5 Millionen Einwohnern der Europäischen Union im Jahr 2019, https://ec.europa.eu/eurostat/databrowser/view/ttr00012/default/table?lang=de, Stand 1. Mai 2020).

51 Die zu übermittelnden Datensätze, die durch Art. 8 Abs. 1 Satz 1 i.V.m. Anhang I PNR-Richtlinie vorgegeben werden, sind sehr umfangreich und umfassen neben den Namen und Adressen der Fluggäste sowie dem gesamten Reiseverlauf auch Angaben über ihr Gepäck, ihre Mitreisenden, alle Arten von Zahlungsinformationen sowie nicht näher definierte „allgemeine Hinweise“. Aus der Gesamtheit dieser Daten lassen sich sehr genaue Rückschlüsse auf das Privat- und Geschäftsleben der betroffenen Personen ziehen. Aus ihnen ergibt sich nämlich, wer wann in wessen Begleitung wohin gereist ist, welches Zahlungsmittel dabei genutzt und welche Kontaktdaten angegeben wurden und ob die betroffene Person mit leichtem oder schwerem Gepäck gereist ist. Über das Freitextfeld der „allgemeinen Hinweise“ können noch weitere Daten, deren Umfang völlig unklar ist (dazu weiter unten), anfallen.

52 Das vorlegende Gericht sieht hier eine Vergleichbarkeit der PNR-Daten-Verarbeitung und -speicherung mit der Vorratsdatenspeicherung im Telekommunikationsbereich. Zu dieser hat der Europäische Gerichtshof richtigerweise ausgeführt, dass sie einen Eingriff

von großem Ausmaß und besonderer Schwere in die Art. 7 und Art. 8 GRCh darstellt. Denn eine massenhafte, anlasslose Speicherung umfangreicher Datensätze, die Rückschlüsse auf das Privat- und Geschäftsleben der betroffenen Personen zulassen, sind geeignet, bei ihnen ein Gefühl ständiger Überwachung zu erzeugen (EuGH, Urteil vom 8. April 2014, Digital Rights Ireland u.a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 37).

53 In seinem ersten Urteil zur Vorratsdatenspeicherung hat der EuGH selbige unter anderem deshalb für grundrechtswidrig erachtet, weil auch Daten von Personen auf Vorrat gespeichert werden sollen, bei denen keinerlei Anhaltspunkte dafür vorliegen, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte (EuGH, Urteil vom 8. April 2014, Digital Rights Ireland u.a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 58). Dies trifft auf die Verarbeitung und Speicherung von PNR-Daten ebenfalls zu, was zeigt, dass die Regelungen der PNR-Richtlinie die Grenzen dessen überschreiten, was zur Erreichung der Ziele der PNR-Richtlinie erforderlich ist, und somit unverhältnismäßig im Sinne der Rechtsprechung des Europäischen Gerichtshofes sind. Hinzu kommt, dass die PNR-Daten, anders als die Telekommunikationsverkehrsdaten im Rahmen der Vorratsdatenspeicherung, nicht nur anlasslos gespeichert, sondern auch weiterverarbeitet, das heißt automatisiert mit Datenbanken und sog. „Mustern“ abgeglichen werden.

Zu Frage 2 a) „schwere Kriminalität“

54 Fraglich ist auch die Bestimmtheit und Verhältnismäßigkeit der Erhebung und Verarbeitung der umfangreichen Datensätze im Hinblick auf die Delikte, die durch dieses Vorgehen bekämpft werden sollen. Erklärtes Ziel der PNR-Richtlinie ist die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Art. 3 Nr. 9 PNR-Richtlinie definiert schwere Kriminalität als die in Anhang II aufgeführten strafbaren Handlungen, die nach dem nationalen Recht eines Mitgliedstaates mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind. In Anhang II zur PNR-Richtlinie ist eine Liste von 26 strafbaren Handlungen gemäß Art. 3 Nr. 9 PNR-Richtlinie enthalten. Hierzu zählen beispielsweise Korruption (Nr. 6), Betrugsdelikte (Nr. 7), Computerstraftaten/Cyberkriminalität (Nr. 9) sowie Umweltkriminalität (Nr. 10).

55 Zunächst steht hier die Bestimmtheit der Regelungen in Frage. So kennt das deutsche Strafrecht beispielsweise keinen Straftatbestand der „Korruption“. Korruption bildet vielmehr einen Oberbegriff für eine Vielzahl von denkbaren Straftaten. Für nationale Behörden ist somit nicht eindeutig und klar definiert, welche Delikte genau unter diese Regelung fallen sollen. Selbiges gilt auch für die die Begriffe der „Betrugsdelikte“, „Computerstraftaten“ und „Umweltkriminalität“. Unter alle diese Begriffe kann eine Mehrzahl von mehr oder weniger konkreten Delikten subsummiert werden.

56 Dies und die Bezugnahme auf das jeweilige Strafmaß in den einzelnen Mitgliedstaaten in Art. 3 Nr. 9 PNR-Richtlinie führen dazu, dass die PNR-Daten in unterschiedlichen Mitgliedstaaten der Union uneinheitlich verwendet werden, da es nämlich den strafrechtlichen Regelungen der einzelnen Mitgliedstaaten überlassen bleibt, bestimmte Delikte über die jeweilige Strafandrohung im nationalen Strafgesetzbuch als „schwere Kriminalität“ im Sinne der Richtlinie zu erfassen oder eben nicht.

57 Zweifelhaft ist im Hinblick auf die Angemessenheit der Regelung zudem die in Art. 3 Nr. 9 PNR-Richtlinie festgelegte „Mindestgrenze“ der Strafandrohung von im Höchstmaß drei Jahren Freiheitsstrafe. Denn diese Regelung ist sehr weitgehend.

58 Nach dem deutschen Strafrecht ist davon eine enorme Vielzahl von Delikten erfasst, deren Einordnung als „schwere Kriminalität“ sehr fragwürdig erscheint. So beträgt gemäß § 263 des deutschen Strafgesetzbuches (StGB) der Strafrahmen für einen gewöhnlichen Betrug bereits bis zu fünf Jahren Freiheitsstrafe. Gleiches gilt beispielsweise für die Hehlerei (§ 259 StGB), den Computerbetrug (§ 263a StGB) oder die Untreue (§ 266 StGB). Alle diese Delikte lassen sich unter den Katalog strafbarer Handlungen im Anhang II PNR-Richtlinie, dort insbesondere Nr. 6 „Betrugsdelikte“ subsummieren. Solche Delikte zählen jedoch zur vielfach auftretenden „Alltagskriminalität“ und können auch und gerade in minderschweren Fällen auftreten. Dann aber hat ihre Erfassung durch die PNR-Richtlinie mit der Bekämpfung von Terrorismus und auch der Verhinderung bzw. Bekämpfung und Verfolgung von schwerer Kriminalität, die in diesem Zusammenhang als Pendent zu terroristischen Straftaten auch ein vergleichbares Gewicht haben müsste, nichts zu tun und müsste unterlassen werden.

59 Das vorlegende Gericht hat erhebliche Bedenken, ob eine – von der Buchung einer Flugreise abgesehen – anlasslose Erhebung einer so großen Vielzahl von Daten zur Verfolgung auch solcher verhältnismäßig geringfügiger und nicht konkret bestimmter Straftaten noch als angemessen betrachtet werden kann. Es drängt sich für das vorlegende Gericht der Eindruck auf, dass die Richtlinie weniger der Bekämpfung von Terrorismus und schwerer Kriminalität dient, sondern vielmehr darauf ausgelegt ist eine Vielzahl von eher mittel- oder minderschweren Straftaten als „Beifang“ verfolgen zu können (so auch bei der Richtline (EU) 2015/849 in der Fassung der Richtline (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, welche in der praktischen Umsetzung im Wesentlichen der Aufdeckung von Steuerdelikten, wie Erbschaftssteuerhinterziehung, also gerade nicht der Terrorismusfinanzierung führt; siehe dazu Antwort des Bundesministeriums der Finanzen auf die Kleine Anfrage des Abgeordneten Fabia De Masi vom 26. Juli 2018, Nr. 3 h), wonach keine Erkenntnisse der Terrorismusfinanzierung bekannt sind, https://www.linksfraktion.de/fileadmin/user_upload/PDF_Dokumente/180814-Antwort-KA-Geldwa-schebeka-mpfung-193586.pdf, Stand 1. Mai 2020).

60 Zumindest hat der Richtliniengeber in Art. 3 des Fluggastdaten-Abkommens zwischen der EU und Australien (Abkommen zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records - PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service vom 14.7.2012 (ABl. Nr. L 186 S. 4, ber. Abl. Nr. L 302 S. 14)) eine Regelung vorgesehen, nach der neben terroristischen nur schwere *grenzüberschreitende* Straftaten vorgebeugt, aufgedeckt, untersucht oder verfolgt werden sollen. Auch eine solche Einschränkung wurde in der PNR-Richtlinie nicht vorgesehen, auch wenn sich hier das gleiche Problem der Konkretisierung der einzelnen Straftatbestände ergibt. So entsteht der Eindruck, dass es Ziel der Formulierung der Richtlinie war, sie bewusst sehr weit zu fassen. Vor dem Hintergrund der Einschränkung der Grundrechte und der Rechtspre-

chung des Europäischen Gerichtshofes, der bei ihrer Auslegung eine Beschränkung auf das absolut Notwendige fordert, erscheint dies mehr als sehr fragwürdig.

Frage 2 b) Bestimmtheit der PNR-Daten

61 Die hinreichende Bestimmtheit einiger Formulierungen der laut des Kataloges in Anhang I PNR-Richtlinie von den Luftfahrtunternehmen an die PNR-Zentralstellen der Mitgliedstaaten zu übermittelnden PNR-Daten ist vor dem Hintergrund, dass der Gerichtshof in seiner ständigen Rechtsprechung klare und präzise Regelungen für die Tragweite und Anwendung der betreffenden Maßnahmen einfordert (vgl. nur EuGH-Gutachten 1/15 vom. 27. Juli 2017, EU:C:2017:592, Rn. 141), nicht gegeben.

62 Es ist nicht klar ersichtlich, was mit dem zu übermittelnden „Name(n)“ (Anhang I Nr. 4 PNR-Richtlinie) gemeint ist. Dies wird an der deutschen Umsetzung durch § 2 Nr. 1 und Nr. 9 FlugDaG, wonach der Familienname, der Geburtsname, die Vornamen und ein eventuell bestehender Doktorgrad sowie sonstige Namensabgaben übermittelt werden sollen, gut ersichtlich. Im allgemeinen Sprachgebrauch wird auf die Frage nach dem Namen üblicherweise nicht auch der Geburtsname genannt. So bleibt unklar, ob dieser unter die von Anhang I Nr. 4 PNR-Richtlinie gemeinten Name(n) fällt. Fraglich ist auch, ob ein akademischer Titel als Namensbestandteil im Sinne der Richtlinie anzusehen ist.

63 Hinsichtlich der Übermittlung und Verarbeitung von Daten zu Vielflieger-Einträgen (Anhang I Nr. 8 PNR-Richtlinie) liegt ebenfalls eine Unbestimmtheit der Regelung vor. Denn es ist nicht klar ersichtlich, was unter diesen Begriff zu fassen sein soll. Insbesondere ist unklar, ob lediglich die Teilnahme an Bonusprogrammen für Vielflieger an sich oder aber auch konkrete Informationen über Flüge und Buchungen der an einem solchen Programm teilnehmenden Person gemeint sind.

64 Die Formulierung „allgemeine Hinweise, einschließlich […]“ in Anhang I Nr. 12 PNR-Richtlinie ist sehr weit gefasst und nicht greifbar. Wie aus dem Wort *einschließlich* hervorgeht, handelt es sich nur um eine beispielhafte, nicht abschließende Aufzählung. Zudem könnten beim Ausfüllen dieses Freitextfeldes auch Informationen mitgeteilt werden, die keinerlei Bezug zum Zweck der Erhebung der Fluggastdaten haben (so auch schon EuGH-Gutachten 1/15 vom. 27. Juli 2017, EU:C:2017:592, Rn. 160). Die Formulierung könnte insbesondere auch erlauben, Informationen zu übermitteln, die die PNR-Richtlinie nicht zulassen will, nämlich insbesondere sensible Daten, die ausweislich des Erwägungsgrundes Nr. 15 zur PNR-Richtlinie nicht erhoben werden sollen (siehe hierzu auch Frage 4).

Zu Frage 2 c) Drittbetroffene

65 Gemäß Art. 1 Abs. 1 PNR-Richtlinie soll diese die Übermittlung von PNR-Daten zu Fluggästen von Drittstaatsflügen durch Fluggesellschaften und die Verarbeitung dieser Daten durch die Mitgliedstaaten regeln. Gemäß Art. 3 Nr. 4 PNR-Richtlinie ist Fluggast jede Person, einschließlich Transfer- oder Transitfluggästen, mit Ausnahme der Besatzungsmitglieder, die mit Zustimmung der Fluggesellschaft in einem Luftfahrzeug befördert wird oder befördert werden soll, wobei diese Zustimmung durch die Eintragung der Person in die Fluggastliste belegt wird. In Anhang I der PNR-Richtlinie finden sich jedoch mehrere im Rahmen der Fluggastdatenverarbeitung zu übermittelnde Daten, die nicht zu den so definierten „Fluggästen“ gehören. Insoweit sind die Regelungen der PNR-Richtlinie in sich widersprüchlich.

66 So widerspricht es Art. 3 Nr. 4 PNR-Richtlinie, wenn Anhang I Nr. 9 PNR-Richtlinie vorsieht, im Rahmen der Fluggastdatenverarbeitung Informationen zum Reisebüro und dem dortigen Sachbearbeiter zu erfassen. Nach Anhang I Nr. 12 der PNR-Richtlinie sind im Freitextfeld der „Allgemeinen Hinweise“ insbesondere Informationen zu den Begleitpersonen von Minderjährigen bei Abflug und Ankunft sowie zu begleitenden Flughafenmitarbeitern zu übermitteln.

67 Alle genannten Daten fallen ersichtlich nicht unter die in Art. 3 Nr. 4 PNR-Richtlinie definierten Gruppe der Fluggäste. Gleichwohl sollen sie betreffende Daten im direkten Widerspruch zum Wortlaut der eigenen Definition der PNR-Richtlinie auf der Basis der PNR-Richtlinie (hier Anhang I) durch die Luftfahrtunternehmen an die PNR-Zentralstellen der Mitgliedstaaten übermittelt und dort gespeichert werden. Insofern geht das vorlegende Gericht davon aus, dass sich diese Regelungen allesamt nicht auf das absolut Notwendige im Sinne der Rechtsprechung des Europäischen Gerichtshofes beschränken (vgl. nur EuGH-Gutachten 1/15 vom. 27. Juli 2017, EU:C:2017:592, Rn. 141). Für alle Drittbetroffenen stellt sich zudem die Frage, wie sie über die Verarbeitung ihrer personenbezogenen Daten nach Art. 14 DS-GVO informiert werden sollen.

68 Gemäß Anhang I Nr. 17 PNR-Richtlinie sollen auch die PNR-Daten von Mitreisenden der Fluggäste übermittelt und verarbeitet werden. Hinsichtlich der Mitreisenden führt dies zu einer Doppelerfassung, da diese als Fluggäste ja ohnehin bereits von der Fluggastdatenverarbeitung betroffen werden. Mithin wird hier gravierend gegen das Gebot der Datenminimierung verstoßen (vgl. Art. 5 lit. c) DS-GVO).

Zu Frage 2 d) Minderjährige

69 Nach der PNR-Richtlinie haben die Luftfahrtunternehmen die PNR-Daten ausnahmslos aller Fluggäste an die jeweiligen PNR-Zentralstellen der Mitgliedstaaten zu übermitteln, sodass auch minderjährige Fluggäste betroffen sind. Durch Anhang I Nr. 12 PNR-Richtlinie, der die Übermittlung *„allgemeine[r] Hinweise, einschließlich aller verfügbaren Daten zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen […]“* vorsieht, wird dies nochmals unterstrichen.

70 Die Verarbeitung von Daten von Minderjährigen kann einerseits zum Zweck präventiven und/oder repressiven Vorgehens gegen Minderjährige, die (mutmaßlich) in Terrorismus oder schwere Kriminalität verstrickt sind, erfolgen und andererseits aus Gründen des Minderjährigenschutzes, beispielsweise um der Aufdeckung oder Verfolgung von Kinderhandel zu dienen. Diese beiden unterschiedlichen Zielsetzungen erfordern differenzierte Regelungen. Dies verdeutlicht Art. 6 Richtlinie (EU) 2016/680. Dieser regelt, dass, soweit möglich, zwischen den personenbezogenen Daten verschiedener Kategorien klar zu unterscheiden ist. Zu diesen zu unterscheidenden Kategorien zählen insbesondere Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in absehbarer Zeit begehen werden (Art. 6 lit. a) Richtlinie (EU) 2016/680) und Opfer einer Straftat oder Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten (Art. 6 lit. c) Richtlinie (EU) 2016/680; siehe auch Erwägungsgrund 31 der Richtlinie (EU) 2016/680).

71 Soweit die Daten zum Zweck des repressiven oder präventiven Vorgehens gegen Minderjährige erhoben und verarbeitet werden, wäre aber zu beachten, dass eine Strafverfolgung aufgrund von Erkenntnissen aus der Fluggastdatenverarbeitung ohnehin nur bei

bereits strafmündigen Jugendlichen in Betracht kommt. Insoweit geht die PNR-Richtlinie über das absolut Notwendige hinaus, da sie eine Beschränkung zum Beispiel auf die Daten strafmündiger Minderjähriger nicht enthält.

72 In Bezug auf die Erhebung und Verarbeitung von PNR-Daten zum Zweck des Minderjährigenschutzes ist zu beachten, dass Kinder und Jugendliche besonders schutzbedürftig sind. Dies verdeutlicht Art. 24 GRCh, der ihnen zu ihrem besonderen Schutz eigene Unionsgrundrechte einräumt. Diese besondere Schutzbedürftigkeit gilt auch im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten. Soweit die Erhebung und Verarbeitung von PNR-Daten minderjähriger Fluggäste der Verhinderung bzw. Verfolgung von Kriminalität gegen die betroffenen Minderjährigen dienen sollen, die sich gegen Kinder richtet, so erscheinen die Regelungen der PNR-Richtlinie hierfür nicht geeignet zu sein. Die PNR-Datenverarbeitung ist auf das Auffinden bzw. Erkennen von verdächtigen Personen ausgerichtet. Hierzu werden die PNR-Daten automatisiert mit Datenbanken und Mustern abgeglichen, **um verdächtige Personen ausfindig** machen zu können, vgl. Art 6 Abs. 2 PNR-Richtlinie. Die Daten der Minderjährigen sind im Kontext des Schutzes Minderjähriger vor Kinderhandel aber gerade keine Daten von Verdächtigen, sondern im Gegenteil von Schutzbedürftigen. Daher müssten sie auch anders behandelt werden. Die Notwendigkeit von Musterabgleichen besteht dann gerade nicht. Insoweit fehlt es der PNR-Richtlinie in Bezug auf den Umgang mit den PNR-Daten minderjähriger Fluggäste offensichtlich an hinreichend differenzierten Regelungen.

Zu Frage 2 e) API-Daten

73 Art. 8 Abs. 2 PNR-Richtlinie regelt, dass die Mitgliedstaaten die erforderlichen Maßnahmen zu treffen haben, um sicherzustellen, dass auch erweiterte Fluggastdaten im Sinne von Anhang I Nr. 18 PNR-Richtlinie (API-Daten), auch wenn sie durch die Luftfahrtunternehmen in technisch anderer Weise vorgehalten werden sollten, als die zu übermittelnden PNR-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 an die PNR-Zentralstellen übermittelt werden. Insoweit bestehen zahlreiche Überschneidungen der API-Daten mit den ohnehin zu übermittelnden PNR-Daten, wie den planmäßigen Abflugdaten (Anhang I Nr. 3 PNR-Richtlinie), den Namen (Anhang I Nr. 4 PNR-Richtlinie) oder dem gesamten Reiseverlauf (Anhang I Nr. 7 PNR-Richtlinie).

74 Diese doppelte oder mehrfache Verarbeitung der Fluggastdaten steht im Widerspruch zu dem unter anderem in der Richtlinie (EU) 2016/680 verankerten Grundsatz der Datensparsamkeit. Dieser lässt sich zunächst aus dem Art. 4 Abs. 1 lit. c) Richtlinie (EU) 2016/680 entnehmen, welcher regelt, dass personenbezogene Daten in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sein sollen. Art. 20 Abs. 1 Richtlinie (EU) 2016/680 konkretisiert diesen Grundsatz dahingehend, dass die Mitgliedstaaten vorsehen sollen, dass der für die Datenverarbeitung Verantwortliche Maßnahmen trifft, um die Datenschutzgrundsätze wie etwa die Datenminimierung wirksam umzusetzen. Zudem regelt Art. 20 Abs. 2 Richtlinie (EU) 2016/680, dass nur personenbezogene Daten, deren Verarbeitung für den jeweiligen Verarbeitungszweck erforderlich sind, verarbeitet werden sollen.

75 Eine doppelte Verarbeitung bestimmter inhaltlich identischer Daten, nämlich sowohl aus PNR-Daten als auch als API-Daten gleichen Inhalts, ist mit dem Grundsatz der Daten-

minimierung bzw. Datensparsamkeit nicht in Einklang zu bringen und somit nicht erforderlich. Ein zwingender Grund für ein solches Vorgehen ist nicht erkennbar. Aufgrund der doppelten Erfassung und Verarbeitung dieser Daten beschränkt sich der mit der Übermittlung dieser Daten an die PNR-Zentralstellen der Mitgliedstaaten und die dortige Verwendung verbundene Eingriff in Art. 7 und Art. 8 GRCh daher nach Ansicht des vorlegenden Gerichts nicht auf das absolut Notwendige.

Zu Frage 2 f) Rechtsgrundlage für Muster

76 Gemäß Art. 6 Abs. 3 lit. b) PNR-Richtlinie sollen die durch die Luftfahrtunternehmen an die PNR-Zentralstellen der Mitgliedstaaten übermittelten Datensätze mit im Voraus festgelegten Kriterien (sog. Mustern) abgeglichen werden. In Art. 6 Abs. 4 Satz 2 und 4 PNR-Richtlinie ist bestimmt, dass die im Voraus festgelegten Kriterien zielgerichtet, verhältnismäßig und bestimmt sein müssen und Grundlage für diese Kriterien nicht 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 sein dürfen. Die Erstellung der Muster ist gemäß Art. 6 Abs. 4 Satz 3 PNR-Richtlinie Aufgabe der jeweiligen PNR-Zentralstellen der Mitgliedstaaten.

77 Die gesamte Ausgestaltung des Musterabgleiches bleibt also inhaltlich vollständig der Exekutive der einzelnen Mitgliedstaaten überlassen. Dies muss dazu führen, dass die Mitgliedstaaten der Union unterschiedliche Muster verwenden und Fluggäste damit abhängig vom Reiseziel unterschiedlichen Mustern unterworfen werden, die zu völlig unterschiedlichen Ergebnissen führen können.

78 Es ist fraglich, ob dies mit Art. 8 Abs. 2 und Art. 52 GRCh sowie Art. 16 Abs. 2 AEUV vereinbar ist. Gemäß Art. 8 Abs. 2 GRCh dürfen personenbezogene Daten nur nach Treu und Glauben **für festgelegte Zwecke** und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Nach Art. 52 Abs. 1 Satz 1 GRCh muss jede Einschränkung der Ausübung der in der Grundrechtecharta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein. Gemäß Art. 16 Abs. 2 AEUV erlassen das Europäische Parlament und der Rat **gemäß dem ordentlichen Gesetzgebungsverfahren** Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstige Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen.

79 Es gilt somit zur Rechtfertigung von Eingriffen in die Unionsgrundrechte im Allgemeinen und in Art. 8 GRCh im Besonderen der Vorbehalt des Gesetzes. Um diesem Erfordernis zu genügen, ist nicht nur die Existenz irgendeiner gesetzlichen Regelung erforderlich, vielmehr muss diese auch hinreichend bestimmt sein (vgl. nur EuGH, Urteil vom 21. Dezember 2016, AGET Iraklis, C-201/15, ECLI:EU:C:2016:972, Rn. 99). Der Gesetzesunterworfene muss die Gesetzesfolgen vorhersehen können, wobei eine offene Regelung hinzunehmen ist, wenn eine genauere Regelung für den Regelungsgegenstand nicht möglich ist (EuGH, Urteil vom 20. Mai 2003, Österreichischer Rundfunk u.a., C-465/00, C-138/01 und C-139/01, ECLI:EU:C:2003:294, Rn. 77).

80 Diese Vorgaben erfüllt Art. 6 Abs. 4 PNR-Richtlinie nicht. Bei Art. 6 Abs. 4 Satz 2 PNR-Richtlinie handelt es sich um unbestimmte Worthülsen, mit denen eine Konkretisierung der Kriterien vorgetäuscht wird, die in Wahrheit gar nicht existiert. Aus den Schlagwor-

ten der Zielgerichtetheit, Bestimmtheit und Verhältnismäßigkeit lässt sich nichts Greifbares für die Erstellung der Muster schlussfolgern. Es bleibt völlig ungeklärt, wie die zu entwickelnden „Algorithmen“ eine unzulässige Diskriminierung, wie sie auch Art. 13 Abs. 4 PNR-Richtlinie explizit untersagt, zuverlässig ausschließen sollen. Art. 6 Abs. 4 Satz 3 PNR-Richtlinie überlässt die wesentliche und grundsätzlich bedeutsame Entscheidung, welche Daten für die Erstellung von Kriterien bzw. Mustern für den automatisierten Abgleich verwendet werden sollen, vollständig den einzelnen Mitgliedstaaten. Dies ist indes nicht aufgrund des Regelungsgegenstandes zwingend notwendig. Es wäre dem Europäischen Gesetzgeber ohne weiteres möglich gewesen, bestimmte Daten bzw. Kriterien zu benennen, die bei der Mustererstellung zu verwenden oder nicht zu verwenden sein sollen. Insoweit unterscheiden sich weder die in den einzelnen Mitgliedstaaten stattfindende Kriminalität bzw. der Terrorismus, noch die Kriterien, nach denen Verdächtige ausfindig gemacht werden können, von einem Mitgliedstaat zum anderen. Dies insbesondere, da die zu verarbeitenden PNR-Daten schon aufgrund der grenzüberschreitenden Reise der betroffenen Personen zwingend einen gewissen innereuropäischen und internationalen Kontext haben.

81 Als einzigen Kontrollmechanismus für die Verhältnismäßigkeit der von den Mitgliedstaaten erdachten Muster sieht Art. 6 Abs. 7 in Verbindung mit Art. 5 PNR-Richtlinie vor, dass der Datenschutzbeauftragte der PNR-Zentralstelle Zugang zu ihnen erhält. Der Datenschutzbeauftragte wird jedoch gemäß Art. 5 Abs. 1 PNR-Richtlinie von der PNR-Zentralstelle selbst ernannt und ist in der Regel bei dieser beschäftigt, sodass seine Unabhängigkeit von vornherein nicht gewährleistet ist (zur Unabhängigkeit der Datenschutzaufsichtsbehörde siehe EuGH, Urteil vom 9. März 2010, Kommission/Deutschland, C-518/07, sowie Urteil vom 16. Oktober 2012, Kommission/Österreich, C-614/10, EU:C:2012:631). Insofern ist der Zugang des Datenschutzbeauftragten keine hinreichende Garantie für die Verhältnismäßigkeit der von den einzelnen Mitgliedstaaten bzw. ihren PNR-Zentralstellen verwendeten Muster. Hier ist nach der Auffassung des vorlegenden Gerichts eine Regelung in der PNR-Richtlinie selbst erforderlich und für den Regelungsgegenstand auch möglich.

Zu Frage 2 g) Speicherdauer

82 Gemäß Art. 12 Abs. 1 PNR-Richtlinie werden die durch die Luftfahrtunternehmen erhobenen und durch die PNR-Zentralstellen der Mitgliedstaaten verarbeiteten PNR-Daten für einen Zeitraum von fünf Jahren gespeichert. Nach dem Erwägungsgrund 25 der PNR-Richtlinie soll das Wesen der PNR-Daten und ihr Verarbeitungszweck es mit sich bringen, dass diese so lange gespeichert werden müssen, wie nötig. Warum dies der Fall sein soll und warum eine Speicherdauer von fünf Jahren notwendig sein soll, wird jedoch gerade nicht aufgeführt.

83 Es ist nicht ersichtlich und begründet, warum solche langen Speicherungszeiten erforderlich sind. Nachdem die Fluggäste vor ihrer planmäßigen Einreise in einen Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat gemäß Art. 6 Abs. 4 Satz 1 PNR-Richtlinie überprüft wurden, ohne dass es hierbei zu Treffern oder anderen Auffälligkeiten gekommen wäre, besteht keinerlei objektiver Anhaltspunkt dafür, dass sie in einem auch nur mittelbaren Zusammenhang mit terroristischen Straftaten oder schwerer Kriminalität stehen könnten. Somit fehlt es am hinreichenden Zusammenhang zwischen der Speicherung der Datensätze und den mit der PNR-Richtlinie verfolgten Zielen. Nur im Falle von konkreten Anhaltspunkten für eine Gefährdung durch bestimmte Flugpassa-

giere erscheint eine dauerhafte Speicherung als angemessen (vgl. EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 204 ff.). Die **bloße theoretische Möglichkeit**, dass die Daten irgendwann einmal sicherheitsrelevant werden könnten, dürfte hingegen nicht ausreichen, um den anlasslosen und tiefgreifenden Grundrechtseingriff der jahrelangen Speicherung personenbezogener Daten zu rechtfertigen.

84 Die lange Speicherdauer ist auch nicht erforderlich und damit unverhältnismäßig, da die Ziele der Fluggastdatenspeicherung durch mildere Maßnahmen erreicht werden können.

85 So ist die Speicherdauer allgemein zu verkürzen. Der Europäische Gerichtshof hat bereits im Zusammenhang mit der Vorratsdatenspeicherung – einer anderen Form der anlasslosen, massenhaften Speicherung personenbezogener Daten – festgestellt, dass eine Richtlinie, die eine Speicherdauer von bis zu 24 Monaten vorsieht, den Eingriff nicht auf das absolut Notwendige beschränkt (EuGH, Urteil vom 8. April 2014, Digital Rights Ireland u.a., C-293/12 und C-594/12, ECLI:EU:2014:238, Rn. 63). Wenn schon 24 Monate im Falle der Vorratsdatenspeicherung zu lang sind, so sind dies erst Recht fünf Jahre, wie vorliegend.

86 Soweit es überhaupt eine sachliche Begründung für eine längere Speicherdauer gäbe, könnte vorgesehen werden, dass in Fällen, in denen der automatisierte Abgleich keinen „Treffer“ produziert hat und eine individuelle Untersuchung insofern nicht stattfindet, eine Löschung oder zumindest eine umgehende Anonymisierung der PNR-Daten zu erfolgen hat. Eine solche Differenzierung sieht die PNR-Richtlinie jedoch nicht vor. Schon in seinem ersten Urteil zur Vorratsdatenspeicherung hat der der Europäische Gerichtshof jedoch die Wichtigkeit der Unterscheidung zwischen verschiedenen Datenkategorien nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder anhand der betroffenen Personen betont (EuGH, Urteil vom 8. April 2014, Digital Rights Ireland u.a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 63). Ohne diese Differenzierung überschreitet die in der PNR-Richtlinie vorgesehene Speicherungsdauer von fünf Jahren die Grenze dessen, was als absolut notwendig zur Erreichung ihrer Ziele angesehen werden kann. Hieran ändert auch die sogenannte Depersonalisierung nichts.

Zu Frage 2 h) Depersonalisierung

87 Die sogenannte Depersonalisierung soll nach dem Erwägungsgrund 25 der PNR-Richtlinie ein hohes Datenschutzniveau gewährleisten. Dies erscheint äußerst zweifelhaft. Die in Art 12 Abs. 2 PNR-Richtlinie so bezeichnete „Depersonalisierung“ der Datensätze, welche nach sechs Monaten erfolgen soll, ändert an der Unverhältnismäßigkeit der Speicherdauer nichts.

88 Zunächst ist dabei festzustellen, dass die Bezeichnung als „Depersonalisierung“ systemfremd und irreführend ist. Es handelt sich schlicht um eine Pseudonymisierung der Daten im Sinne von Art. 3 Nr. 5 Richtlinie (EU) 2016/680 nebst Anlage I. Diese unterscheidet sich von einer Anonymisierung dadurch, dass anders als bei dieser, eine Zuordnung der Daten zu einer bestimmten Person nicht dauerhaft und endgültig unmöglich gemacht wird, sondern eine De-Depersonalisierung (vgl. Art. 12 Abs. 3 PNR-Richtlinie) möglich bleibt, also ein unmittelbarer Personenbezug ohne Probleme wieder hergestellt werden kann. Unklar ist daher, warum nicht der Begriff der Pseudonymisierung, wie er auch in der Richtlinie (EU) 2016/680 verwendet wird, genutzt wird. Eine Pseudonymisie-

rung vermindert aber die Intensität des Grundrechtseingriffs aufgrund ihrer Umkehrbarkeit erheblich weniger als eine echte Anonymisierung.

89 Zudem ist Art. 4 Abs. 1 lit. e) Richtlinie (EU) 2016/680 zu beachten. Nach dieser Vorschrift sollen personenbezogene Daten nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht. Im Falle der in Art. 12 Abs. 2 PNR-Richtlinie so bezeichneten Depersonalisierung bleibt eine Identifizierung der betroffenen Person während der gesamten fünfjährigen Speicherdauer möglich, wie auch Art. 12 Abs. 3 PNR-Richtlinie, der die (Wieder-)Offenlegung nach Ablauf von sechs Monaten regelt, belegt. Dass dies für die Zwecke der PNR-Richtlinie zwingend erforderlich wäre, ist aber nicht ersichtlich und vom Richtliniengeber auch nicht begründet worden. Wie bereits ausgeführt, besteht bei Betroffenen, deren Daten im Rahmen des automatisierten Abgleiches mit Datenbanken und Mustern völlig unauffällig geblieben sind, allenfalls eine rein theoretische Möglichkeit, dass ihre Daten einmal sicherheitsrelevant werden könnten. Eine solche theoretische Möglichkeit ist jedoch nicht ausreichend, um eine jahrelange Speicherung der Daten in einer Art und Weise, die die Identifizierung der Betroffenen ermöglicht, zu rechtfertigen.

Zu Frage 2 i) Benachrichtigung nach De-Depersonalisierung

90 In der PNR-Richtlinie gibt es keine Regelung, die vorsehen würde, dass Betroffene darüber zu informieren wären, wenn ihre durch die PNR-Zentralstellen der Mitgliedstaaten gespeicherten Daten gemäß Art. 12 Abs. 3 PNR-Richtlinie de-depersonalisiert werden. Geregelt ist lediglich, dass die De-Depersonalisierung durch eine „Justizbehörde“ oder eine andere nationale Behörde genehmigt werden muss (Art. 12 Abs. 3 lit. b) PNR-Richtlinie).

91 Der Europäische Gerichtshof hat bereits in seinem Gutachten zum EU-Kanada-Abkommen ausgeführt, dass nach diesem geplanten Abkommen die Fluggäste zwar über die generelle Verarbeitung ihrer Daten im Rahmen von Sicherheits- und Grenzkontrollen über eine Webseite informiert werden sollten, dass sie jedoch durch diese allgemeine Information nicht erfahren konnten, ob ihre Daten über diese Kontrollen hinaus von den zuständigen Behörden verwendet werden (EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 223). Weiter heißt es im Gutachten des Europäischen Gerichtshofes wörtlich: „In Fällen […], in denen objektive Anhaltspunkte vorliegen, die eine solche Verwendung rechtfertigen und eine vorherige Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsstelle erforderlich machen, ist daher eine individuelle Information der Fluggäste erforderlich. Dasselbe gilt für Fälle, in denen die PNR-Daten an andere Behörden oder an Einzelpersonen weitergegeben werden“ (EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 223).

92 Das Gericht hält diese Einschätzung des Europäischen Gerichtshofes auf die PNR-Richtlinie für übertragbar und ist deshalb der Auffassung, dass die Betroffenen individuell über die De-Depersonalisierung ihrer Daten zu informieren sind. Sollte der Europäische Gerichtshof der Auffassung sein, dass eine umgehende Benachrichtigung der Betroffenen über die De-Depersonalisierung den verfolgten Zweck der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität zu stark beeinträchtigen könnte, so wäre nach Ansicht des Gerichts eine Information der Betroffenen spätestens in dem Zeitpunkt notwendig, in dem eine Gefährdung des

Zweckes der De-Depersonalisierung, beispielsweise wegen des Abschlusses der Ermittlungsmaßnahmen, nicht mehr zu besorgen ist.

93 Auch hat der Betroffene nach Art. 47 GRCh ein Recht darauf, dass eine Überprüfung vor einem unabhängigen, unparteiischen und zuvor durch Gesetz errichteten Gericht und nicht durch eine „Justizbehörde“ zu erfolgen hat. Vorliegend wird jedoch jeglicher Rechtsbehelf ausgeschlossen, der Rechtsweg verschlossen.

Zu Frage 3 Übermittlung an Drittstaaten

94 Gemäß Art. 11 Abs. 1 PNR-Richtlinie dürfen die PNR-Daten und die Ergebnisse der Verarbeitung dieser Daten grundsätzlich im Einzelfall an einen Drittstaat übermittelt werden, wenn die Bedingungen des Artikels 13 des Rahmenbeschlusses 2008/977/JI erfüllt sind, die Übermittlung für die Zwecke der PNR-Richtlinie erforderlich ist, der Drittstaat sich bereit erklärt, die Daten nur dann an einen anderen Drittstaat zu übermitteln, wenn dies für die Zwecke der PNR-Richtlinie unbedingt notwendig ist und nur wenn der jeweilige Mitgliedstaat ausdrücklich zustimmt und die Bedingungen des Art. 9 Abs. 2 PNR-Richtlinie erfüllt sind.

95 Art. 11 Abs. 2 PNR-Richtlinie enthält eine Ausnahme von diesem Erfordernis, indem er bestimmt, dass ungeachtet des Artikels 13 Abs. 2 des Rahmenbeschlusses 2008/977/JI (nunmehr Art. 38 Richtlinie (EU) 2016/680) Übermittlungen von PNR-Daten an Drittstaaten ohne vorherige Zustimmung des Mitgliedstaates, von dem die Daten eingeholt wurden, nur unter außergewöhnlichen Umständen zulässig sind, nämlich wenn die Übermittlung an den Drittstaat unerlässlich ist, um eine bestimmte und gegenwärtige Bedrohung durch terroristische Straftaten oder schwere Kriminalität in einem Mitgliedstaat oder Drittstaat abzuwehren und die vorherige Zustimmung nicht rechtzeitig eingeholt werden kann.

96 Da durch die Weitergabe an Drittstaaten deren Behörden faktisch Zugang zu den PNR-Daten enthalten, müssen alle die Verwendung der Daten betreffenden Grundsätze, die die Verhältnismäßigkeit der damit verbundenen Grundrechtseingriffe und ein angemessenes Datenschutzniveau sicherstellen sollen, auch für die Drittstaaten gelten. Insofern hat der Europäische Gerichtshof in seinem Gutachten zum EU-Kanada-Abkommen klargestellt, dass eine Weitergabe personenbezogener Daten aus der Union in ein Drittland nur dann zulässig ist, wenn das Drittland ein Schutzniveau der Grundfreiheiten und Grundrechte gewährleistet, das dem in der Union garantierten Niveau der Sache nach gleichwertig ist. Damit soll verhindert werden, dass das im Abkommen vorgesehene Schutzniveau durch die Weitergabe personenbezogener Daten an Drittländer umgangen werden könnte, und gewährleistet werden, dass das vom Unionsrecht gewährte Schutzniveau fortbesteht (EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 214). Daraus hat der Europäische Gerichtshof gefolgert, dass die Weitergabe personenbezogener Daten an ein Drittland nur zulässig ist, wenn entweder ein Abkommen zwischen der Union und dem betreffenden Drittland besteht, das dem EU-Kanada-Abkommen äquivalent ist, oder wenn ein Beschluss der Kommission gemäß Art. 25 Abs. 6 der Richtlinie 95/46 (nunmehr Art. 45 Abs. 3 DS-GVO) existiert, mit dem festgestellt wird, dass das Drittland ein angemessenes Schutzniveau im Sinne des Unionsrechts gewährleistet, und dieser Beschluss sich auf die Behörden erstreckt, an die PNR-Daten weitergegeben werden sollen (EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 214).

97 Diese Voraussetzungen werden durch Art. 11 PNR-Richtlinie unterlaufen. Art. 11 Abs. 1 a) PNR-Richtlinie verweist auf Art. 13 des Rahmenbeschlusses 2008/977/JI. Dieser Rahmenbeschluss wurde mit der Richtlinie (EU) 2016/680 aufgehoben. Verweise auf den Rahmenbeschluss gelten nun als Verweise auf Richtlinie (EU) 2016/680 (auch Gefahrenabwehrrichtlinie genannt), vgl. Art. 59 Richtlinie (EU) 2016/680. Dem Art. 13 des alten Rahmenbeschlusses 2008/977/JI entsprechen im Wesentlichen Art. 35 bis 38 der Richtlinie (EU) 2016/680.

98 Gemäß Art. 35 Abs. 1 lit. d) Richtlinie (EU) 2016/680 setzt die Datenübermittlung an einen Drittstaat voraus, dass die Kommission gemäß Art. 36 Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat oder, wenn ein solcher Beschluss nicht vorliegt, dass geeignete Garantien im Sinne des Art. 37 Richtlinie (EU) 2016/680 vorliegen oder, sollten auch solche nicht vorhanden sein, dass ein **Ausnahmefall nach Art. 38 Richtlinie (EU) 2016/680** gegeben ist. Insofern stellt der Verweis des Art. 11 Abs. 1 a) PNR-Richtlinie auf Art. 13 des Rahmenbeschlusses 2008/977/JI und damit auf Art. 35 Richtlinie (EU) 2016/680 kein angemessenes Datenschutzniveau des Drittstaates sicher, indem er es durch den Verweis auch auf Art. 38 Richtlinie (EU) 2016/680 zulässt, PNR-Daten auch ohne Vorliegen eines Angemessenheitsbeschlusses oder geeigneter Garantien an Drittstaaten zu übermitteln. Dies insbesondere, weil der Begriff des Ausnahmefalls im Sinne des Art. 38 Richtlinie (EU) 2016/680 sehr weit gefasst wird. Diese Vorschrift ermöglicht es nämlich, PNR-Daten an Drittstaaten ohne angemessenes Datenschutzniveau zu übermitteln, wenn dies im Einzelfall für die Zwecke des Art. 1 Absatz 1 Richtlinie (EU) 2016/680 (Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit) oder im Zusammenhang mit diesen Zwecken zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist, vgl. Art. 38 Abs. 1 lit d) und e) Richtlinie (EU) 2016/680.

Zu Frage 4 Essenswünsche im Freitextfeld

99 Gemäß Art. 6 Abs. 4 Satz 4 PNR-Richtlinie dürfen für die Kriterien, mit denen die PNR-Daten durch die PNR-Zentralstellen der Mitgliedstaaten automatisiert abgeglichen werden (sog. Muster), unter keinen Umständen 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 als Grundlage herangezogen werden.

100 Dies entspricht zunächst dem Rechtsgedanken der Art. 10 Richtlinie (EU) 2016/680 und Art. 9 DS-GVO, die die Verarbeitung besonderer Kategorien personenbezogener Daten regeln. Besondere Kategorien personenbezogener Daten sind nach diesen Vorschriften insbesondere solche, aus denen die rassische und ethnische Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Die Verarbeitung dieser besonders sensiblen Daten ist grundsätzlich untersagt und nur unter sehr strengen Voraussetzungen möglich. Gemäß Art. 10 Richtlinie (EU) 2016/680 nämlich nur dann, wenn die Verarbeitung dieser Daten unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und sie (a) nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist, (b) der Wahrung lebenswichtiger Interessen

der betroffenen oder einer anderen natürlichen Person dient oder (c) sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.

101 Eine effektive Regelung, um diesen hohen Anforderungen gerecht zu werden, enthält die PNR-Richtlinie aber nicht. Denn Art. 6 Abs. 4 Satz 4 PNR-Richtlinie enthält lediglich eine Absichtserklärung, die insbesondere durch Anhang I Nr. 12 PNR-Richtlinie konterkariert wird. Denn über das dort verpflichtend in ausnahmslos jedem einzelnen Fall an die PNR-Zentralstellen zu übermittelnde Freitextfeld „allgemeine Hinweise“ kann eine unüberschaubare Vielzahl von Informationen an die PNR-Zentralstellen übermittelt und von diesen genutzt werden, insbesondere auch besonders sensible Daten. So könnte über dieses Freitextfeld beispielsweise übermittelt werden könnte, dass ein Fluggast koscheres Essen oder halal-Speisen gewünscht hat. Aus dieser Information kann jedoch ein Rückschluss auf die religiösen Überzeugungen der betroffenen Person gezogen werden, sodass es sich um ein besonders sensibles Datum im vorgenannten Sinne handelt.

102 Es ist für das vorlegende Gericht nicht ersichtlich, dass die Übermittlung auch besonderer Kategorien von personenbezogenen Daten im Rahmen der Fluggastdatenverarbeitung unbedingt erforderlich wäre. Nach Anhang I der PNR-Richtlinie ist bereits eine sehr große Anzahl konkret benannter personenbezogener Daten an die PNR-Zentralstellen der Mitgliedstaaten zu übermitteln. Über ein praktisch uferloses Freitextfeld alle möglichen weiteren Informationen übermitteln zu können, dürfte die Grenze des absolut Notwendigen überschreiten.

Zu Frage 5 Information durch die Luftfahrtunternehmen

103 Gemäß Art. 13 Abs. 3 der PNR-Richtlinie berührt diese nicht die Anwendbarkeit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates auf die Verarbeitung personenbezogener Daten durch Fluggesellschaften, insbesondere deren Pflichten, geeignete technische und organisatorische Maßnahmen zum Schutz der Sicherheit und Vertraulichkeit der personenbezogenen Daten zu treffen. Auch Art. 21 Abs. 2 PNR-Richtlinie stellt nochmals klar, dass die Anwendbarkeit der Richtlinie 95/46/EG auf die Verarbeitung personenbezogener Daten durch Fluggesellschaften nicht berühren werden soll.

104 Die Richtlinie 95/46/EG ist durch die 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 (DS-GVO) ersetzt worden (siehe Art. 94 Abs. 2 DS-GVO, wonach Verweise auf die Richtlinie 95/46/EG als Verweise auf die DS-GVO gelten).

105 Gemäß Art. 13 DS-GVO sind den betroffenen Personen im Falle der Erhebung personenbezogener Daten die dort aufgeführten Informationen zu erteilen. Gemäß Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Die Erhebung der PNR-Daten der Fluggäste und Drittbetroffenen durch die Luftfahrtunternehmen stellt eine Erhebung personenbezogener Daten in die-

sem Sinne dar, sodass Art. 13 DS-GVO vorliegend für die Luftfahrtunternehmen Anwendung findet.

106 Aufgrund der bereits dargelegten Schwere der mit der PNR-Datenverarbeitung verbundenen Grundrechtseingriffe sind hinsichtlich der Informationspflichten nach Auffassung des vorlegenden Gerichts strenge Maßstäbe anzulegen. Dies auch vor dem Hintergrund, dass eine nur unzureichende Information der Fluggäste unter Verstoß gegen Art. 13 DS-GVO zu einer Intensivierung der Grundrechtseingriffe durch die PNR-Zentralstellen der Mitgliedstaaten führen dürfte, da deren Maßnahmen noch schwerer wiegen würden, wenn die Betroffenen von den Befugnissen der PNR-Zentralstellen keine Kenntnis hätten.

107 Nach diesseitiger Auffassung obliegt es den Luftfahrtunternehmen, die Betroffenen nach Art. 13 und Art. 14 DS-GVO zu informieren, weil andernfalls eine Lücke vorläge, die mit Art. 7 und Art. 8 GRCh unvereinbar wäre. Daher dürfte es erforderlich sein, dass die Luftfahrtunternehmen die Fluggäste explizit über sämtliche durch sie erhobene PNR-Daten, die intendierte Weitergabe an die PNR-Zentralstellen der Mitgliedstaaten und die dortige Weiterverarbeitung der Datensätze inklusive der fünfjährigen Speicherdauer und über ihre konkreten Betroffenenrechte informieren. Denn ohne diese Informationen werden die betroffenen Fluggäste kaum in der Lage sein, ihre genannten Betroffenenrechte auszuüben. Dazu zählen auch die jeweiligen Flughafenmitarbeiter und Mitarbeiter der Reisebüros.

108 Regelungen dazu enthält die PNR-Richtlinie nicht. Sie enthält nur Regelungen zu Betroffenenrechten hinsichtlich der PNR-Daten bei den PNR-Zentralstellen.

109 Der Europäische Gerichtshof hat bereits in seinem Gutachten zum EU-Kanada-Abkommen ausgeführt, dass es zur Gewährleistung dieser Rechte erforderlich ist, dass den Fluggästen die Weitergabe ihrer PNR-Daten an Kanada und die Verwendung der Daten mitgeteilt werden, sobald dies die Ermittlungen der im geplanten Abkommen genannten Behörden nicht mehr beeinträchtigen kann. Diese Mitteilung ist nämlich der Sache nach erforderlich, damit die Fluggäste ihr Recht auf Auskunft über die sie betreffenden PNR-Daten und gegebenenfalls auf Berichtigung der Daten sowie ihr Recht, gemäß Art. 47 Abs. 1 der Charta bei einem Gericht einen wirksamen Rechtsbehelf einzulegen, ausüben können (EuGH-Gutachten 1/15 vom 26. Juli 2017, ECLI:EU:C:2017:592, Rn. 220).

110 Als Beispiel für die unzureichende Information der Fluggäste durch die Luftfahrtunternehmen seien hier die Hinweise der vom Kläger genutzten Fluglinie benannt. Die von der E. auf ihrer Internetseite (https://www.xxx/de/, zuletzt abgerufen am 11. Mai 2020) aufgeführten Informationen sind die folgenden:

„***Wer ist der Verantwortliche?***

Die E. […] informiert Sie im Folgenden über die Verarbeitung Ihrer personenbezogenen Daten im Rahmen unserer Angebote. Direkten Zugang zu diesen Angeboten erhalten Sie über E.com („Webseite“) und über die E. App.

Wenn wir im Folgenden von den E Group Airlines sprechen, sind damit die Fluggesellschaften E., F., G. und H. gemeint. Die E. Group umfasst die E Group Airlines sowie die sonstigen Gesellschaften des E. Konzerns.

An wen kann ich mich wenden?

Sollten Sie darüber hinaus Fragen zum Datenschutz im Zusammenhang mit unserer Webseite oder den darauf angebotenen Services haben, kontaktieren Sie unseren Datenschutzbeauftragten:

Konzerndatenschutzbeauftragte […]

Ein Auskunftsersuchen richten Sie bitte an:
E. AG
Datenauskunft

[…]

Aufgrund welcher weiteren Verpflichtungen verarbeiten wir Ihre Daten?

Wir verarbeiten Fluggastdaten aufgrund gesetzlicher Verpflichtungen nach Art. 6 Abs. 1 S. 1 lit. c) DSGVO:

Sofern wir dazu gesetzlich verpflichtet sind, verarbeiten wir personenbezogene Daten, um handels- oder steuerrechtlichen Aufbewahrungspflichten nachzukommen oder um sicherheitsrechtliche Anforderungen zu erfüllen (bspw. § 7 LuftSiG). Weitere Informationen zu Aufbewahrungsfristen finden Sie unter „Dauer der Datenverarbeitung“.

*Übermittlungen an **Einreisebehörden**:*

• Aufgrund des Fluggastdatenabkommens zwischen EU und USA bzw. Kanada

• Aufgrund des Fluggastdatengesetzes in Deutschland

• API (Advance Passenger Information) Datenübermittlung sofern wir zur Mitwirkung bei Kontrolltätigkeiten im internationalen Reiseverkehr verpflichtet sind*

**Die Daten der maschinenlesbaren Zone des Passes oder Personalausweises*
Weitere Informationen erhalten Sie bei den zuständigen Behörden.

[…]

Wer bekommt Ihre Daten?

Im Kontext der vorstehenden Datenverarbeitungen und der genannten jeweiligen Rechtsgrundlage (Vertragsdurchführung, im berechtigten Interesse, mit Einwilligung oder aufgrund gesetzlicher Verarbeitungspflichten) können Ihre Daten an folgende Kategorien von Empfängern weitergegeben werden:

[…]

staatliche Stellen und Behörden, z.B. aufgrund von Einreisebestimmungen oder von Polizei- und Ermittlungstätigkeiten.

Dabei kann es vorkommen, dass personenbezogene Daten in Drittländer oder an internationale Organisationen übermittelt werden. Zu Ihrem Schutz und dem Schutz Ihrer personenbezogenen Daten sind bei derartigen Datenübermittlungen gemäß und im Einklang mit den gesetzlichen Voraussetzungen geeignete Garantien vorgesehen.

Soweit diese Übermittlungen nicht auf einer gesetzlichen Grundlage beruhen oder in ein Land erfolgen für das kein durch die EU Kommission erlassener Angemessenheitsbeschluss vorliegt, verwenden wir die EU-Standardvertragsklauseln.

Welche Datenschutzrechte haben Sie?

Für E. ist es ein wichtiges Anliegen, unsere Verarbeitungsprozesse fair und transparent zu gestalten. Daher ist es uns wichtig, dass betroffene Personen neben dem Widerspruchsrecht bei Vorliegen der jeweiligen gesetzlichen Voraussetzung folgende Rechte ausüben können:

Recht auf Auskunft, Art. 15 DSGVO
Recht auf Berichtigung, Art. 16 DSGVO
Recht auf Löschung („Recht auf Vergessenwerden"), Art. 17 DSGVO
Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO
Recht auf Datenübertragbarkeit, Art. 20 DSGVO
Recht auf Widerspruch, Art. 21 DSGVO

Um Ihre Recht auszuüben, können Sie sich per E-Mail an xxx@yyy.de wenden.

Zur Identifizierung bitten wir Sie um folgende Angaben:

Name
Postanschrift
E-Mail-Adresse sowie optional: Kundenummer oder Buchungscode oder Ticketnummer

Sollten Sie uns eine Kopie Ihres Ausweises zusenden, so bitten wir alle Angaben bis auf Name, Vorname, Adresse zu schwärzen.

Um Ihren Antrag bearbeiten zu können, sowie zu Identifizierungszwecken, weisen wir darauf hin, dass wir Ihre personenbezogenen Daten gemäß Art. 6 Abs. 1 lit. c DSGVO verarbeiten werden.

Darüber hinaus haben Sie nach Art. 77 DSGVO i.V.m. § 19 BDSG das Recht auf Beschwerde bei einer Aufsichtsbehörde. Die für E. zuständige Aufsichtsbehörde ist:

[...]."

111 Diese Informationen dürften nach dem oben Gesagten unzureichend und irreführend sein. So ist insbesondere der Hinweis, dass bei den API-Daten nur der maschinenlesbare Teil des Passes oder Personalausweises betroffen sei, offensichtlich unvollständig. Denn nach Anhang I Nr. 18 PNR-Richtlinie sind, die API-Daten, soweit sie erhoben werden, einschließlich u. a. der Fluggesellschaft, der Flugnummer sowie Tagen, Uhrzeiten und Orten

von Ankunft und Abflug zu übermitteln, also keineswegs nur die maschinenlesbaren Teile von Ausweispapieren. Im Übrigen wird an keiner Stelle auf die PNR-Richtlinie, sondern ausschließlich auf das Flugastdatengesetz hingewiesen. Zudem fehlt jeglicher Hinweis auf den Inhalt der PNR-Richtlinie oder des FlugDaG. Für die Betroffenen ist so im Vorhinein einer Flugbuchung nicht transparent, welche Behörde die PNR-Zentralstelle des jeweiligen Mitgliedstaates ist und wie man sich an diese wenden kann, wie genau die PNR-Daten dort verarbeitet werden oder wie lange ihre Daten durch diese gespeichert werden dürfen. Insofern erscheint die durch die E. AG stattfindende Information der Fluggäste nicht die Anforderungen des Art. 13 DS-GVO zu erfüllen, von den anderen Personen, die ebenfalls gemeldet werden soll, ganz zu schweigen.

112 Hier hätte es einer klarstellenden Regelung im Verhältnis zwischen DS-GVO und PNR-Richtlinie bezüglich der jeweiligen Pflichten der Luftverkehrsgesellschaft bedurft, so dass Nebelkerzen vermieden worden wären.

IV.

113 Nach alledem ist eine Vorlage an den Europäischen Gerichtshof geboten.

114 Das Ergebnis des Rechtsstreits hängt von den Vorlagefragen ab. Denn sollte die PNR-Richtlinie gegen europäisches Primärrecht verstoßen, wäre sie unanwendbar. Verstößt die PNR-Richtlinie gegen Unionsrecht, dann erweist sich auch die Umsetzung in nationales Recht durch das FlugDaG als rechtswidrig. Dieses Gesetz könnte die mit der PNR-Daten-Verarbeitung verbundenen Grundrechtseingriffe dann nicht rechtfertigen, sodass das vorlegende Gericht von seiner Kompetenz Gebrauch machen würde, das FlugDaG wegen Verstoßes gegen (vorrangiges) europäisches Recht unangewendet zu lassen.

115 Eine gesonderte weitere Vorlage in dem Verfahren 6 K 806/19.WI des Verwaltungsgerichts Wiesbaden wird primär Fragen aufwerfen, die sich durch die Öffnungsklausel in Art. 2 PNR-Richtlinie ergeben.

V.

116 Der Beschluss ist unanfechtbar.