EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

8. Februar 2023

Stellungnahme 6/2023

zu den Vorschlägen für Verordnungen über die Erhebung und Übermittlung vorab übermittelter Fluggastdaten (API-Daten)

edps.europa.eu

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 52 Absatz 2 der Verordnung (EU) 2018/1725 im „Hinblick auf die Verarbeitung personenbezogener Daten ... sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Datenschutz, von den Organen und Einrichtungen der Union geachtet werden"; er ist gemäß Artikel 52 Absatz 3 „für die Beratung der Organe und Einrichtungen der Union und der betroffenen Personen in allen Fragen der Verarbeitung personenbezogener Daten" zuständig.

Am 5. Dezember 2019 wurde Wojciech Rafał Wiewiórowski für einen Zeitraum von fünf Jahren zum Europäischen Datenschutzbeauftragten ernannt.

*Gemäß **Artikel 42 Absatz 1** der Verordnung 2018/1725 konsultiert die Kommission den Europäischen Datenschutzbeauftragten „[n]ach der Annahme von Vorschlägen für einen Gesetzgebungsakt, für Empfehlungen oder Vorschläge an den Rat nach Artikel 218 AEUV sowie bei der Ausarbeitung von delegierten Rechtsakten und Durchführungsrechtsakten, die Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten haben".*

Diese Stellungnahme bezieht sich auf den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Erhebung und Übermittlung vorab übermittelter Fluggastdaten (API) zur Verbesserung und Erleichterung der Kontrollen an den Außengrenzen, zur Änderung der Verordnung (EU) 2019/817 und der Verordnung (EU) 2018/1726 sowie zur Aufhebung der Richtlinie 2004/82/EG des Rates (COM(2022) 729 final) und auf den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Erhebung und Übermittlung von API-Daten zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität und zur Änderung der Verordnung (EU) 2019/818 (COM(2022) 731 final).

Die vorliegende Stellungnahme schließt künftige zusätzliche Kommentare oder Empfehlungen des EDSB nicht aus, insbesondere wenn weitere Probleme festgestellt oder neue Informationen bekannt werden. Diese Stellungnahme greift etwaigen künftigen Maßnahmen, die der EDSB in Ausübung seiner Befugnisse gemäß der Verordnung (EU) 2018/1725 ergreifen mag, nicht vor. Diese Stellungnahme beschränkt sich auf die Bestimmungen der beiden Vorschläge, die unter dem Gesichtspunkt des Datenschutzes relevant sind.

Zusammenfassung

Am 13. Dezember 2022 legte die Europäische Kommission zwei Legislativvorschläge zur Erhebung und Übermittlung vorab übermittelter Fluggastdaten („API-Daten“) vor: einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Erhebung und Übermittlung vorab übermittelter Fluggastdaten (API) zur Verbesserung und Erleichterung der Kontrollen an den Außengrenzen, (Vorschlag „API Grenzmanagement“) und einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Erhebung und Übermittlung von API-Daten zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (Vorschlag „API Strafverfolgung“) (gemeinsam „die Vorschläge“).

Ziele des Vorschlags „API Grenzmanagement“ sind die Verbesserung und Erleichterung der Wirksamkeit und Effizienz der Kontrollen an den Außengrenzen und die Bekämpfung der illegalen Einwanderung sowie die Ersetzung der bestehenden Richtlinie 2004/82/EG des Rates („API-Richtlinie“). Ziel des Vorschlags „API Strafverfolgung“ ist es, ergänzend zur bestehenden Richtlinie (EU) 2016/681 („PNR-Richtlinie“) bessere Vorschriften für die Erhebung und Übermittlung von API-Daten durch Fluggesellschaften zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität festzulegen.

Unter Berücksichtigung der Tatsache, dass die sich aus den Vorschlägen ergebenden Datenverarbeitungsvorgänge bereits im Unionsrecht vorgesehenen Datenverarbeitungsvorgängen entsprechen oder diese ergänzen würden, wird in dieser Stellungnahme in erster Linie auf die Notwendigkeit und Verhältnismäßigkeit der geplanten Verarbeitung von API-Daten aus EU-Flügen und ihre Vereinbarkeit mit der PNR-Richtlinie in der Auslegung durch das Urteil des EuGH in der Rechtssache C-817/19 eingegangen.

Wenngleich der EDSB die vorgeschlagene Lösung für EU-Flüge im Großen und Ganzen für ausreichend erachtet, um die Einhaltung des Urteils des EuGH zu Artikel 2 der PNR-Richtlinie zu gewährleisten, fordert er die Mitgesetzgeber auf, die Entwicklung harmonisierter Kriterien für die Auswahl von EU-Flügen, von denen API-Daten im Einklang mit den vom Gerichtshof festgelegten Bedingungen erhoben werden sollen, in Erwägung zu ziehen. Ferner empfiehlt der EDSB eine weitere Stärkung der Sicherheit bei der Verarbeitung von API-Daten im Router durch zusätzliche Garantien wie die Pseudonymisierung und/oder Verschlüsselung der API-Daten, sofern dies technisch und operativ durchführbar ist.

Die Stellungnahme enthält auch andere spezifische Empfehlungen, beispielsweise in Bezug auf die Notwendigkeit, in den Vorschlägen ausdrücklich klarzustellen, dass die Daten automatisch gelöscht werden sollten, wenn es dem Router technisch nicht möglich ist, die von den Fluggesellschaften übermittelten API-Daten an die zuständigen nationalen Behörden zu übermitteln.

Inhalt

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[1], insbesondere auf Artikel 42 Absatz 1, –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

1. Am 13. Dezember 2022 legte die Europäische Kommission zwei Legislativvorschläge zur Erhebung und Übermittlung vorab übermittelter Fluggastdaten (im Folgenden „Vorschläge“) vor:

- einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Erhebung und Übermittlung vorab übermittelter Fluggastdaten (API-Daten) zur Verbesserung und Erleichterung der Kontrollen an den Außengrenzen, zur Änderung der Verordnung (EU) 2019/817 und der Verordnung (EU) 2018/1726 sowie zur Aufhebung der Richtlinie 2004/82/EG des Rates („API Grenzmanagement“),

- einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Erhebung und Übermittlung von API-Daten zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität und zur Änderung der Verordnung (EU) 2019/818 („Vorschlag „API Strafverfolgung““).

2. Ziel des Vorschlags „API Grenzmanagement“ ist die Verbesserung und Erleichterung der Wirksamkeit und Effizienz der Kontrollen an den Außengrenzen und die Bekämpfung der illegalen Einwanderung[2], wodurch folglich die bestehende Richtlinie 2004/82/EG des Rates („API-Richtlinie“)[3] ersetzt wird.

3. Ziel des Vorschlags „API Strafverfolgung“ ist es, in Ergänzung der bestehenden Richtlinie (EU) 2016/681 („PNR-Richtlinie“)[4] bessere Vorschriften für die Erhebung und Übermittlung von API-Daten durch Fluggesellschaften zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität[5] festzulegen.

[1] ABl. L 295 vom 21.11.2018, S. 39.
[2] Siehe Artikel 1 des Vorschlags „API Grenzmanagement“.
[3] Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln (ABl. L 261 vom 6.8.2004, S. 24).
[4] Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, *ABl. L 119 vom 4.5.2016, S. 132*.

[5] COM(2022) 731 final, Begründung des Vorschlags „API Strafverfolgung“, S. 3.

4. Die Vorschläge stehen im Einklang mit der Schengen-Strategie vom Juni 2021, die in der Mitteilung der Kommission „Strategie für einen reibungslos funktionierenden und resilienten Schengen-Raum“ vorgestellt wurde, in der ausdrücklich die Notwendigkeit einer verstärkten Nutzung von API-Daten in Verbindung mit PNR-Daten betont wurde, um die innere Sicherheit im Einklang mit dem Grundrecht auf Schutz personenbezogener Daten und dem Grundrecht auf Freizügigkeit erheblich zu verbessern.[6] Darüber hinaus forderten auch der Sicherheitsrat der Vereinten Nationen und die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) auf internationaler Ebene wiederholt die Einrichtung und weltweite Einführung von API- und PNR-Systemen für Strafverfolgungszwecke.[7]

5. Mit der vorliegenden Stellungnahme des EDSB wird das Konsultationsersuchen der Europäischen Kommission vom 14. Dezember 2022 gemäß Artikel 42 Absatz 1 EU-DSVO beantwortet. Der EDSB begrüßt den Verweis auf diese Konsultation in Erwägungsgrund 44 des Vorschlags „API Grenzmanagement“ und in Erwägungsgrund 29 des Vorschlags „API Strafverfolgung“. In diesem Zusammenhang stellt der EDSB erfreut fest, dass er bereits informell gemäß Erwägungsgrund 60 EU-DSVO konsultiert wurde.

6. In Anbetracht der engen Abstimmung zwischen den Vorschlägen[8] und der zahlreichen darin enthaltenen Querverweise scheint es für den EDSB am zweckmäßigsten, sie in einer einzigen Stellungnahme zu bewerten.

2. Allgemeine Bemerkungen

7. Der EDSB stellt fest, dass die in den Vorschlägen vorgesehenen spezifischen Datenverarbeitungsvorgänge bereits bestehenden und im Unionsrecht vorgesehenen Datenverarbeitungsvorgängen entsprechen oder diese ergänzen. In Bezug auf den Vorschlag „API Grenzmanagement“ ist es der Rechtsrahmen für Grenzkontrollen an den Außengrenzen, insbesondere der Schengener Grenzkodex[9], und in Bezug auf API-Strafverfolgungsvorschlag ist es die bereits erwähnte PNR-Richtlinie.

8. Darüber hinaus berücksichtigt der EDSB, dass der Gerichtshof der Europäischen Union (EuGH) in Rechtssache C-817/19[10] vor Kurzem die Gültigkeit der PNR-Richtlinie bestätigte und gleichzeitig wichtige Klarstellungen zu einer Reihe ihrer Bestimmungen formulierte, darunter im Wesentlichen zusätzliche Einschränkungen bei der Verarbeitung personenbezogener Daten, um die Einhaltung der Artikel 7 und 8 der Charta sicherzustellen. Insbesondere legte der Gerichtshof eine Reihe von Bedingungen fest, die die nationalen Rechtsvorschriften zur Umsetzung der PNR-Richtlinie in Bezug auf die Anwendung der PNR-Richtlinie auf EU-Flüge erfüllen müssen.

9. Die vom Gerichtshof in seinem Urteil festgelegten Bedingungen stellen einen wichtigen Bezugspunkt für die Bewertung der Vorschläge dar, insbesondere im Hinblick auf die

[6] COM(2021) 277 final.
[7] Resolutionen des Sicherheitsrats der Vereinten Nationen 2178(2014), 2309(2016), 2396(2017), 2482(2019) und Beschluss 6/16 des OSZE-Ministerrats vom 9. Dezember 2016 über die verstärkte Nutzung von vorab übermittelten Fluggastdaten.
[8] Siehe Erwägungsgrund 11 des Vorschlags „API Strafverfolgung“.
[9] Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Unionskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) (ABl. L 77 vom 23.3.2016, S. 1).
[10] Urteil des EuGH vom 21. Juni 2022 in der Rechtssache C-817/19, Ligue des droits humains, ECLI:EU:C:2022:491.

Verarbeitung von API-Daten aus EU-Flügen. In diesem Zusammenhang begrüßt der EDSB die ausdrückliche Bezugnahme auf das Urteil des Gerichtshofs in Erwägungsgrund 14 und in der Begründung des Vorschlags „API Strafverfolgung“.[11]

10. Gleichzeitig ist zu berücksichtigen, dass das Urteil des EuGH die Verarbeitung von PNR-Daten betrifft, die 18 Datenkategorien umfassen.[12] Die API-Daten sind nur eine Teilmenge davon. Die Auswirkungen der Verarbeitung von API-Daten auf die Grundrechte der Fluggäste könnten daher trotz der auf EU-Ebene neu geschaffenen Verpflichtung zur Erhebung von API-Daten als geringer im Vergleich zur Verarbeitung von PNR-Daten angesehen werden. Darüber hinaus sei daran erinnert, dass Fluggesellschaften bereits bei der Abfertigung des Fluggastes API-Daten erheben (beim Online-Check-in und am Flughafen), während ihre Praktiken zugleich vielfältig und widersprüchlich sind.[13]

11. Was schließlich das Verhältnis zwischen den beiden Vorschlägen und dem EU-Rechtsrahmen für den Datenschutz betrifft, begrüßt der EDSB die Klarstellung, dass die allgemein geltenden Rechtsakte der Union über den Schutz personenbezogener Daten, insbesondere die Verordnung (EU) 2016/679 (DSGVO)[14], die EU-DSVO und die Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei der Strafverfolgung)[15], von den geplanten API-Verordnungen[16] nicht betroffen wären. Der EDSB hält es jedoch weder für sinnvoll noch für richtig, darauf hinzuweisen, dass die vorgeschlagenen Rechtsvorschriften die allgemein geltenden Rechtsakte über den Schutz personenbezogener Daten „ergänzen“ würden, da der vorgeschlagene Rechtsakt einfach mit ihnen in Einklang stünde, wie dies bei allen sektoralen Rechtsvorschriften der Fall ist.

3. Verarbeitung von API-Daten aus EU-Flügen

12. Ähnlich wie im derzeitigen Rechtsrahmen – der API-Richtlinie und der PNR-Richtlinie – wird in den beiden Vorschlägen zwischen Drittstaatsflügen und EU-Flügen unterschieden.[17] Die API-Daten von Drittstaatsflügen werden für die Zwecke 1) der Grenzkontrollen an den Außengrenzen und der Bekämpfung der illegalen Einwanderung (weiter beschränkt nur auf EU-Flüge) und 2) der Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität verarbeitet. Umgekehrt dürfen die API-Daten von EU-Flügen nur für die Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität im Sinne der PNR-Richtlinie und nicht für Einwanderungszwecke verarbeitet werden.

---

[11] COM(2022) 731 final, Begründung des Vorschlags „API-Strafverfolgung“, S. 3.
[12] Siehe Anhang I der PNR-Richtlinie.
[13] COM(2022) 731 final, Begründung des API-Strafverfolgungsvorschlag, S. 1.
[14] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR) (ABl. L 119 vom 4.5.2016, S. 1).
[15] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).
[16] Siehe Erwägungsgrund 25 des Vorschlags „API Grenzmanagementvorschlag und Erwägungsgrund 17 des Vorschlags „API Strafverfolgung“.
[17] Siehe Artikel 3 Buchstabe c des Vorschlags „API Grenzmanagement“ und Artikel 3 Buchstabe b des Vorschlags „API Strafverfolgung“.

13. Der EDSB stellt fest, dass gemäß Artikel 2 und Artikel 4 Absätze 1 und 6 des Vorschlags „API Strafverfolgung" Fluggesellschaften verpflichtet wären, API-Daten für [alle] Fluggesellschaften, „die Drittstaatsflüge oder EU-Flüge in Form von Linien- oder Gelegenheitsflügen durchführen" zu erheben und anschließend an einen „Router" zu übermitteln[18]. Der Router würde dann an die Zentralstellen für PNR-Daten der Mitgliedstaaten, in deren Hoheitsgebiet der Flug starten und landen wird, nur die API-Daten der von den Mitgliedstaaten gemäß Artikel 2 der PNR-Richtlinie ausgewählten EU-Flüge nach der Auslegung des EuGH-Urteils übermitteln. Zu diesem Zweck würde eu-LISA eine vertrauliche Liste der ausgewählten EU-Flüge führen, die regelmäßig aktualisiert würde.[19]

14. Der EDSB stellt ferner fest, dass gemäß Artikel 12 Buchstabe b des Vorschlags „API Grenzmanagement" die API-Daten von EU-Flügen, die nicht in der Liste aufgeführt sind, „unverzüglich, dauerhaft und automatisch" aus dem Router gelöscht würden. Ebenso wären Fluggesellschaften verpflichtet, die API-Daten von EU-Flügen nach Abschluss der Übermittlung an den Router unverzüglich und dauerhaft zu löschen.[20]

15. Der Kommission zufolge zielt die vorgeschlagene technische Lösung darauf ab, die Übermittlung von API-Daten an Zentralstellen für PNR-Daten auf benannte Flüge zu beschränken, ohne vertrauliche Informationen darüber offenzulegen, welche EU-Flüge ausgewählt wurden, angesichts des Risikos, dass Personen, die an schweren Straftaten oder terroristischen Aktivitäten beteiligt sind, diese Flüge umgehen würden.[21]

16. Der EDSB ist der Ansicht, dass bei der Beurteilung der Einhaltung der vorgeschlagenen Lösung für EU-Flüge die im oben genannten Urteil des EuGH dargelegten Bedingungen zwar einen wichtigen Bezugspunkt darstellen, jedoch entsprechend (*mutatis mutandis*) angewandt werden müssen. Der Gerichtshof hat klargestellt, dass eine Einschränkung der in Artikel 7 und 8 der Charta verankerten Rechte geprüft werden muss, indem die Schwere des mit einer solchen Einschränkung verbundenen Eingriffs bestimmt und geprüft wird, ob die mit ihr verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zu dessen Schwere steht.[22] Im gegenständlichen Zusammenhang sollte berücksichtigt werden, dass das Urteil ein anderes System betrifft, das unter anderem die Verarbeitung von viel mehr Kategorien personenbezogener Daten als API-Daten umfasst. Daher ist der EDSB der Auffassung, dass der Vorschlag eine geringere Einschränkung dieser Grundrechte zur Folge hätte als vom Gerichtshof angenommen.

17. Gemäß EuGH steht das Unionsrecht, insbesondere Artikel 2 der Richtlinie 2016/681 in Verbindung mit Artikel 3 Absatz 2 EUV, Artikel 67 Absatz 2 AEUV und Artikel 45 der Charta, einer nationalen Regelung entgegen, die ein System für die Übermittlung von PNR-Daten aller EU-Flüge durch Fluggesellschaften und für die Verarbeitung dieser Daten durch die zuständigen Behörden vorsieht. Eine solche Verarbeitung ist hingegen zulässig, wenn

[18] Artikel 1 Buchstabe a des Vorschlags „API Strafverfolgung", der sich auf ausgewählte EU-Flüge bezieht, scheint einen Widerspruch (möglicherweise ein Schreibfehler) zu enthalten. Aus Artikel 4 und den allgemeinen Erläuterungen in den Erwägungsgründen und der Begründung (Seite 10) desselben Vorschlags geht jedoch klar hervor, dass die beabsichtigte Auswahl nach der Übermittlung an den Router erfolgen soll, um die Offenlegung der ausgewählten Flüge zu vermeiden.
[19] Siehe Artikel 5 und Erwägungsgrund 14 des Vorschlags „API Strafverfolgung".
[20] Artikel 4 Absatz 8 Buchstabe b des Vorschlags „API Strafverfolgung".
[21] COM(2022) 731 final, Begründung des Vorschlags „API Strafverfolgung", S. 11.
[22] Siehe Urteile des EuGH in der Rechtssache C-817/19 vom 21. Juni 2022, Ligue des droits humains, ECLI:EU:C:2022:491, Rn. 116, und in der Rechtssache C-207/16 vom 2. Oktober 2018, Ministerio Fiscal, EU:C:2018:788, Rn. 55 und die dort angeführte Rechtsprechung.

ein Mitgliedstaat „mit einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung konfrontiert ist".[23]

18. In diesem Zusammenhang ist entscheidend, ob die vorgeschlagene technische Lösung in der Praxis zu einer willkürlichen Übermittlung von API-Daten von allen EU-Flügen an die zuständigen nationalen Behörden führt, und zwar außerhalb der außergewöhnlichen Situationen einer terroristischen Bedrohung.

19. Nach Ansicht des EDSB schließt die geplante automatische Verarbeitung im Router – d. h. das „Filtern" der API-Daten auf der Grundlage einer offiziellen Liste ausgewählter Flughäfen oder Strecken, die Übermittlung von Daten nur aus vorausgewählten Flügen und die sofortige Löschung der Daten aus nicht ausgewählten Flügen – die Möglichkeit für Zentralstellen für Fluggastdaten aus, API-Daten von EU-internen Flügen, zu denen sie keinen Zugang haben sollen, in irgendeiner Weise zu empfangen und zu verarbeiten.

20. Darüber hinaus ist der EDSB der Auffassung, dass die Erhebung und Übermittlung von API-Daten an den Router einerseits und die Verarbeitung der API-Daten durch die zuständigen nationalen Behörden andererseits untrennbar miteinander verbunden sind und daher nicht isoliert betrachtet werden sollten. Da es für die Mitgliedstaaten nicht nur rechtlich ausgeschlossen, sondern auch technisch unmöglich ist, auf API-Daten von EU-Flügen zuzugreifen, die sie nicht formell ausgewählt und mitgeteilt haben, ist der EDSB der Auffassung, dass dieses Element der Vorschläge mit dem einschlägigen EU-Recht in der Auslegung durch den EuGH im Einklang steht.

21. Des Weiteren geht der EDSB davon aus, dass derzeit keine zufriedenstellende (leicht verfügbare, technisch tragfähige und wirtschaftlich wirksame) Alternativlösung besteht, die vergleichbare Garantien und Schutzmaßnahmen für EU-Flüge bieten würde.

22. Problematisch erscheint beispielsweise die direkte Übermittlung von API-Daten durch Fluggesellschaften für alle EU-Flüge an die Zentralstellen für Fluggastdaten und die Entscheidung über die Notwendigkeit der API-Daten und die Löschung der übrigen Daten durch die Mitgliedstaaten. Dies würde in der Tat eine systematische Verarbeitung von Daten aus allen EU-Flügen durch nationale Behörden mit sich bringen, einschließlich der von ihnen nicht ausgewählten Flüge.

23. Das „Filtern" von API-Daten auf Ebene der Fluggesellschaften bietet wiederum keine ausreichenden Garantien und könnte zusätzliche Herausforderungen in Bezug auf die Vertraulichkeit (z. B. Umgehung von Flügen durch Personen, die an schwerer Kriminalität oder terroristischen Aktivitäten beteiligt sind), die Zuverlässigkeit und die Kohärenz der Verarbeitung mit sich bringen, da die API-Daten von mehreren Akteuren auf der Grundlage von Anweisungen aus allen Mitgliedstaaten gefiltert werden. In diesem Zusammenhang ist darauf hinzuweisen, dass der Folgenabschätzung zu den Vorschlägen zufolge derzeit rund 1 000 Fluggesellschaft in der EU tätig sind, von denen etwa 150 ausschließlich in der Union tätig sind.[24]

24. Daraus folgt, dass die auf der Ebene des Routers erfolgende Verarbeitung aller API-Daten angesichts des Ausmaßes des Eingriffs in die betroffenen Grundrechte und der

[23] Urteil des EuGH in der Rechtssache C-817/19 vom 21. Juni 2022, Ligue des droits humains, ECLI:EU:C:2022:491, S. 7 des Urteils und Rn. 171 und 173.
[24] SWD(2022) 422 final, Folgenabschätzung, Anhang 4, S. 71.

vorgesehenen Garantien, insbesondere der rechtlichen und technischen Unmöglichkeit für die Zentralstellen für Fluggastdaten der Mitgliedstaaten, API-Daten, die sich nicht auf die ausgewählten Flüge beziehen, zu empfangen und anderweitig zu verarbeiten, in einem angemessenen Verhältnis zu dem verfolgten Ziel stehen.

25. Schließlich erinnert der EDSB daran, dass gemäß dem Urteil des EuGH die Auswahl von EU-Flügen auf das absolut Notwendige beschränkt werden muss. Zu diesem Zweck muss die Entscheidung der Mitgliedstaaten auf der Grundlage [objektiver] Anhaltspunkte gerechtfertigt sein und regelmäßig überprüft werden.[25] Um divergierende Praktiken zu vermeiden, fordert der EDSB daher die Mitgesetzgeber auf, die Einführung von Bestimmungen in Erwägung zu ziehen, einschließlich einer spezifischen Ermächtigung der Kommission gemäß den Artikeln 290 und/oder 291 AEUV, sofern dies für angemessen erachtet wird, zur Ausarbeitung harmonisierter Kriterien und Methoden für die Auswahl von EU-Flügen, von denen API-Daten erhoben werden sollen.

4. Sicherheit von API-Daten

26. Angesichts des Umfangs der Verarbeitung und der Zahl der betroffenen Personen kann die geplante Erhebung und Übermittlung von API-Daten potenzielle Risiken bergen und muss daher mit wirksamen Garantien zur Gewährleistung eines hohen Sicherheitsniveaus einhergehen. In diesem Zusammenhang stellt der EDSB fest, dass der Vorschlag „API Grenzmanagement“ zusätzlich zu den allgemeinen Verpflichtungen in Bezug auf die Sicherheit personenbezogener Daten gemäß Artikel 33 der EU-DSVO und Artikel 32 der DSGVO eine detaillierte Bestimmung in Bezug auf die Sicherheit der API-Daten und des Routers vorsieht.[26] Gleichzeitig ist die entsprechende Bestimmung im Vorschlag „API Strafverfolgung“[27] sehr allgemein und sieht weder spezifische Maßnahmen vor, noch verweist sie auf die einschlägigen Vorschriften im Vorschlag „API Grenzmanagement“.

27. Darüber hinaus erinnert der EDSB an die Verpflichtung der Behörden der Mitgliedstaaten, der Fluggesellschaften und von eu-LISA, geeignete technische und organisatorische Maßnahmen im Einklang mit den Anforderungen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Artikel 27 der EU-DSVO, Artikel 25 der DSGVO und Artikel 20 der Richtlinie zum Datenschutz bei der Strafverfolgung umzusetzen.

28. Der EDSB empfiehlt daher, dass im Vorschlag „API Strafverfolgung“ spezifische Maßnahmen zur Gewährleistung der Sicherheit von API-Daten vorgesehen werden sollten, die zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung terroristischer Straftaten und schwerer Kriminalität verarbeitet werden, oder alternativ auf die einschlägigen Bestimmungen im Vorschlag „API Grenzmanagement“ Bezug genommen werden sollte.

[25] Siehe Urteil des EuGH in der Rechtssache C-817/19 vom 21. Juni 2022, Rn. 174.
[26] Artikel 17 des Vorschlags „API Grenzmanagement“.
[27] Artikel 8 des Vorschlags „API Strafverfolgung“.

29. Des Weiteren empfiehlt der EDSB eu-LISA, bei der Gestaltung und Entwicklung des Routers die Verwendung der Pseudonymisierung und/oder Verschlüsselung der API-Daten in Erwägung zu ziehen, sofern dies technisch und operativ durchführbar ist.

5. Funktionen und Zuständigkeiten

30. In den Vorschlägen ist vorgesehen, dass die Fluggesellschaften im Zusammenhang mit der Erhebung dieser Daten und ihrer Übermittlung an den Router im Sinne von Artikel 4 Absatz 7 DSGVO Verantwortliche für die Verarbeitung von API-Daten, die personenbezogene Daten darstellen, sind.[28]

31. Darüber hinaus werden im Rahmen des Vorschlags „API-Grenzmanagementvorschlag" die zuständigen Grenzbehörden als Verantwortliche für die Verarbeitung von personenbezogenen API-Daten durch den Router, einschließlich der Übermittlung, sowie die Verarbeitung von personenbezogenen API-Daten benannt. Ebenso wären im Rahmen des Vorschlags „API-Strafverfolgung" die Zentralstellen für Fluggastdaten im Sinne von Artikel 3 Nummer 8 der Richtlinie (EU) 2016/680 Verantwortliche in Bezug auf die Verarbeitung von personenbezogenen API-Daten durch den Router, einschließlich der Übermittlung.

32. Schließlich wird eu-LISA als Auftragsverarbeiter im Sinne von Artikel 3 Nummer 12 der Verordnung (EU) 2018/1725 für die Verarbeitung von personenbezogenen API-Daten durch den Router benannt.[29]

33. Angesichts der Aufteilung der Zuständigkeiten zwischen den verschiedenen Akteuren, ausgelegt im Lichte der einschlägigen Bestimmungen der DSGVO, der EU-DSVO und der Richtlinie zum Datenschutz bei der Strafverfolgung sowie unter Berücksichtigung der Leitlinien des EDSB zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" nach der Verordnung (EU) 2018/1725[30] sowie der Leitlinien des EDSA 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO[31], hält der EDSB diese Rollenverteilung aus den folgenden Gründen für angemessen.

34. Der EDSB stellt fest, dass die Behörden der Mitgliedstaaten in ihrer Funktion als Verantwortliche innerhalb des durch die Vorschläge geschaffenen Rechtsrahmens die Zwecke und wesentlichen Mittel der Verarbeitung über den Router festlegen. Gemäß den Leitlinien des EDSA sind „wesentliche Mittel" eng mit dem Zweck und dem Umfang der Verarbeitung verbunden. Was die Zwecke betrifft, verarbeitet eu-LISA zwar alle API-Daten, doch handelt es sich bei den letztendlich von den Behörden der Mitgliedstaaten verarbeiteten Daten nur um die Daten, die sich auf die von den Mitgliedstaaten ausgewählten Flüge beziehen. Letztere legen daher fest, welche spezifischen Teilmengen von Daten sie erhalten und „warum" im Sinne der oben genannten EDSA-

[28] Siehe Artikel 15 des Vorschlags „API-Grenzmanagement" und Artikel 7 des Vorschlag „API-Strafverfolgung".
[29] Artikel 16 des Vorschlags „API-Grenzmanagement".
[30] https://edps.europa.eu/sites/default/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf
[31] https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

Leitlinien 7/2020.[32] Die wesentlichen Mittel sind gesetzlich geregelt: die API-Daten, die eu-LISA vorgelegt werden; die Dauer der Verarbeitung; die Kategorien von Empfängern (die zuständigen Zentralstellen für Fluggastdaten und Grenzbehörden) und die Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden (Fluggäste, die in den Anwendungsbereich der API-Verordnungen fallen).

35. Bei den „nicht wesentlichen Mitteln" geht es eher um praktische Aspekte der Umsetzung, wie die Wahl einer bestimmten Hard- oder Software oder die detaillierten Sicherheitsmaßnahmen, über die eu-LISA zu entscheiden hat, und über welche der Auftragsverarbeiter entscheiden könnte. Darüber hinaus ist es nach Ansicht des EDSA nicht erforderlich, dass der Verantwortliche tatsächlich Zugang zu den Daten hat, die verarbeitet werden (d. h. zu den Daten im Router).

36. In der Praxis bietet eu-LISA anstelle einer eigenständigen Datenbank einen Kommunikationskanal zwischen den Fluggesellschaften und den Verantwortlichen in den Mitgliedstaaten an (es kommt nicht zu einer „echten" Speicherung von API-Daten im Router). Die Agentur verfolgt für die Verarbeitung von API-Daten keine anderen Zwecke als die Übermittlung an die zuständigen Verantwortlichen in den Mitgliedstaaten.

37. Ungeachtet der Benennung von eu-LISA als Auftragsverarbeiter im Namen der Behörden der Mitgliedstaaten sehen die Vorschläge eine erhebliche Verantwortung für die Gewährleistung einer rechtmäßigen und sicheren Verarbeitung der API-Daten im Router bei der Agentur vor. eu-LISA muss unter anderem gewährleisten, dass nur ordnungsgemäß ausgewählte API-Daten für EU-Flüge die PNR-Zentralstellen erreichen, die verbleibenden API-Daten gelöscht werden und ein hohes Sicherheitsniveau gewährleistet ist, um jeden unbefugten Zugriff auf die Daten zu verhindern.[33]

38. In diesem Zusammenhang erinnert der EDSB daran, dass die EU-DSVO in Bezug auf die Aufsichtsbefugnisse des EDSB gemäß Artikel 58 oder die möglichen Sanktionen für Verstöße gemäß Artikel 66 nicht zwischen Verantwortlichen und Auftragsverarbeitern unterscheidet. In jedem Fall plant der EDSB, die Wahrnehmung der Aufgaben von eu-LISA im Rahmen der Vorschläge im Einklang mit seinem Mandat gemäß der EU-DSVO genau zu überwachen.

6. Berichterstattung und Statistikerstellung

39. Der EDSB stellt fest, dass eu-LISA gemäß Artikel 31 des Vorschlags „API Grenzverwaltung" die Aufgabe hätte, tägliche Statistiken über die Verarbeitung von Daten im Router im zentralen Speicher für Berichte und Statistiken (CRRS) gemäß Artikel 39 der Verordnung (EU) 2019/817 (Interoperabilitätsverordnung)[34] zu speichern und verschiedene statistische Berichte zu erstellen. Zu diesem Zweck hätte eu-LISA das Recht auf Zugriff auf bestimmte

[32] Leitlinien 07/2020 des EDSA zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, Rn. 35.
[33] Siehe Artikel 17, Artikel 22-24 des Vorschlags „API-Grenzmanagement".
[34] Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27).

API-Daten, die an den Router übermittelt werden, „wobei dieser Zugriff jedoch keine Identifizierung der betreffenden Reisenden ermöglichen darf".

40. In seiner Stellungnahme 4/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität[35] hat der EDSB bereits deutlich gewarnt, dass die vorgeschlagene Einrichtung des CRRS eine große Belastung für die eu-LISA darstellen würde. Diese Auffassung hat der EDSB in seinen Stellungnahmen zu EES[36], ETIAS[37], SIS[38], VIS[39] und eu-LISA[40] wiederholt. In diesem Zusammenhang hat der EDSB eine Reihe von Empfehlungen bezüglich des CRRS gegeben, unter anderem zu dem Erfordernis, eine gründliche Abschätzung der Gefahren für die Informationssicherheit vorzunehmen, angemessene Sicherheitsvorkehrungen zu treffen und den Grundsatz des Datenschutzes durch Technikgestaltung anzuwenden. Diese Empfehlungen behalten ihre volle Gültigkeit im Zusammenhang mit den Vorschlägen.

7. Löschung von API-Daten aus dem Router

41. In Artikel 12 des Vorschlags „API-Grenzmanagement" sind zwei Situationen vorgesehen, in denen die automatische Löschung von API-Daten vom Router ausgelöst würde:
a) wenn die Übermittlung der API-Daten an die jeweils zuständigen Grenzbehörden oder Zentralstellen für Fluggastdaten abgeschlossen ist;
B) in Bezug auf den Vorschlag „API Strafverfolgung", wenn sich die API-Daten auf andere EU-Flüge beziehen als die in den Listen gemäß Artikel 5 Absatz 2 der genannten Verordnung aufgeführten (d. h. Flüge, die von keinem Mitgliedstaat ausgewählt wurden).

42. Der EDSB stellt ferner fest, dass in Artikel 14 des Vorschlags „API-Grenzmanagement" die Maßnahmen beschrieben werden, die zu ergreifen sind, wenn die Nutzung des Routers technisch nicht möglich ist. Im Allgemeinen wären Fluggesellschaften in solchen Situationen nicht verpflichtet, API-Daten an den Router zu übermitteln. In den Vorschlägen wird jedoch nicht ausdrücklich festgelegt, was geschehen sollte, wenn eine Fluggesellschaft API-Daten an den Router übermittelt hat, bevor es ihr aufgrund eines Ausfalls der Systeme oder Infrastruktur eines oder mehrerer Mitgliedstaaten technisch unmöglich geworden ist, die API-Daten anschließend zu übermitteln.

43. Der EDSB empfiehlt daher, in Artikel 12 des Vorschlags „API-Grenzmanagement" klarzustellen, dass die Daten automatisch gelöscht werden, wenn es dem Router technisch nicht möglich ist, die API-Daten anschließend an die zuständigen nationalen Behörden zu übermitteln.

[35] https://edps.europa.eu/sites/default/files/publication/2018-04-16_interoperability_opinion_en.pdf
[36] https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf
[37] https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_en.pdf
[38] https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_en.pdf
[39] https://edps.europa.eu/sites/default/files/publication/18-12-13_opinion_vis_en.pdf
[40] https://edps.europa.eu/sites/edp/files/publication/17-10-10_eu-lisa_opinion_en_0.pdf

8. Sonstige Bemerkungen

44. Der EDSB stellt fest, dass Artikel 4 Absatz 1 Satz 2 des Vorschlags „API Strafverfolgung“ ausdrücklich die Zuweisung der Verpflichtung zur Übermittlung von API-Daten in den Fällen klarstellt, in denen der Flug unter mehreren Fluggesellschaften aufgeteilt ist. Der Vorschlag „API Grenzmanagement“ enthält jedoch keine ähnliche Vorschrift. Daher empfiehlt der EDSB, in den Vorschlag „API Grenzmanagement“ eine ähnliche Bestimmung über Code-Sharing-Flüge aufzunehmen.

9. Schlussfolgerungen

45. Vor diesem Hintergrund spricht der EDSB folgende Empfehlungen an die Mitgesetzgeber aus:

(1) die Ausarbeitung harmonisierter Kriterien und Methoden für die Auswahl von EU-Flügen in Erwägung zu ziehen, von denen API-Daten erhoben werden sollten;

(2) in dem Vorschlag „API Strafverfolgung“ spezifische Maßnahmen vorzusehen, die die Sicherheit von API-Daten gewährleisten, die zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität verarbeitet werden, oder alternativ auf die einschlägigen Sicherheitsvorschriften im Vorschlag „API Grenzmanagement“ zu verweisen;

(3) in Artikel 12 des Vorschlags „API Grenzmanagement“ klarzustellen, dass die Daten automatisch gelöscht werden sollten, wenn es dem Router technisch nicht möglich ist, die API-Daten anschließend an die zuständigen nationalen Behörden zu übermitteln;

(4) im Vorschlag „API Grenzmanagement“ die Zuweisung der Verpflichtung zur Übermittlung von API-Daten in Fällen klarzustellen, in denen der Flug Gegenstand von Code-Sharing seitens mehrerer Fluggesellschaften ist.

Brüssel, den 8. Februar 2023

(elektronisch unterzeichnet)
Wojciech Rafał WIEWIÓROWSKI