



# EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data  
protection authority

25. Mai 2021

## Stellungnahme 8/2021

zu der Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Kooperationsabkommen zwischen der EU und Interpol

*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“; gemäß Artikel 52 Absatz 3 ist er „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 Wiewiorowski für einen Zeitraum von fünf Jahren zum Europäischen Datenschutzbeauftragten ernannt.*

**Artikel 42 Absatz 1** der Verordnung (EU) 2018/1725 besagt: „Nach 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, konsultiert die Kommission den EDSB“, und gemäß Artikel 57 Absatz 1 Buchstabe g muss der EDSB „von sich aus oder auf Anfrage alle Organe und Einrichtungen der Union bei legislativen und administrativen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten beraten.“

*In dieser Stellungnahme geht es um den Auftrag des EDSB, die EU-Organe bezüglich der kohärenten und konsequenten Anwendung der EU-Datenschutzgrundsätze im Zusammenhang mit der Aushandlung von Abkommen im Bereich der Strafverfolgung zu beraten. Diese Stellungnahme basiert auf der allgemeinen Verpflichtung, dass von der EU geschlossene internationale Vereinbarungen mit den Bestimmungen des AEUV übereinstimmen und die Grundrechte, die ein zentraler Grundsatz des Unionsrechts sind, wahren müssen. Insbesondere ist die Einhaltung von Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union sowie Artikel 16 AEUV sicherzustellen.*

## Zusammenfassung

Am 14. April 2021 nahm die Kommission eine Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Kooperationsabkommen zwischen der EU und der Internationalen Kriminalpolizeilichen Organisation (Interpol) an.

Trotz der bestehenden Zusammenarbeit mit Interpol ermittelte die Kommission Bereiche, in denen die Zusammenarbeit intensiviert oder sogar in neuen Bereichen eingerichtet werden könnte und sollte, um einer Reihe unverzichtbarer operativer Erfordernisse gerecht zu werden und bestehende Rechtsakte umzusetzen, um die Mitgliedstaaten bei der Verhütung und Bekämpfung von Terrorismus und organisierter Kriminalität besser zu unterstützen. Diese operativen Erfordernisse erfordern den Abschluss eines Kooperationsabkommens mit Interpol.

Der EDSB möchte betonen, dass das Ziel, die (gegenwärtige und künftige) Zusammenarbeit zwischen der EU und Interpol bei einer breiten Palette von Tätigkeiten in einem einzigen Rechtsinstrument zu unterstützen, das geplante Abkommen sehr heterogen macht. Er betont daher, dass **eine eingehende Folgenabschätzung** erforderlich sein wird und dass der Ansatz nicht zu einer Schwächung der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihrer Rechte auf Datenschutz und Privatsphäre, führen darf.

Das Datenschutzrecht der EU sieht grundsätzlich vor, dass Datenübermittlungen an eine internationale Organisation ohne zusätzliche Anforderungen nur dann erfolgen können, wenn diese internationale Organisation ein angemessenes Schutzniveau gewährleistet. Sichert die internationale Organisation kein angemessenes Schutzniveau zu, gelten Ausnahmen für spezifische Datenübermittlungen, sofern geeignete Schutzmaßnahmen ergriffen werden. Daher spricht der EDSB im Wesentlichen drei Empfehlungen aus, um sicherzustellen, dass das geplante Abkommen geeignete Garantien bieten kann:

- In den Verhandlungsrichtlinien sollte klargestellt werden, dass sichergestellt werden muss, dass das geplante Abkommen generell mit der Charta, den einschlägigen horizontalen Datenschutzvorschriften (Verordnung (EU) 2018/1725, Verordnung (EU) 2016/679 und Richtlinie (EU) 2016/680) sowie den spezifischen Datenschutzerfordernissen und Garantien in den Basisrechtsakten zur Errichtung der EU-Agenturen oder IT-Systeme im Einklang steht.
- In dem künftigen Abkommen sollte ausdrücklich klargestellt werden, dass Interpol keinen direkten oder indirekten Zugang zu den EU-Datenbanken haben wird.
- Im Zusammenhang mit Weiterübermittlungen sollte ausdrücklich festgelegt werden, dass die von der EU an Interpol übermittelten personenbezogenen Daten nicht dazu verwendet werden, eine Todesstrafe oder eine Form grausamer und unmenschlicher Behandlung zu beantragen, zu verhängen oder zu vollstrecken.

Schließlich empfiehlt der EDSB, dass die Bezugsvermerke in der Präambel der Empfehlung nicht nur auf die angemessene verfahrensrechtliche Grundlage, sondern auch auf die einschlägige materiellrechtliche Grundlage verweisen, darunter in Anbetracht des Gegenstands des künftigen Abkommens Artikel 16 AEUV.

Der EDSB steht auch weiterhin während der Verhandlungen und der förmlichen Konsultation, die zu dem Vorschlag an den Rat für die Unterzeichnung und den Abschluss des Abkommens gemäß

Artikel 218 AEUV gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 stattfinden muss, beratend zur Verfügung.

# Inhalt

<b>1. Einleitung und Hintergrund.....</b>	<b>5</b>
<b>2. Ganzheitlicher Ansatz.....</b>	<b>7</b>
2.1. <b>Es fehlt eine eingehende Folgenabschätzung zu den Grundrechten.....</b>	<b>7</b>
2.2. <b>Das geplante Abkommen sollte das Schutzniveau nicht senken.....</b>	<b>8</b>
<b>3. Zur Notwendigkeit angemessener Datenschutzgarantien.....</b>	<b>10</b>
<b>4. Zur Rechtsgrundlage des künftigen Beschlusses des Rates.....</b>	<b>15</b>
<b>5. Schlussfolgerungen .....</b>	<b>15</b>

## **DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –**

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf die Artikel 7 und 8,

gestützt auf 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 (Datenschutz-Grundverordnung)<sup>1</sup>,

gestützt auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates<sup>2</sup>,

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<sup>3</sup>, insbesondere auf Artikel 42 Absatz 1 –

### **HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:**

## **1. Einleitung und Hintergrund**

1. Die Internationale Kriminalpolizeiorganisation (Interpol)<sup>4</sup> ist mit 194 Mitgliedstaaten die weltweit größte zwischenstaatliche kriminalpolizeiliche Organisation. Die EU und Interpol arbeiten bereits seit langem intensiv in einer Reihe von Rechtsdurchsetzungsbereichen zusammen. Interpol ist ein wichtiger Partner der EU im Bereich der inneren und äußeren Sicherheit, einschließlich der Bekämpfung von Terrorismus und organisierter Kriminalität, sowie im Bereich des integrierten Grenzmanagements.
2. In der EU-Strategie für eine Sicherheitsunion von 2020<sup>5</sup> werden die Mitgliedstaaten aufgefordert, die Zusammenarbeit zwischen der EU und Interpol zu intensivieren, da dies für die Verbesserung der Zusammenarbeit und des Informationsaustauschs von wesentlicher Bedeutung ist. In der Strategie wird eingeräumt, dass Interpol in dieser Hinsicht eine wichtige Aufgabe zukommt. Neben der bestehenden Zusammenarbeit mit Interpol wurden Bereiche ermittelt, in denen die Zusammenarbeit verstärkt oder auch erst eingerichtet werden könnte, um einer Reihe operativer Erfordernisse gerecht zu werden und bestehende Rechtsakte umzusetzen, um die Mitgliedstaaten bei der Verhütung und Bekämpfung von Terrorismus und organisierter Kriminalität besser zu unterstützen.
3. Daher hat die Kommission am 14. April 2021 eine Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Kooperationsabkommen zwischen der EU und Interpol<sup>6</sup> (im Folgenden „Empfehlung“) angenommen.

4. Der Begründung zufolge<sup>7</sup> sollen mit dem geplanten Kooperationsabkommen zwischen der EU und Interpol folgende Ziele verfolgt werden:
- Regelung der Beziehungen zwischen der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (**Europol**)<sup>8</sup> und Interpol, unter Berücksichtigung der jüngsten Entwicklungen bei der Bekämpfung des Terrorismus sowie der grenzüberschreitenden und transnationalen schweren organisierten Kriminalität sowie der derzeitigen operativen Erfordernisse, des Mandats von Europol und der neuesten Datenschutzregelung der EU.
  - Bereitstellung der erforderlichen Schutzvorkehrungen und Garantien für einen kontrollierten Zugang zu Interpols Datenbank für gestohlene und verlorene Reisedokumente (SLTD) und zur Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (TDAWN) über das Europäische Suchportal (ESP) **durch EU-Mitgliedstaaten und EU-Agenturen**, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, im Einklang mit ihren Zugangsrechten, mit EU- oder nationalem Recht, das einen solchen Zugang abdeckt, und in voller Übereinstimmung mit den EU-Datenschutzanforderungen und den Anforderungen der Grundrechte.<sup>9</sup>
  - Bereitstellung der erforderlichen Schutzvorkehrungen und Garantien, damit die **EU-Mitgliedstaaten** und **Frontex**<sup>10</sup> (ihre Zentraleinheit für das Europäische Reiseinformations- und -genehmigungssystem (ETIAS)) über das ESP unter Wahrung der EU-Datenschutzanforderungen und der Grundrechte auf die Interpol-Datenbanken zugreifen können.
  - Bereitstellung der erforderlichen Schutzvorkehrungen und Garantien für die Umsetzung einer **überarbeiteten Verordnung über das Visa-Informationssystem**<sup>11</sup>, die es den **EU-Mitgliedstaaten** ermöglicht, bei der Prüfung von Visumanträgen oder Aufenthaltstiteln über das ESP auf die Datenbanken SLTD und TDAWN zuzugreifen, und zwar in voller Übereinstimmung mit den EU-Datenschutzanforderungen und den Anforderungen an die Grundrechte.
  - Aufbau und Regelung der Zusammenarbeit zwischen der durch die Verordnung (EU) 2017/1939 („EUSa-Verordnung“)<sup>12</sup> eingerichteten Europäischen Staatsanwaltschaft („EUSa“) und Interpol im Einklang mit ihren Mandaten und in voller Übereinstimmung mit den EU-Datenschutzanforderungen und den Anforderungen der Grundrechte.
  - Schaffung der Rechtsgrundlage für die Ermächtigung von **Europol, von Frontex-Personal der Kategorie 1** (Statutspersonal der ständigen Reserve<sup>13</sup>) und **EUSa zum Zugriff auf einschlägige Interpol-Datenbanken** zur Erfüllung ihrer Aufgaben, in voller Übereinstimmung mit den EU-Datenschutzanforderungen und den Anforderungen der Grundrechte.
  - Schaffung der Rechtsgrundlage für die Ermächtigung von **Eurojust<sup>14</sup> und der EUSa** zum Austausch **operativer Informationen** mit Interpol in voller Übereinstimmung mit den EU-Datenschutzanforderungen und den Anforderungen an die Grundrechte.
5. Gemäß Artikel 42 Absatz 1 der Verordnung 2018/1725 konsultiert die Kommission nach der Annahme einer Empfehlung an den Rat nach Artikel 218 AEUV, die Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten hat, den EDSB. Der EDSB wurde bereits während der Ausarbeitung der Empfehlung auch informell konsultiert und übermittelte seine informellen Anmerkungen

im August 2020. Er begrüßt, dass seine Ansichten in einem frühen Stadium des Verfahrens eingeholt (und in gewissem Umfang umgesetzt) wurden, und fordert die Kommission auf, dieses bewährte Verfahren fortzusetzen.

6. Der EDSB wurde formell am 14. April 2021 von der Kommission konsultiert und erwartet, dass in der Präambel des Ratsbeschlusses auf die vorliegende Stellungnahme verwiesen wird. Diese Stellungnahme greift etwaigen künftigen zusätzlichen Bemerkungen oder Empfehlungen des EDSB nicht vor, insbesondere wenn weitere Probleme festgestellt werden oder neue Informationen verfügbar werden, sowie der förmlichen Konsultation, die gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 zu den Vorschlägen für die Unterzeichnung und den Abschluss des Abkommens an den Rat stattfinden muss. In diesem Zusammenhang begrüßt der EDSB Erwägungsgrund 19 der Empfehlung, wonach die Kommission ihn während der Aushandlung des Abkommens bzw. in jedem Fall vor Abschluss des Abkommens konsultieren sollte. Darüber hinaus greift diese Stellungnahme etwaigen künftigen Maßnahmen, die der EDSB in Ausübung seiner Befugnisse gemäß Artikel 58 der Verordnung (EU) 2018/1725 einleitet, nicht vor.

## 2. Ganzheitlicher Ansatz

7. Der EDSB betont, dass das Ziel, einen erheblichen Umfang der (derzeitigen und künftigen) Zusammenarbeit zwischen der EU und Interpol mit einem einzigen Rechtsinstrument zu untermauern, das geplante Abkommen **sehr heterogen** macht, da es ein breites Spektrum von Tätigkeiten umfasst, darunter die polizeiliche Zusammenarbeit (Artikel 87 und 88 AEUV), die justizielle Zusammenarbeit in Strafsachen (Artikel 82 und 85 AEUV), die Grenzsicherheit als Teil des Grenzmanagements (Artikel 77 AEUV), Visa und Aufenthaltstitel und die Europäische Staatsanwaltschaft (Artikel 86 AEUV), an der sich nicht alle Mitgliedstaaten beteiligen.<sup>15</sup>
8. Angesichts dieses heterogenen Ansatzes unterstreicht er 1) die Notwendigkeit einer eingehenden Folgenabschätzung und 2), dass der Ansatz nicht zu einer Schwächung der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihrer Rechte auf Datenschutz und Privatsphäre führen sollte.

### 2.1. Es fehlt eine eingehende Folgenabschätzung zu den Grundrechten

9. Die Heterogenität des geplanten Abkommens und die möglichen Auswirkungen eines solchen Abkommens auf die Grundrechte, insbesondere auf den Schutz der Privatsphäre und den Datenschutz, erfordern eine eingehende Folgenabschätzung. Der EDSB bedauert, dass die Empfehlung der Kommission nicht mit einer Folgenabschätzung zu den Grundrechten einherging und fordert den Rat auf, eine eingehende Folgenabschätzung in Bezug auf Grundrechte und Datenschutz durchzuführen<sup>16</sup>, die a) die **Notwendigkeit und Verhältnismäßigkeit jeder geplanten Maßnahme, sofern sie** das Recht auf Privatsphäre und den Schutz personenbezogener Daten<sup>17</sup> **einschränkt**, und b) die **rechtliche Durchführbarkeit** einer Regulierung all dieser Maßnahmen im Rahmen eines **einzig** übergreifenden Abkommens umfasst.<sup>18</sup> Besondere Vorsicht ist geboten<sup>19</sup> angesichts der Sensibilität der betreffenden Daten und der Zahl der Drittländer, die Interpol-Mitglieder sind und kein gleichwertiges Abkommen mit der EU abgeschlossen haben oder deren Behörden, an

die personenbezogene Daten übermittelt werden sollen, nicht von einem Angemessenheitsbeschluss der Kommission erfasst werden.<sup>20</sup>

10. Bei der Bewertung der Notwendigkeit und Verhältnismäßigkeit der geplanten Anwendungsfälle im Rahmen jedes Ziels sollte insbesondere auf die **Zwecke der Verarbeitung sowie die Menge und die Kategorien der betreffenden personenbezogenen Daten** eingegangen werden. Insbesondere sollte geprüft werden, auf welche Datenbanken – beispielsweise auch die Interpol-Ausschreibungen – zugegriffen werden sollte und nach welchen Modalitäten. Aus der Bewertung sollte auch die Notwendigkeit des vorgesehenen Zugriffs auf die **einzelnen Interpol-Datenbanken** (im Vergleich zu bereits verfügbaren Datenbanken) hervorgehen.
11. Die Folgenabschätzung sollte auch **mit Blick auf die Risiken für die betroffenen Personen** durchgeführt werden, wobei zu berücksichtigen ist, dass es sich dabei um schutzbedürftige Personen wie Migranten und möglicherweise Asylsuchende handeln könnte.

## 2.2. Das geplante Abkommen sollte das Schutzniveau nicht senken

12. Der EDSB ist der Auffassung, dass **die Empfehlung präzisiert werden sollte, um zu vermeiden, dass das derzeit durch das Primär- und Sekundärrecht der EU gewährleistete Schutzniveau für Einzelpersonen gesenkt wird.**
13. Er weist darauf hin, dass **der in der Empfehlung vorgesehene Austausch personenbezogener Daten möglicherweise nicht immer im Einklang mit dem Sekundärrecht der EU steht, mit dem die Tätigkeiten der Organe, Einrichtungen und sonstigen Stellen der EU, die mit Interpol zusammenarbeiten, festgelegt oder geregelt werden.**
14. Der Mangel an Klarheit in Bezug auf die spezifischen Zwecke, die Art der auszutauschenden Daten sowie die genaue Zuweisung der Aufgaben und Zuständigkeiten wirkt sich nachteilig auf das Erfordernis der Qualität des Rechts aus, das für **alle Maßnahmen, mit denen** die in den Artikeln 7 und 8 der Charta und in Artikel 16 AEUV verankerten **Rechte eingeschränkt werden**, von größter Bedeutung ist.
15. Diese Bedenken werden insbesondere durch Formulierungen wie „das Abkommen sollte *die Rechtsgrundlage für die Ermächtigung von Europol, von Frontex-Personal Kategorie 1 (Statutpersonal der ständigen Reserve) und der EUStA zum Zugriff auf einschlägige Interpol-Datenbanken zur Erfüllung ihrer Aufgaben schaffen*“ hervorgerufen.<sup>21</sup> Angesichts des sensiblen Charakters der betreffenden Daten bekräftigt der EDSB, dass **es von entscheidender Bedeutung ist, dass alle erforderlichen Spezifikationen in die Verhandlungsrichtlinien aufgenommen werden.**
16. Der EDSB ist insbesondere der Auffassung, dass **wirklich jede Art der Zusammenarbeit** mit Interpol, die im Rahmen des geplanten übergreifenden Abkommens geregelt ist,
  - klar **den/die Zweck(e) und die Ziele der Zusammenarbeit zwischen Interpol und den betreffenden Organen, Einrichtungen und sonstigen Stellen der EU** angibt. Es ist wichtig, dass der angegebene Zweck nicht über das hinausgeht, was in den bestehenden Rechtsinstrumenten vorgeschrieben ist, und insbesondere im Einklang mit dem jeweiligen Mandat der betreffenden Organe, Einrichtungen oder sonstigen Stellen der EU steht. Mit dem geplanten Abkommen sollten keine neuen Datenverarbeitungsvorgänge eingeführt werden, die nicht durch die bestehenden Rechtsgrundlagen abgedeckt sind. In diesem Zusammenhang empfehlen wir klarzustellen, dass das geplante Abkommen **keinen**

**gegenseitigen direkten oder indirekten Zugang von Interpol zu EU-Datenbanken vorsieht;**

- **dem Unterschied** zwischen der *justiziellen Zusammenarbeit in Strafsachen* und der *polizeilichen Zusammenarbeit* einerseits und dem *Grenzmanagement* andererseits gebührend Rechnung tragen;
- den **Vorschriften entsprechen, die in den EU-Rechtsakten** zur Einrichtung der Agenturen, Ämter und Einrichtungen der Union, zur Regelung ihrer Tätigkeiten oder im Rahmen des EU-Datenschutzrahmens **festgelegt sind**.

17. Hierzu ist unter **Punkt 2 im Anhang** über die Verhandlungsrichtlinien festgelegt, dass das Abkommen die Schutzvorkehrungen und Garantien bereitstellen sollte, die erforderlich sind, um EU-Mitgliedstaaten und **EU-Agenturen** einen kontrollierten Zugang zu den Datenbanken SLTD und TDawn über das ESP zu genehmigen, **soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, im Einklang mit ihren Zugangsrechten**, mit EU- oder nationalem Recht, das einen solchen Zugang abdeckt, und in voller Übereinstimmung mit den EU-Datenschutzanforderungen und den Anforderungen an die Grundrechte“ (Hervorhebung hinzugefügt). Nach Auffassung des EDSB ist dieser Passus unklar, da der Zugang von Frontex (ETIAS und Frontex-Personal der Kategorie 1), Europol und der EUStA zu diesen Datenbanken bereits durch andere Verhandlungsrichtlinien abgedeckt ist.<sup>22</sup> **Nach Auffassung des EDSB wurde die Notwendigkeit eines solchen Zugangs für andere EU-Agenturen nicht nachgewiesen.** Sollte sie nachgewiesen werden<sup>23</sup>, **sollte in den Verhandlungsrichtlinien eindeutig festgelegt werden, welche EU-Agenturen für welche ihrer spezifischen Aufgaben Zugangsrechte haben sollten.**
18. Mit Blick auf Frontex wird in **Erwägungsgrund 13** der Empfehlung auf Artikel 68 Absatz 1 der Frontex-Verordnung als geeignete Rechtsgrundlage für die Zusammenarbeit von Frontex mit Interpol verwiesen und erklärt, dass gemäß Artikel 82 Absatz 1 dieser Verordnung Mitgliedern von Teams der Kategorie 1 der Zugang zu den Interpol-Datenbanken (insbesondere SLTD) gewährt werden sollte, um Aufgaben und Befugnisse für Grenzkontrollen gemäß Artikel 8 Absatz 3 Buchstabe a Ziffer i, Artikel 8 Absatz 3 Buchstabe a Ziffer ii und Artikel 6 Absatz 1 Buchstabe e der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates<sup>24</sup> („Schengener Grenzkodex“) wahrnehmen zu können. Nach diesen Bestimmungen können solche Frontex-Mitarbeiter Drittstaatsangehörige mit den Interpol-Datenbanken, insbesondere SLTD, an den Außengrenzen der Mitgliedstaaten und der Drittländer, die bei der Umsetzung, Anwendung und Weiterentwicklung des Schengen-Besitzstands in Bezug auf Personenkontrollen an den Außengrenzen assoziiert sind, abgleichen. Die letztgenannte Bestimmung enthält neben anderen Einreisevoraussetzungen für Drittstaatsangehörige die Bedingung, dass Drittstaatsangehörige keine Gefahr für die öffentliche Ordnung, die innere Sicherheit, die öffentliche Gesundheit oder die internationalen Beziehungen eines Mitgliedstaats darstellen. Die Empfehlung scheint jedoch über den Anwendungsbereich dieser Bestimmung hinauszugehen, wenn in ihrer Begründung<sup>25</sup> darauf hingewiesen wird, dass ein solcher Zugang nicht nur dem Zweck von Grenzübertrittskontrollen, sondern auch der Verhütung und Untersuchung terroristischer Straftaten dient. Daher **empfiehlt der EDSB, in der Empfehlung klarzustellen, zu welchen Zwecken ein solcher Zugang gewährt werden sollte, wobei die Kohärenz mit Artikel 10 Buchstabe q und Artikel 90 der Frontex-Verordnung zu gewährleisten ist, wenn zu diesen Zwecken auch die Verhütung und Untersuchung terroristischer Straftaten gehören sollte. Außerdem sollte im Mandat klargestellt werden, auf welche Datenbanken und zu welchen Zwecken die Mitglieder von Teams der Kategorie 1 zugreifen können sollten.** In jedem Fall stellt der EDSB gemäß der in Erwägungsgrund 13 genannten Rechtsgrundlage fest, dass

das geplante Abkommen nur den Zugang zu den Interpol-Datenbanken für die Überprüfung von Drittstaatsangehörigen abdecken würde.

19. Ganz allgemein vertritt der EDSB die Auffassung, dass das geplante Abkommen keine Verpflichtung für die EU-Agenturen begründen sollte, mit Interpol über das Maß hinaus zusammenzuarbeiten, das bereits im einschlägigen Unionsrecht vorgesehen ist.
20. Schließlich sollte klargestellt werden, ob sich der Begriff „**operative Informationen**“ im Sinne von **Punkt 7 des Anhangs** der Empfehlung auf Informationen bezieht, die bei Einsätzen, auch zu Verwaltungszwecken (wie Befragungen oder administrative Bearbeitung eingehender Personen usw.) erhoben und analysiert werden, oder ob er sich auf „operative personenbezogene Daten“ im Sinne der Verordnung (EU) 2018/1725 bezieht, d. h. auf personenbezogene Daten, die von Einrichtungen oder sonstigen Stellen der Union bei der Ausübung von Tätigkeiten verarbeitet werden, die in den Anwendungsbereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Sinne der Definition im AEUV fallen, um die Ziele und Aufgaben zu erfüllen, die in ihren Gründungsrechtsakten festgelegt sind. **In dieser Hinsicht ist der unter Punkt 7 des Anhangs verwendete Wortlaut noch sehr weit gefasst, so dass er so verstanden werden könnte, dass er ein Mandat für die Begründung einer Zusammenarbeit über das bereits im Sekundärrecht der EU vorgesehene Maß hinaus erteilt.**

### 3. Zur Notwendigkeit angemessener Datenschutzgarantien

21. Der *Besitzstand* der EU im Bereich des Datenschutzes, der vor dem Hintergrund von Artikel 8 der Charta und Artikel 16 AEUV zu lesen ist, sieht grundsätzlich vor, dass internationale Datenübermittlungen an eine internationale Organisation ohne zusätzliche Anforderungen nur dann erfolgen können, wenn diese internationale Organisation ein angemessenes Schutzniveau gewährleistet. Sichert die internationale Organisation kein angemessenes Schutzniveau zu, gelten Ausnahmen für spezifische Datenübermittlungen, sofern geeignete Garantien geboten werden.
22. In Ermangelung eines Angemessenheitsbeschlusses in Bezug auf Interpol könnte das geplante Abkommen daher eine Rechtsgrundlage bieten, die die Übermittlung personenbezogener Daten an Interpol **unter der Voraussetzung erlaubt, dass es rechtsverbindlich und gegenüber allen Vertragsparteien des Abkommens durchsetzbar wäre und angemessene Datenschutzgarantien enthalten** würde. Gemäß Artikel 46 der Verordnung (EU) 2018/1725 muss jede Übermittlung personenbezogener Daten durch Organe, Einrichtungen und sonstige Stellen der EU an internationale Organisationen auch die Bedingungen der anderen Bestimmungen der Verordnung erfüllen. Daher muss jede Übermittlung den Datenschutzgrundsätzen von Artikel 4 entsprechen und eine der in den Artikeln 5 und 10 (bezüglich besonderer Datenkategorien) vorgesehenen Rechtsgrundlagen haben. Somit muss ein zweistufiger Ansatz verfolgt werden: Erstens sollte die Datenverarbeitung gemäß allen einschlägigen Bestimmungen der Verordnung rechtmäßig sein, und zweitens müssen die Bestimmungen von Kapitel V eingehalten werden. Artikel 46 sieht vor, dass eine Übermittlung von Daten an eine internationale Organisation das durch diese Verordnung garantierte Schutzniveau nicht beeinträchtigen darf, und insbesondere müssen **den betroffenen Personen durchsetzbare und wirksame Rechte eingeräumt werden**.<sup>26</sup>
23. Der EDSB begrüßt, dass in mehreren Verhandlungsrichtlinien im Anhang auf die Gewährleistung der Zusammenarbeit in voller Übereinstimmung mit den EU-

Datenschutzanforderungen und den Anforderungen an die Grundrechte der EU verwiesen wird. Im Mandat sollte jedoch klargestellt werden, dass dieser Ausdruck „*in voller Übereinstimmung mit den EU-Datenschutzanforderungen und den Anforderungen an die Grundrechte*“ eine Übereinstimmung auf folgenden drei Ebenen umfasst:

- generell mit der Charta, insbesondere mit den Artikeln 7, 8 und 52;
- mit den einschlägigen horizontalen Datenschutzvorschriften: Verordnung (EU) 2018/1725, Richtlinie (EU) 2016/680 und Verordnung (EU) 2016/679;
- mit den spezifischen Datenschutzanforderungen und Garantien in den Basisrechtsakten zur Einrichtung der EU-Agenturen oder IT-Systeme.

24. In diesem Zusammenhang betont der EDSB, dass Artikel 94 der Verordnung (EU) 2018/1725 auf die Übermittlung operativer Daten zu Gefahrenabwehr- und Strafverfolgungszwecken Anwendung findet, mit Ausnahme der EUSa und Europols, für die ihre jeweiligen Verordnungen gelten.<sup>27</sup> Daher begrüßen wir **Erwägungsgrund 16** zur Übermittlung operativer Daten, doch dürfte er **unvollständig sein**, da er nicht auf die spezifischen Bestimmungen für die Übermittlung operativer Daten durch Europol und die EUSa verweist, die nicht unter die Verordnung (EU) 2018/1725, sondern unter die Europol- bzw. die EUSa-Verordnung fällt. Außerdem sollte ein **Verweis auf die Eurojust-Verordnung** hinzugefügt werden, da die allgemeinen Bestimmungen des gesonderten Kapitels der Verordnung (EU) 2018/1725 über die Verarbeitung operativer Daten unbeschadet der spezifischen Datenschutzbestimmungen in der Eurojust-Verordnung gelten.<sup>28</sup>
25. Gleichzeitig begrüßt der EDSB, dass in Buchstabe c des Anhangs vorgesehen ist, dass das Abkommen „*eine genaue Formulierung der Schutzvorkehrungen und Kontrollen, die für den Schutz personenbezogener Daten sowie der Grundrechte und Grundfreiheiten natürlicher Personen, unabhängig von der Staatsangehörigkeit und ihrem Wohnort, beim Austausch personenbezogener Daten mit Interpol erforderlich sind*“ vorsieht und dass in den Ziffern i bis xi einige Grundsätze und Garantien aufgeführt werden. Er betont jedoch, wie wichtig es ist, **konkrete, spezifische und wirksame Garantien für jede Art der Zusammenarbeit im Abkommen** vorzusehen. In Anbetracht des Strafverfolgungskontexts und der potenziellen Risiken, die solche Übermittlungen für betroffene Personen bedeuten können, sollten die in dem geplanten Abkommen mit Interpol vorgesehenen Garantien auf zufriedenstellende Weise auf diese Risiken eingehen und sie mindern.
26. Der ganzheitliche Ansatz birgt besondere Risiken für die Grundrechte: erstens die Gefahr, dass das Schutzniveau, das im derzeitigen EU-Rechtsrahmen vorgesehen ist, gesenkt wird, und zweitens die Gefahr, dass Rechtsunsicherheit entsteht. **In den Verhandlungsrichtlinien, insbesondere unter Buchstabe c über die erforderlichen Schutzvorkehrungen und Kontrollen, wird nicht klar zwischen den verschiedenen Arten von Tätigkeiten und der Datenverarbeitung unterschieden**, obwohl sie in unterschiedlichen Rechtsinstrumenten geregelt sind<sup>29</sup> und daher erforderlichenfalls geeignete Schutzvorkehrungen und Anforderungen verlangen, die an jedes „Szenario“ angepasst sind. In diesem Zusammenhang weist der EDSB darauf hin, dass die Europäische Kommission im EU-Sekundärrecht in Bezug auf den Zugang zu den Interpol-Datenbanken SLTD und TDAWN über das ESP für Grenzen und Visa einerseits und die polizeiliche Zusammenarbeit andererseits unterschiedliche Ansätze verfolgt hat. Dieser Zugang wurde in zwei getrennten Verordnungen (Verordnungen (EU) 2019/817 und 2019/818) geregelt, um, wie die Europäische Kommission in ihren Vorschlägen für diese Instrumente erläutert hat, „die Unterscheidung zwischen den Bereichen, die eine Weiterentwicklung des Schengen-Besitzstands in Bezug auf Grenzen und Visa darstellen, und anderen Systemen, die

den Schengen-Besitzstand im Bereich der polizeilichen Zusammenarbeit betreffen oder nicht mit dem Schengen-Besitzstand in Zusammenhang stehen (...) zu respektieren“.

27. Vor diesem Hintergrund empfiehlt der EDSB, in **Erwägungsgrund 17** der Empfehlung auch **auf die Datenschutzbestimmungen der Rechtsakte zur Errichtung der von dem geplanten Abkommen betroffenen Agenturen und Stellen der Union** Bezug zu nehmen. Der EU-Rechtsrahmen für den Datenschutz setzt sich in der Tat aus verschiedenen Rechtsquellen zusammen, darunter eine Reihe von EU-Sekundärrechtsvorschriften, die für spezifische Datenübermittlungen gelten und in der Regel die Übermittlung an internationale Organisationen untersagen und nur im Ausnahmefall unter strengen Bedingungen zulassen.<sup>30</sup>
28. Was **Europol** anbelangt, so ersucht der EDSB den Rat, dafür Sorge zu tragen, dass das geplante Abkommen nicht unter das Niveau der Datenschutzgarantien gemäß der Europol-Verordnung – in der ausdrücklich auf die Zusammenarbeit und den Austausch von Informationen, einschließlich personenbezogener Daten, zwischen Interpol und Europol Bezug genommen wird – und unter das des derzeitigen bilateralen Abkommens geht. So heißt es beispielsweise im Anhang unter **Buchstabe c Ziffer ii**: *„Das Abkommen muss einen Geltungsbereich beinhalten, um bei der Übermittlung der Daten etwaige Zugangs- oder Nutzungsbeschränkungen anzugeben, einschließlich einer Beschränkung der Datenübertragung, -löschung oder -vernichtung.“* Artikel 19 Absatz 2 der Europol-Verordnung sieht in Bezug auf solche Einschränkungen ferner vor: *„Sollten sich derartige Einschränkungen erst nach der Übermittlung der Informationen als notwendig erweisen, so setzen [internationale Organisationen] Europol hiervon in Kenntnis. Europol leistet diesen Einschränkungen Folge.“* **Eine solche Unterrichtungspflicht sollte in das geplante Abkommen ebenfalls aufgenommen werden.** In Ziffer iv des Anhangs ist bestimmt: *„Im Abkommen muss festgelegt werden, anhand welcher Kriterien die Zuverlässigkeit der Quellen und die sachliche Richtigkeit der Daten festgestellt wird.“* Die Europol-Verordnung enthält jedoch bereits eine spezifische Bestimmung über die Zuverlässigkeit der Quelle und die Richtigkeit der von einem Mitgliedstaat stammenden Informationen (Artikel 29), in dem in Absatz 5 Folgendes festgelegt ist: *„Dieser Artikel gilt entsprechend, wenn Europol Daten oder Informationen von [...] [einer] internationalen Organisation [...] erhält.“* **Die Verhandlungsrichtlinien sollten geändert werden, um klarzustellen, dass das geplante Abkommen die in der Europol-Verordnung festgelegten Kriterien in Bezug auf die Zuverlässigkeit der Quelle und die Richtigkeit der Information<sup>31</sup> nicht untergraben sollte.** Ebenso sind in Bezug auf andere in die Empfehlung aufgenommene Agenturen und Einrichtungen weitere Änderungen erforderlich, um sicherzustellen, dass die einschlägigen Bestimmungen über die Verantwortung für die Richtigkeit der in ihren jeweiligen Mandaten enthaltenen Informationen durch das künftige EU-Interpol-Abkommen nicht untergraben werden .
29. In Bezug auf **Eurojust** enthalten die Artikel 47 und 56 (Allgemeine Grundsätze für die Übermittlung operativer personenbezogener Daten an Drittstaaten und internationale Organisationen) auch spezifische verbindliche Anforderungen für eine Zusammenarbeit, die die Übermittlung personenbezogener Daten an eine internationale Organisation mit sich bringt, einschließlich strenger Vorschriften für die Weiterübermittlung.
30. Die **EUStA** darf nach Artikel 80 (Allgemeine Grundsätze für die Übermittlung operativer personenbezogener Daten) der EUStA-Verordnung *„operative personenbezogene Daten unter Einhaltung der übrigen Bestimmungen dieser Verordnung, insbesondere Artikel 50, an ein Drittland oder an eine internationale Organisation nur übermitteln, wenn die Bedingungen gemäß den Artikeln 80 bis 83 eingehalten werden“*.

31. **Des Weiteren** betont der EDSB, wie wichtig es ist, ausreichende Schutzvorkehrungen vorzusehen, um sicherzustellen, dass die von Interpol übermittelten Informationen **sachlich richtig und vollständig** sind, da sie für Entscheidungen über Personen verwendet werden (so könnte z. B. im Zusammenhang mit ETIAS Einzelpersonen die Einreise in das Hoheitsgebiet der EU verweigert werden).
32. Darüber hinaus **empfiehlt der EDSB**, in den Anhang mindestens folgende Schutzvorkehrungen aufzunehmen:
- In dem geplanten Abkommen sollte klar geregelt werden, **wann und unter welchen Umständen automatisierte Einzelentscheidungen zulässig sind** (oder nicht) (**Buchstabe c Ziffer viii**);
  - **weitere Einzelheiten zur Benachrichtigungspflicht von Interpol im Falle einer Verletzung des Schutzes personenbezogener Daten (Buchstabe c Ziffer ix)**. Aus dem derzeitigen Wortlaut geht nicht hervor, wer wen zu benachrichtigen hat und wer die betroffenen Personen informiert. Je nach Art der Verletzung des Schutzes personenbezogener Daten sollte klargestellt werden, wann und ob Interpol die zuständigen Behörden (z.B. die EU-Agentur, die die Informationen bereitgestellt hat, ihre Aufsichtsstelle) und erforderlichenfalls die betroffenen Personen benachrichtigen sollte. Darüber hinaus sollte das Abkommen eine Beschreibung der Mindestangaben enthalten, die bei der Meldung der Verletzung (an die Aufsichtsstelle und die betroffene Person) zu übermitteln sind; und
  - **es sollten weitere operative Einzelheiten zu technischen und organisatorischen Maßnahmen für die Sicherheit** personenbezogener Daten bereitgestellt werden, einschließlich z. B. zu der Frage, wie die Vertraulichkeit der elektronischen Kommunikation gewährleistet würde.
33. Was den „**Austausch operativer Informationen**“ mit Interpol anbelangt, so werden in der Empfehlung die Modalitäten, Bedingungen, Grenzen und der Umfang der an Interpol übermittelten Daten, einschließlich personenbezogener Daten, nicht ausreichend spezifiziert. Noch kritischer wird diese Frage durch die Möglichkeit von **Weiterübermittlungen** von Interpol an andere internationale Organisationen oder Drittstaaten, einschließlich derer, für die kein Angemessenheitsbeschluss gemäß **Buchstabe c Ziffer x** des Anhangs ergangen ist. Für personenbezogene Daten, die von Agenturen und Einrichtungen der EU übermittelt werden, gilt gemäß Artikel 46 der Verordnung (EU) 2018/1725, dass eine Übermittlung personenbezogener Daten, die nach ihrer Übermittlung an eine internationale Organisation verarbeitet werden oder verarbeitet werden sollen, nur dann erfolgen dürfen, wenn vorbehaltlich der anderen Bestimmungen dieser Verordnung der Verantwortliche und der Auftragsverarbeiter die in deren Kapitel V festgelegten Bedingungen einhalten, einschließlich der Weiterübermittlung personenbezogener Daten von einer internationalen Organisation an ein anderes Drittland oder an eine andere internationale Organisation, um zu gewährleisten, dass der Schutz natürlicher Personen nicht durch diese Verordnung beeinträchtigt wird.
34. **Der EDSB empfiehlt** insbesondere, **die folgenden Schutzvorkehrungen in Bezug auf Weiterübermittlungen in die Verhandlungsrichtlinien aufzunehmen**:
- die Tatsache, dass die Übermittlung personenbezogener Daten der **Geheimhaltungspflicht** unterliegt und

– die Tatsache, dass die personenbezogenen Daten nicht verwendet werden, **um die Todesstrafe oder eine Form der grausamen und unmenschlichen Behandlung zu beantragen, zu verhängen oder zu vollstrecken.**<sup>32</sup>

35. In Artikel 50 der Verordnung (EU) 2018/1725 sind ferner **Ausnahmen** vorgesehen, denen zufolge eine Übermittlung trotz fehlender Angemessenheit oder geeigneter Garantien erfolgen kann, wenn dies zum Schutz lebenswichtiger Interessen einer Person erforderlich ist. Dies gilt jedoch nur, wenn die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben; eine Ausnahme zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit ist nicht vorgesehen. Ausnahmen sind darüber hinaus auch nicht vorgesehen für die Übermittlung operativer Daten gemäß Artikel 94 der Verordnung (EU) 2018/1725. Nur im Zusammenhang mit der Richtlinie (EU) 2016/680 ist eine Ausnahme aufgrund der öffentlichen Sicherheit eines Mitgliedstaats oder eines Drittlandes vorgesehen (Artikel 38 Absatz 1 Buchstabe c). **Der EDSB empfiehlt daher, die Anwendung von Ausnahmen für Weiterübermittlungen auf die Fälle zu beschränken, die bereits für die betreffenden Agenturen und Einrichtungen der EU bei der Übermittlung personenbezogener Daten zulässig sind.** In diesem Zusammenhang weist der EDSB erneut darauf hin, dass sichergestellt werden muss, **dass die spezifischen Anforderungen, die in den Verordnungen zur Einrichtung der betreffenden Agentur oder Stelle der EU festgelegt sind, eingehalten werden.**
36. In den Verhandlungsrichtlinien heißt es lediglich unter **Buchstabe c Ziffer x** des Anhangs: *„Die Weitergabe von Informationen von Interpol an andere internationale Organisationen oder Drittländer darf nur für die Zwecke des Abkommens gestattet werden“*, während beispielsweise Artikel 23 Absatz 7 der **Europol-Verordnung** vorsieht: *„Eine Weiterübermittlung von bei Europol gespeicherten personenbezogenen Daten durch [...] internationale Organisationen ist **nur mit vorheriger ausdrücklicher Genehmigung von Europol zulässig.**“* (Hervorhebung hinzugefügt.) Artikel 47 der **Eurojust-Verordnung** enthält Garantien für Weiterübermittlungen, an die das geplante Abkommen angepasst werden sollte. So heißt es insbesondere in Artikel 47 Absatz 6 der Eurojust-Verordnung ganz eindeutig: *„Eine **Weiterübermittlung** personenbezogener Daten, die Eurojust von [...] internationalen Organisationen erhalten hat, **an Dritte ist unzulässig, wenn nicht alle der folgenden Bedingungen erfüllt sind:**“*
- (a) *Eurojust hat die vorherige Zustimmung des Mitgliedstaats, der die Daten übermittelt hat, erhalten;*
- (b) *Eurojust hat nach Abwägung der Umstände des Einzelfalls der Weiterübermittlung ausdrücklich zugestimmt;*
- (c) *die Weiterübermittlung erfolgt nur zu einem bestimmten Zweck, der mit dem Zweck, zu dem die Daten übermittelt wurden, nicht unvereinbar ist.“* (Hervorhebung hinzugefügt.)
37. Ferner besagt Artikel 80 Absatz 1 Buchstabe e der **EUStA-Verordnung**, dass *„im Fall der Weiterübermittlung an ein anderes Drittland oder eine andere internationale Organisation durch ein Drittland oder eine internationale Organisation die EUStA das Drittland oder die internationale Organisation verpflichtet, **für die Weiterübermittlung bei ihr eine vorherige Genehmigung** einzuholen, welche die EUStA nur nach gebührender Berücksichtigung sämtlicher maßgeblicher Faktoren, einschließlich der Schwere der Straftat, des Zwecks der ursprünglichen Übermittlung operativer personenbezogener Daten und des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die operative personenbezogene Daten weiterübermittelt werden, erteilen darf“.*

38. Der EDSB stellt abschließend fest, dass **Buchstabe e des Anhangs** der Empfehlung die Möglichkeit vorsieht, das betreffende Abkommen auszusetzen oder zu kündigen. **Der EDSB empfiehlt, im Mandat festzulegen, dass das Abkommen bei Verstößen gegen seine Bestimmungen über personenbezogene Daten durch eine der Parteien eine solche Möglichkeit vorsehen sollte und dass personenbezogene Daten, die in den Geltungsbereich des Abkommens fallen und vor seiner Aussetzung oder Kündigung übermittelt wurde, weiterhin im Einklang mit dem Abkommen verarbeitet werden dürfen.**

## 4. Zur Rechtsgrundlage des künftigen Beschlusses des Rates

39. Aus der Begründung der Empfehlung<sup>33</sup> geht hervor, dass der Gegenstand des künftigen Abkommens insbesondere dem Bereich der Datenschutzinstrumente (Artikel 16 AEUV) zuzuordnen wäre. Die materielle Rechtsgrundlage des Rechtsakts wird jedoch in den Bezugsvermerken in der Präambel der Empfehlung nicht genannt.
40. Gemäß Artikel 296 Absatz 2 AEUV und der ständigen Rechtsprechung des EuGH<sup>34</sup> stellt der EDSB infrage, dass die Bezugsvermerke in der Präambel des Beschlusses des Rates nur auf die maßgebliche verfahrensrechtliche Grundlage und nicht ebenso auf die einschlägige materiellrechtliche Grundlage verweisen.
41. **Der EDSB empfiehlt, dass die Bezugsvermerke und Erwägungsgründe des Beschlusses des Rates nicht nur auf die angemessene verfahrensrechtliche Grundlage, sondern auch auf die einschlägige materiellrechtliche Grundlage verweisen, darunter Artikel 16 AEUV.** Aus dem Anhang mit den Verhandlungsrichtlinien ist ersichtlich, dass die Kommission während der Verhandlungen über das geplante Abkommen gleichzeitig mehrere Ziele verfolgen sollte, darunter die Wahrung der in der Charta verankerten Grundrechte, einschließlich der Rechte auf Schutz der Privatsphäre und auf Schutz personenbezogener Daten, damit eine rechtmäßige Übermittlung personenbezogener Daten erfolgen kann. Das geplante Abkommen würde sich somit direkt auf das von Artikel 16 AEUV verfolgten Zweck beziehen.
42. Der EDSB erinnert daran, dass der EuGH in einem ähnlichen Zusammenhang der Strafverfolgung befand, dass *„der Beschluss des Rates über den Abschluss des geplanten Abkommens [zwischen Kanada und der Europäischen Union über die Übertragung und Verarbeitung von Fluggastdatensätzen] auf Art. 16 Abs. 2 gemeinsam mit Art. 87 Abs. 2 Buchst. a AEUV zu stützen ist“*.<sup>35</sup>

## 5. Schlussfolgerungen

43. Der EDSB begrüßt, dass das Abkommen die Grundrechte und die in der Charta anerkannten Grundsätze uneingeschränkt achten sollte, insbesondere das Recht auf ein Privat- und Familienleben, das in Artikel 7 der Charta verankert ist, das Recht auf den Schutz personenbezogener Daten, das in Artikel 8 der Charta verankert ist, und das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht gemäß Artikel 47 der Charta.
44. Im Mandat sollte jedoch klargestellt werden, dass das Abkommen die folgenden drei Ebenen der Einhaltung umfassen sollte:

- generell der Charta;
  - der einschlägigen horizontalen Datenschutzvorschriften: Verordnung (EU) 2018/1725, Richtlinie (EU) 2016/680 und Verordnung (EU) 2016/679;
  - der spezifischen Datenschutzerfordernungen und Garantien in den Basisrechtsakten zur Einrichtung der EU-Agenturen oder IT-Systeme.
45. Auch das Ziel, einen erheblichen Teil der (derzeitigen und künftigen) Zusammenarbeit zwischen der EU und Interpol in einem einzigen Rechtsinstrument zu untermauern, macht das geplante Abkommen sehr heterogen, da es ein breites Spektrum von Tätigkeiten umfasst. Der EDSB betont daher, dass eine eingehende Folgenabschätzung erforderlich ist und dass der Ansatz nicht zu einer Schwächung der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihrer Rechte auf Datenschutz und Privatsphäre führen sollte.
46. In Ermangelung eines Angemessenheitsbeschlusses in Bezug auf Interpol könnte das geplante Abkommen eine Rechtsgrundlage für die Übermittlung personenbezogener Daten an Interpol sein, sofern es rechtsverbindlich und gegenüber allen Vertragsparteien des Abkommens durchsetzbar wäre und angemessene Datenschutzgarantien enthalten würde.
47. Nach Auffassung des EDSB sollte die Einführung geeigneter Garantien implizieren, dass das mit Interpol geschlossene internationale Abkommen
- gewährleistet, dass es Schutzvorkehrungen im geltenden EU-Recht in Bezug auf die Übermittlung durch die betreffenden Agenturen und Einrichtungen der EU und die Weiterübermittlung personenbezogener Daten, einschließlich der besonderen Bestimmungen über die Übermittlung operativer Daten durch Europol und die EUSStA gibt. Insbesondere sollte im Zusammenhang mit Weiterübermittlungen ausdrücklich festgelegt werden, dass von der EU an Interpol übermittelte personenbezogene Daten nicht dazu verwendet werden dürfen, eine Todesstrafe oder eine Form grausamer und unmenschlicher Behandlung zu beantragen, zu verhängen oder zu vollstrecken;
  - ausdrücklich klarstellt, dass Interpol keinen direkten oder indirekten Zugang zu den EU-Datenbanken haben wird;
  - angibt, wann und unter welchen Umständen automatisierte Einzelentscheidungen zulässig sind (oder nicht);
  - weitere Einzelheiten zur Meldepflicht von Interpol im Falle einer Verletzung des Schutzes personenbezogener Daten enthält;
  - weitere operative Einzelheiten zu technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit personenbezogener Daten angibt.
48. Ferner empfiehlt der EDSB, im Mandat die Möglichkeit festzulegen, das Abkommen auszusetzen oder zu kündigen, wenn eine der Parteien gegen seine Bestimmungen über personenbezogene Daten verstößt, und dass personenbezogene Daten, die in den Geltungsbereich des Abkommens fallen und vor seiner Aussetzung oder Kündigung übermittelt wurden, weiterhin im Einklang mit dem Abkommen verarbeitet werden dürfen.

49. Der EDSB empfiehlt, dass die Bezugsvermerke und Erwägungsgründe des Beschlusses des Rates nicht nur auf die angemessene verfahrensrechtliche Grundlage, sondern auch auf die einschlägige materiellrechtliche Grundlage verweisen, darunter Artikel 16 AEUV.

Brüssel, den 25. Mai 2021

Wojciech Rafał WIEWIÓROWSKI

*[elektronisch unterzeichnet]*

## Endnoten

---

<sup>1</sup> ABl. L 119 vom 4.5.2016, S. 1.

<sup>2</sup> ABl. L 119 vom 4.5.2016, S. 89.

<sup>3</sup> ABl. L 295 vom 21.11.2018, S. 39.

<sup>4</sup> Gründung der IKPO-Interpol [I/CONS/GA/1956 (2017)].

<sup>5</sup> Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „EU-Strategie für eine Sicherheitsunion“, Brüssel, 24.7.2020, COM(2020)605 final.

<sup>6</sup> COM(2021)177 final.

<sup>7</sup> Seite 8.

<sup>8</sup> Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI, ABl. L 135 vom 24.5.2016, S. 53 („Europol-Verordnung“). Der Begründung zufolge besteht bereits ein Kooperationsabkommen mit Interpol, das den Austausch personenbezogener Daten vorsieht und 2001, also lange vor der Europol-Verordnung, geschlossen wurde. Durch dieses hat Europol jedoch keinen direkten oder indirekten Zugang zu Informationen und den Datenbanken von Interpol, insbesondere nicht zu den Ausschreibungen, die Informationen über Terroristen enthalten. Darüber hinaus tauscht die Agentur nur über den Verbindungsbeamten von Interpol bei Europol oder ihren Verbindungsbeamten bei Interpol Informationen mit Interpol aus oder greift zur Erfüllung ihrer Aufgaben auf die Datenbanken von Interpol zu. Das Abkommen wurde später durch mehrere auf die Zusammenarbeit bezogene Dokumente ergänzt, die zwischen den Organisationen vereinbart oder abgeschlossen wurden, z. B. über die Zusammenarbeit durch Verbindungsbeamte und indem eine sichere Kommunikationsleitung für den Informationsaustausch eingerichtet. In Gang gesetzt und betrieben wurde.

<sup>9</sup> Nach der Annahme der Verordnungen über die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa, also der 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) und der Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816, (ABl. L 135 vom 22.5.2019, S. 85).

<sup>10</sup> Frontex bezeichnet die Europäische Agentur für die Grenz- und Küstenwache. Verordnung (EU) 2019/1896 des Europäischen Parlaments und des Rates vom 13. November 2019 über die Europäische Grenz- und Küstenwache und zur Aufhebung der Verordnungen (EU) Nr. 1052/2013 und (EU) 2016/1 (ABl. L 295 vom 14.11.2019, S. 1) („Frontex-Verordnung“).

<sup>11</sup> Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) (ABl. L 218 vom 13.8.2008, S. 60); Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 767/2008, der Verordnung (EG) Nr. 810/2009, der Verordnung (EU) 2017/2226, der Verordnung (EU) 2016/399, der Verordnung XX/2018 [Interoperabilitäts-Verordnung] und des Beschlusses 2004/512/EG sowie zur Aufhebung des Beschlusses 2008/633/JI des Rates (COM/2018/302 final) und siehe politische Einigung: <https://data.consilium.europa.eu/doc/document/ST-5537-2021-INIT/en/pdf>

<sup>12</sup> Verordnung (EU) 2017/1939 des Rates vom 12. Oktober 2017 zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft („EUStA“) (ABl. L 283 vom 31.10.2017, S. 1).

<sup>13</sup> Gemäß Artikel 54 der Frontex-Verordnung muss sich die ständige Reserve der Europäischen Grenz- und Küstenwache aus vier Kategorien von Personal zusammensetzen. Kategorie 1 umfasst Statutpersonal, das gemäß Artikel 55 dieser Verordnung als Teammitglieder in Einsatzbereiche entsandt wird. Die Agentur trägt zu der ständigen Reserve mit Mitgliedern ihres Statutpersonals (Kategorie 1) bei, die als Teammitglieder mit den Aufgaben und Befugnissen gemäß Artikel 82 dieser Verordnung in Einsatzbereiche entsandt werden. Zu ihren Aufgaben gehört die Bekämpfung von grenzüberschreitender Kriminalität und Terrorismus.

<sup>14</sup> Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates vom 14. November 2018 betreffend die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) und zur Ersetzung und Aufhebung des Beschlusses 2002/187/JI des Rates (ABl. L 295 vom 21.11.2018, S. 138) („Eurojust-Verordnung“).

<sup>15</sup> Derzeit beteiligen sich 22 Mitgliedstaaten an der Verstärkten Zusammenarbeit zur Errichtung der EUStA.

<sup>16</sup> Siehe beispielsweise im Zusammenhang mit den Vorschlägen der Kommission für Änderungen an den Rechtsinstrumenten der EU-Informationssysteme nach der Annahme der Verordnung (EU) 2018/1240 zur Einrichtung

---

eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) die vom Europäischen Parlament im LIBE-Ausschuss in Auftrag gegebene gezielte substituierende Folgenabschätzung:

[https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS\\_STU\(2019\)642808](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)642808).

<sup>17</sup> Vgl. Toolkit des EDSB zur Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken, abrufbar unter: [https://edps.europa.eu/sites/edp/files/publication/17-06-01\\_necessity\\_toolkit\\_final\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf)

Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken, abrufbar unter: [https://edps.europa.eu/sites/edp/files/publication/19-12-19\\_edps\\_proportionality\\_guidelines2\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf)

<sup>18</sup> Siehe hierzu Gutachten 1/15 des Gerichtshofs der Europäischen Union („EuGH“) (Große Kammer) vom 26. Juli 2017, PNR-Abkommen EU-Kanada, ECLI:EU:C:2017:592, Rn. 77 und 78: „77 Ergibt die Prüfung eines Unionsrechtsakts, dass er zwei Zielsetzungen hat oder aus zwei Komponenten besteht, und lässt sich eine von ihnen als die überwiegende ausmachen, während die andere nur nebensächliche Bedeutung hat, so ist der Rechtsakt nur auf eine Rechtsgrundlage zu stützen, und zwar auf die, die die hauptsächliche oder überwiegende Zielsetzung oder Komponente erfordert. Verfolgt eine Maßnahme dagegen mehrere Zielsetzungen zugleich oder besteht sie aus mehreren Komponenten, die untrennbar miteinander verbunden sind, ohne dass die eine gegenüber der anderen nebensächlich ist, so dass verschiedene Vertragsbestimmungen anwendbar sind, ist sie ausnahmsweise auf die entsprechenden verschiedenen Rechtsgrundlagen zu stützen (Urteil vom 14. Juni 2016, Parlament/Rat, C-263/14, EU:C:2016:435, Rn. 44 und die dort angeführte Rechtsprechung).

<sup>78</sup> Der Rückgriff auf eine doppelte Rechtsgrundlage ist jedoch ausgeschlossen, wenn die für die beiden Rechtsgrundlagen jeweils vorgesehenen Verfahren nicht miteinander vereinbaren lassen (Urteil vom 6. November 2008, Parlament/Rat, C-155/07, EU:C:2008:605, Rn. 37 und die dort angeführte Rechtsprechung).“

<sup>19</sup> Siehe Studie im Auftrag des Europäischen Parlaments, DROI-Ausschuss, „Misuse of Interpol’s Red Notices and impact on human rights - recent developments“, Januar 2019, abrufbar unter:

[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603472/EXPO\\_STU\(2019\)603472\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603472/EXPO_STU(2019)603472_EN.pdf)

<sup>20</sup> Siehe EuGH, Gutachten 1/15 vom 26. Juli 2017, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592.

<sup>21</sup> Hervorhebung hinzugefügt. Siehe Erwägungsgrund 7 der Empfehlung.

<sup>22</sup> Punkte 3 und 6 des Anhangs der Empfehlung.

<sup>23</sup> z. B. als Ergebnis der substituierenden Grundrechtsfolgenabschätzung, siehe Endnote 16.

<sup>24</sup> 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).

<sup>25</sup> Seite 5.

<sup>26</sup> Sie sind abrufbar unter: [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en)

<sup>27</sup> Siehe Artikel 2 der Verordnung (EU) 2018/1725.

<sup>28</sup> Erwägungsgrund 29 der Eurojust-Verordnung.

<sup>29</sup> Zum Datenschutz: Richtlinie (EU) 2016/680 im Falle des Austauschs personenbezogener Daten durch die zuständigen Behörden der Mitgliedstaaten mit Interpol zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten; Verordnung (EU) 2016/679 im Falle des Austauschs personenbezogener Daten durch andere Behörden der Mitgliedstaaten mit Interpol; Verordnung (EU) 2018/1725 im Falle des Austauschs personenbezogener Daten durch Organe, Einrichtungen und sonstige Stellen der EU mit Interpol, insbesondere Kapitel IX, Artikel 94 im Falle der Übermittlung operativer personenbezogener Daten an Interpol durch Einrichtungen und sonstige Stellen der Union, die Tätigkeiten durchführen, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 oder 5 AEUV (Justizielle Zusammenarbeit in Strafsachen oder polizeiliche Zusammenarbeit) fallen, sowie spezifische Datenschutzbestimmungen, die in gesonderten Rechtsakten wie der Europol- oder der EUStA-Verordnung enthalten sind.

<sup>30</sup> Siehe beispielsweise Artikel 31 der Verordnung (EG) Nr. 767/2008 vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt, ABl. L 218 vom 13.8.2008, S. 60.

<sup>31</sup> Artikel 29 Absätze 1 und 2 der Europol-Verordnung „Bewertung der Zuverlässigkeit der Quelle und Richtigkeit der Informationen“  
lauten:

„1. Die Zuverlässigkeit der Quelle der von einem Mitgliedstaat stammenden Informationen wird nach Möglichkeit von dem Mitgliedstaat, der die Informationen liefert, anhand folgender Quellenbewertungskodes bewertet:

(A): Es bestehen keine Zweifel an der Authentizität, Verlässlichkeit und Eignung der Quelle oder die Informationen stammen von einer Quelle, die sich in allen Fällen als verlässlich erwiesen hat;

(B): es handelt sich um eine Quelle, deren Informationen sich in den meisten Fällen als verlässlich erwiesen haben;

(C): es handelt sich um eine Quelle, deren Informationen sich in den meisten Fällen als nicht verlässlich erwiesen haben;

(X): die Verlässlichkeit der Quelle kann nicht beurteilt werden.

2. Die Richtigkeit der von einem Mitgliedstaat stammenden Informationen wird nach Möglichkeit von dem Mitgliedstaat, der die Informationen liefert, anhand folgender Informationsbewertungskodes bewertet:

(1): Informationen, an deren Wahrheitsgehalt kein Zweifel besteht;

- 
- (2): Informationen, die der Quelle, nicht aber dem Beamten, der sie weitergibt, persönlich bekannt sind;  
(3): Informationen, die der Quelle nicht persönlich bekannt sind, die aber durch andere bereits erfasste Informationen erhärtet werden;  
(4): Informationen, die der Quelle nicht persönlich bekannt sind und die sich auf keine andere Weise erhärten lassen.“

<sup>32</sup> Siehe Erwägungsgrund 71 der Richtlinie (EU) 2016/680 in Bezug auf Kriterien, die bei der Bewertung des Vorhandenseins geeigneter Garantien in einem Strafverfolgungskontext zu berücksichtigen sind, wenn kein Angemessenheitsbeschluss vorliegt.

<sup>33</sup> Siehe Abschnitt 3, S. 9 der Empfehlung.

<sup>34</sup> Siehe EuGH-Rechtssache C-687/15, Europäische Kommission gegen Rat der Europäischen Union, ECLI:EU:C:2017:803, Rn. 48 ff.

<sup>35</sup> Gutachten 1/15 vom 26. Juli 2017, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 232.