



**Stellungnahme zu der vom Datenschutzbeauftragten von Frontex empfangenen  
Meldung zur Vorabkontrolle im Hinblick auf die Verarbeitung personenbezogener  
Daten im Rahmen einer Risikoanalyse (Processing of Personal Data for Risk Analysis,  
PeDRA)**

Brüssel, 03. Juli 2015 (Fall 2015-0346)

**1. Verfahren**

Am 15. April 2015 ging beim Europäischen Datenschutzbeauftragten (EDSB) eine Meldung des Datenschutzbeauftragten (DSB) der Europäischen Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union (Frontex) zur Vorabkontrolle im Hinblick auf die Verarbeitung personenbezogener Daten im Rahmen einer Risikoanalyse (PeDRA) ein.

Am 07. und 11. Mai 2015 wurden Fragen übermittelt, die Frontex am 14. Mai 2015 beantwortete. Der Entwurf der Stellungnahme wurde dem DSB am 22. Juni 2015 mit der Bitte um Anmerkungen übermittelt. Eine Antwort ging beim EDSB am 02. Juli 2015 ein.

**2. Sachverhalt**

Das PeDRA-Projekt dient zur Umsetzung von Artikel 11c der geänderten Fassung der Verordnung (EG) Nr. 2007/2004 des Rates<sup>1</sup> („die Frontex-Verordnung“).

Frontex erhält von den Mitgliedstaaten bestimmte Informationen über Personen, die der Beihilfe zur illegalen Einwanderung, Aktivitäten in Bezug auf den Menschenhandel oder anderer grenzüberschreitender krimineller Handlungen verdächtigt werden. Anschließend werden diese Daten für zwei Zwecke verwendet (nachstehend ausführlicher erläutert):

- Risikoanalysen, deren Ergebnisse anonymisiert werden;
- Erstellung von „personenbezogenen Datenpaketen“ (Personal Data Packages, PDPs) zur Übermittlung an Europol.

Betroffene Personen sind Personen, die von den zuständigen Behörden der Mitgliedstaaten der Beihilfe zur illegalen Einwanderung, Aktivitäten in Bezug auf den Menschenhandel oder anderer grenzüberschreitender krimineller Handlungen verdächtigt werden. Opfer von Menschenhandel und geschleuste Migranten werden ausdrücklich aus der Gruppe der betroffenen Personen ausgeschlossen. Diese Informationen werden vorerst in Form von beschreibenden Interview-Berichten zur Verfügung gestellt, die in Zusammenhang mit den von Frontex koordinierten Operationen gesammelt wurden (weitere Datenquellen werden im

---

<sup>1</sup> ABl. L 349/01, 25/11/2004

Laufe des Prozesses hinzugefügt)<sup>2</sup>. Eine nicht erschöpfende Liste von Datenkategorien, die in diese Berichte aufgenommen werden können, wurde wie folgt zur Verfügung gestellt:

- Name(n) der Person, Spitzname
- Geschlecht
- Nationalität/Nationalitäten
- Namen bekannter Komplizen
- Gruppe für organisiertes Verbrechen
- Eingetragene Geschäftsadresse
- Persönliche Adresse
- Adresse der konspirativen Wohnung
- Kommunikationsmittel (Telefonnummer, Deckname in sozialen Netzwerken...)
- Transportmittel (Fahrzeugregistrierung, Bootsname...)
- Waffe
- Foto(s)
- Nicht-Straftat<sup>3</sup>
- Straftat
- Ethnische Herkunft<sup>4</sup>
- Sexuelle Ausrichtung<sup>5</sup>

Für die zukünftige Entwicklung von PeDRA ist vorgesehen, besser strukturierte Formate für die Bereitstellung von Informationen zur Verfügung zu stellen.

Als erste Informationsquelle für diese Berichte werden Befragungen von Migranten herangezogen, die an der Außengrenze der Union aufgegriffen werden. Diese Befragungen werden von den zuständigen Behörden der Mitgliedstaaten durchgeführt. Diese Informationen werden anschließend auf Initiative des übermittelnden Mitgliedstaats über einen sicheren Benachrichtigungskanal an Frontex übermittelt (nachstehend weitere Informationen zu Sicherheitsvorkehrungen).

Die Ermittlungsbeamten der Mitgliedstaaten (die Kontaktstellen, die die Berichte an PeDRA übermitteln; eine pro Mitgliedstaat und gemeinsamer Aktion) erhalten Schulungen zur Handhabung des Tools, um eine Verwendung entsprechend der Rechtsgrundlage sicherzustellen. Fälle, bei denen sich Berichte als nicht rechtmäßig herausstellen, werden für den übermittelnden Mitgliedstaat und den einzelnen Ermittlungsbeamten zum Zwecke der Rückmeldung erfasst (Kontaktstellen). Außerdem plant Frontex den Aufbau eines „Ermittlungsbeamtennetzwerks“, um die Verbreitung bewährter Verfahren zu erleichtern.

Nach dem Eingang bei Frontex wird die Nachricht von einem leitenden PeDRA-Analysten authentifiziert und hinsichtlich ihrer Rechtmäßigkeit überprüft, um festzustellen, ob sie die Kriterien zur Weiterleitung an Frontex gemäß Artikel 11c Absatz 2 der Frontex-Verordnung erfüllt. Nachrichten, die als nicht rechtmäßig erachtet werden, werden vorübergehend gespeichert, bis die Rechtmäßigkeit bestätigt wurde. Frontex kann den übermittelnden Mitgliedstaat um weitere Informationen bitten. Nachrichten, die endgültig als nicht rechtmäßig erachtet werden, werden gelöscht, und der übermittelnde Mitgliedstaat wird

---

<sup>2</sup> Gemeinsame Aktionen, Pilotprojekte, Soforteinsätze

<sup>3</sup> Laut Frontex bezieht sich dieser Begriff auf Vorfälle, die an sich keine Verbrechen im Sinne von PeDRA darstellen, aber in Verbindung zu solchen Verbrechen stehen z. B. Bewegungen zwischen den konspirativen Wohnungen.

<sup>4</sup> Laut Frontex sind diese Informationen notwendig, um Verbindungen zwischen Schleusern/Menschenhändlern aufzudecken, da diese zumeist Personen der eigenen ethnischen Gruppe schleusen bzw. Menschenhandel mit Personen der eigenen ethnischen Gruppe betreiben („soziale Homophilie“).

<sup>5</sup> Laut Frontex werden Migranten in der Regel von Schleusern/Menschenhändlern sexuell missbraucht.

entsprechend unterrichtet. Berichte, die sich offensichtlich nicht im Rahmen des Mandats befinden, werden ohne Bitten um auf Klarstellung zurückgewiesen.

Akzeptierte Nachrichten können für einen oder beide der oben genannten Zwecke verwendet werden. Diese werden im Folgenden näher erläutert:

a) Risikoanalysen

Personenbezogene Daten, die über den Benachrichtigungskanal übermittelt wurden, werden von Frontex für Risikoanalysen herangezogen. Die Ergebnisse der Risikoanalysen enthalten keine personenbezogenen Daten.

b) Erstellung von „personenbezogenen Datenpaketen“ (PDPs) zur Übermittlung an Europol.

Frontex sammelt die von den Mitgliedstaaten übermittelten personenbezogenen Daten in thematischen Ordnern, die nach Kriterien wie Ort, Straftat oder Gruppe der organisierten Kriminalität unterteilt sind. Diese Sammlungen können durch Kontextdokumente wie beispielsweise bestehende Frontex-Risikoanalysen oder andere Informationen (z. B. Karten, Statistiken) und Erläuterungen ergänzt werden. Die genauen Kriterien, nach denen entschieden wird, wann und wie PDPs entnommen und an Europol übermittelt werden, scheinen für die unterschiedlichen Teile der Begleitunterlagen etwas voneinander abzuweichen:

Der Business Case für die Weiterleitung an Europol besagt, dass „gemäß der Frontex-Verordnung von Fall zu Fall entschieden wird, ob eine Weiterleitung an Europol durchgeführt wird, das heißt, dass dies nicht systematisch oder automatisch erfolgt, sondern aufgrund einer Entscheidung, die im Einklang mit den Datenschutzprinzipien der Verhältnismäßigkeit und der Erforderlichkeit steht.“

Laut PeDRA-Business Case wird ein PDP entnommen und an Europol verschickt, wenn der betreffende Ordner eine ausreichende Anzahl an Dokumenten enthält oder wenn die ältesten personenbezogenen Daten im Ordner 90 Tage zuvor von Frontex erhalten wurden.

In ihrer Antwort auf eine Bitte um Klarstellung erklärte Frontex, dass es ihr Ziel sei, die PDPs innerhalb von 48 Stunden an Europol weiterzuleiten. Es wird davon ausgegangen, dass alle eingegangenen Berichte an Europol weitergeleitet werden.

Die PDPs werden sowohl die von den Mitgliedstaaten übermittelten Daten als auch Informations- und Hintergrundmaterial, das von Frontex zur Verfügung gestellt wurde, enthalten.

Personenbezogene Daten werden nach Abschluss der Kontrolle der Rechtmäßigkeit 90 Tage bei Frontex gespeichert.<sup>6</sup> Nach diesem Zeitraum werden die Informationen im aktiven System geschwärzt.<sup>7</sup> Personenbezogene Daten werden jedoch auch in einem inaktiven verschlüsselten

---

<sup>6</sup> Frontex rechtfertigte diesen Startzeitpunkt (anstelle des Zeitpunkts der Validierung der Nachricht) mit dem Argument, dass es etwas dauern könnte, bis die Mitgliedstaaten auf Fragen zur Klarstellung bei der Kontrolle der Rechtmäßigkeit antworten. Dies würde die Zeitspanne, in der die Daten zur Analyse verfügbar wären, in unzulässigem Maße verkürzen. Frontex merkte zudem an, dass es bei erhöhtem Flüchtlingszustrom zu noch größeren Verzögerungen beim Beantworten kommen könnte, d. h. zu dem Zeitpunkt, an dem der Erhalt umfangreicherer PeDRA-relevanter Informationen wahrscheinlich ist.

<sup>7</sup> Entfernen von Verweisen auf konkrete Personen, Adressen, Telefonnummern etc., während Informationen über Vorkommnisse aufbewahrt werden. Dies soll weitestgehend automatisch vonstatten gehen; Freitextdokumente, die personenbezogene Daten enthalten, werden mit einem Datum zur Schwärzung versehen und manuell geschwärzt.

Archiv aufbewahrt. Die Speicherzeit für dieses Archiv soll drei Jahre betragen.<sup>8</sup> In der Meldung wurden „historische Zwecke und Prüfungszwecke“ als Grund für dieses Archiv angegeben. Später stellte Frontex klar, dass mit Hilfe dieses Archivs Details in möglichen anschließenden Gerichtsverfahren geklärt und Anträge von betroffenen Personen beantwortet werden sollen. Der Zugang zu diesem Archiv wird beschränkt.

Übermittlungen an Drittstaaten oder internationale Organisationen sind nicht vorgesehen. Außer Europol soll derzeit kein anderer Dritter personenbezogene Daten von PeDRA erhalten. Die Risikoanalysen dürfen weiter verbreitet werden, enthalten jedoch keine personenbezogenen Daten.

Frontex plant nicht, betroffenen Personen Informationen zur Verarbeitung proaktiv zukommen zu lassen.

Hinsichtlich Zugangsrechten, Berichtigungen, Sperrungen, Löschungen und Widersprüchen gab Frontex bekannt, dass die Anträge von Fall zu Fall beurteilt würden und dass Einschränkungen gemäß Artikel 20 der Verordnung gelten können.

[...]

Wie bekannt gegeben, bezieht sich PeDRA auf die gesamte Umsetzung von Artikel 11c, deren erster operativer Bestandteil ein Pilotprojekt ist, mit dem die Verfahren geprüft werden sollen. Auf das Pilotprojekt soll die schrittweise Einführung bei allen gemeinsamen Aktionen folgen.

### **3. Rechtliche Prüfung**

#### **3.1. Vorabkontrolle**

Artikel 27 Absatz 2 der Verordnung legt eine Reihe von Voraussetzungen fest, unter denen Verarbeitungen vom EDSB vorab kontrolliert werden.

Unter Buchstabe a dieses Artikels wird die Verarbeitung bestimmter Kategorien sensibler Daten genannt, einschließlich Daten über (mutmaßliche) Straftaten als Grund für eine Vorabkontrolle. Wie in der Meldung angegeben und als logische Folge ihres Zwecks, werden im Rahmen von PeDRA personenbezogene Daten über (mutmaßliche) Straftaten verarbeitet, weshalb Vorabkontrollen durchgeführt werden müssen.

Gemäß Artikel 27 Absatz 4 der Verordnung gibt der EDSB seine Stellungnahme innerhalb von zwei Monaten ab. Diese Frist kann ausgesetzt werden, bis weitere Auskünfte vorliegen. Der Fall wurde am 15. April 2015 bekannt gegeben und vom 07. bis zum 14. Mai 2015 ausgesetzt. Vom 22. Juni bis zum 02. Juli 2015 wurde er ausgesetzt, um eine Äußerung zum Entwurf dieser Stellungnahme zu ermöglichen. Folglich muss der EDSB seine Stellungnahme bis zum 6. Juli 2015 abgeben.

#### **3.2. Rechtmäßigkeit der Verarbeitung**

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dafür rechtliche Gründe nach Artikel 5 der Verordnung vorliegen.

In Buchstabe a wird ausgeführt, dass die „Verarbeitung erforderlich ist für die Wahrnehmung einer Aufgabe, die aufgrund der Verträge zur Gründung der Europäischen Gemeinschaften

---

<sup>8</sup> Es besteht die Möglichkeit einer weiteren Verlängerung in Abhängigkeit von der Schwere des Verbrechens. Frontex will diese Zeiträume den Zeiträumen von Europol anpassen (d. h. dem einzigen Empfänger dieser Daten).

oder anderer aufgrund dieser Verträge erlassener Rechtsakte im öffentlichen Interesse ausgeführt wird.“ Dies bedeutet, dass (1) für diese Aufgaben eine Grundlage im Unionsrecht gefunden werden muss und dass (2) die beabsichtigte Verarbeitung für die Wahrnehmung dieser Aufgaben erforderlich sein muss.

Artikel 11c der Frontex-Verordnung lautet wie folgt (Hervorhebungen hinzugefügt):

„1. Unbeschadet der Zuständigkeit der Mitgliedstaaten für die Erfassung personenbezogener Daten im Rahmen von gemeinsamen Aktionen, Pilotprojekten und Soforteinsätzen und vorbehaltlich der in den Absätzen 2 und 3 genannten Einschränkungen kann **die Agentur personenbezogene Daten weiterverarbeiten, die von den Mitgliedstaaten im Rahmen solcher operativer Maßnahmen erfasst und der Agentur übermittelt wurden, um zur Sicherheit der Außengrenzen der Mitgliedstaaten beizutragen.**

2. **Diese Weiterverarbeitung** personenbezogener Daten durch die Agentur **ist auf personenbezogene Daten von Personen beschränkt, die von den zuständigen Behörden der Mitgliedstaaten hinreichend begründet** der Beteiligung an grenzüberschreitenden kriminellen Handlungen, der Beihilfe zur illegalen Einwanderung oder Aktivitäten in Bezug auf den Menschenhandel gemäß Artikel 1 Absatz 1 Buchstaben a und b der Richtlinie 2002/90/EG des Rates vom 28. November 2002 zur Definition der Beihilfe zur unerlaubten Ein- und Durchreise und zum unerlaubten Aufenthalt verdächtigt werden.

3. Die in Absatz 2 genannten personenbezogenen Daten werden durch die Agentur **ausschließlich für folgende Zwecke weiterverarbeitet:**

- (a) die **Weiterleitung von Fall zu Fall** an Europol oder andere Strafverfolgungsbehörden der Union **gemäß Artikel 13;**
- (b) die Verwendung für die **Erstellung von in Artikel 4 genannten Risikoanalysen.** Im **Ergebnis** der Risikoanalysen werden die Daten **anonymisiert.**

4. Die personenbezogenen Daten **werden gelöscht, sobald sie an Europol oder andere Agenturen der Union übermittelt oder für die Erstellung von in Artikel 4 genannten Risikoanalysen verwendet wurden. Die Speicherzeit darf keinesfalls länger sein als drei Monate** nach der Erhebung dieser Daten.

5. Bei der Verarbeitung solcher personenbezogener Daten sind die Prinzipien der Erforderlichkeit und der Verhältnismäßigkeit einzuhalten. Die personenbezogenen Daten **werden von der Agentur nicht** zum Zweck von **Ermittlungen** verwendet; diese unterliegen weiterhin der Verantwortung der zuständigen Behörden der Mitgliedstaaten.

Insbesondere **ist die Verarbeitung auf diejenigen personenbezogenen Daten beschränkt, die für die in Absatz 3 genannten Zwecke erforderlich sind.**

6. Unbeschadet der Verordnung (EG) Nr. 1049/2001 ist die **Weiterleitung** oder anderweitige Mitteilung der personenbezogenen Daten, die von der Agentur verarbeitet wurden, **an Drittländer oder andere Dritte verboten.**

7. Dieser Artikel wird im Einklang mit den in Artikel 11a genannten Maßnahmen angewendet.“

**Bezüglich Paragraph 1** bestätigte Frontex, dass ausschließlich Daten, die von Mitgliedstaaten im Rahmen gemeinsamer Aktionen, Pilotprojekte und Soforteinsätze erhoben werden, an die Agentur übermittelt werden. Daten, die während routinemäßiger Grenzkontrollaktivitäten erhoben werden, sind hiervon ausgenommen.

**Bezüglich Paragraph 2** bestätigte Frontex, dass sich die Verarbeitung personenbezogener Daten auf Personen beschränkt, die des Schleusens/Menschenhandels oder anderer grenzüberschreitender krimineller Handlungen verdächtigt werden. Personenbezogene Daten z. B. über Asylbewerber seien nicht rechtmäßig und würden daher nicht für die Zwecke von PeDRA weiterverarbeitet.

**Nach Paragraph 3 Buchstabe a** über die Weiterleitung an Europol sind Übermittlungen von „Fall zu Fall“ zulässig. Frontex erklärte, dass die erhaltenen personenbezogenen Daten an Europol weitergeleitet und die erhaltenen Berichte innerhalb von 48 Stunden übermittelt werden sollten.

Bezüglich der Weiterleitung personenbezogener Daten an Europol ist auch Artikel 13 zweiter Unterabsatz der Frontex-Verordnung, der in Artikel 11c Absatz 3 genannt wird, von Bedeutung:

„Die **Weiterleitung** oder andere Übermittlung personenbezogener Daten, die von der Agentur verarbeitet werden, an andere Agenturen oder Einrichtungen der Union **unterliegen gesonderten Arbeitsvereinbarungen** betreffend den Austausch von personenbezogenen Daten und der **vorherigen Zustimmung** des Europäischen Datenschutzbeauftragten.“

Bisher hat Frontex lediglich mit Europol eine solche Vereinbarung ausgehandelt und getroffen. Aus diesem Grund wird Europol die einzige Agentur der Europäischen Union sein, die personenbezogene Daten von PeDRA erhält. Vor der Unterzeichnung wurde der Text der Vereinbarung dem EDSB vorgelegt. Der EDSB hatte keine Einwände gegen die Vereinbarung zu erheben und erteilte vorläufig seine Zustimmung, sofern bestimmte Bedingungen erfüllt sind.<sup>9</sup>

Während hinsichtlich der formalen Aspekte dieser Übermittlung (d. h. hinsichtlich der Vereinbarung mit Europol) keine weiteren Erläuterungen nötig sind, sollte das „Fall zu Fall“-Element in Artikel 11c Absatz 3 Buchstabe a nochmals geprüft werden:

Diese Element impliziert, dass Daten nicht grundsätzlich an Europol weitergeleitet werden sollten, sondern erst nach menschlichem Eingreifen und Bewertung. Solche Übermittlungen sollten nur dann stattfinden, wenn gemäß den Informationen, die Frontex vorliegen, aus der Verbindung der einzelnen erhaltenen Berichte und den zusätzlichen Hintergrundinformationen, die von Frontex zur Verfügung gestellt werden, ein Mehrwert geschaffen wird.

Wie bereits in Abschnitt 2 oben erwähnt, scheinen die Erläuterungen von Frontex in den unterschiedlichen Teilen der Begleitunterlagen gelegentlich etwas voneinander abzuweichen.

Die aus dem Business Case zitierte Beschreibung für die Weiterleitung an Europol („die Weiterleitung an Europol wird von Fall zu Fall entschieden, das heißt, dass dies nicht systematisch oder automatisch erfolgt, sondern aufgrund einer Entscheidung, die im Einklang mit den Datenschutzprinzipien der Verhältnismäßigkeit und der Erforderlichkeit steht“) scheint der „Fall zu Fall“-Anforderung zu entsprechen. Wenn alle erhaltenen Berichte kurz vor Ende der Speicherzeit weitergeleitet werden (wie im PeDRA-Business Case erläutert), wäre dieses Kriterium nicht erfüllt. Das erklärte Ziel von Frontex (in ihrer Antwort vom 14. Mai 2015), die Informationen innerhalb von 48 Stunden an Europol weiterzuleiten, lässt ebenfalls Zweifel daran aufkommen, ob eine wirkliche Fall-zu-Fall-Bewertung durchgeführt wird. Im Einklang mit Artikel 11c ihrer Verordnung **sollte Frontex personenbezogene Daten nur dann an Europol weiterleiten, wenn dies von Fall zu Fall den Prinzipien der**

---

<sup>9</sup> EDSB Fall 2015-0129

**Erforderlichkeit und der Verhältnismäßigkeit entspricht.**<sup>10</sup> Das Weiterleiten aller Informationen entspräche nicht dem Fall zu Fall-Prinzip. **Frontex sollte eine Vorgehensweise zur Bewertung der Erforderlichkeit und der Verhältnismäßigkeit von Übermittlungen an Europol definieren und die anderen relevanten Dokumente entsprechend aktualisieren.** Diese Empfehlungen gelten dementsprechend für alle möglichen zukünftigen Übermittlungen an „andere Strafverfolgungsbehörden der Union.“

Artikel 11c Absatz 3 Buchstabe b bezieht sich auf Risikoanalysen gemäß Artikel 4 der Frontex-Verordnung, der wie folgt lautet:

„Die Agentur entwickelt ein gemeinsames integriertes Risikoanalysemodell und wendet es an.

Sie **erstellt sowohl allgemeine als auch spezifische Risikoanalysen**, die dem Rat und der Kommission übermittelt werden.

[...]

Für die Zwecke dieses Artikels **versorgen die Mitgliedstaaten die Agentur mit allen erforderlichen Informationen** zur Lage und zu potenziellen Bedrohungen an den Außengrenzen. [...]"

Wie bereits erwähnt, enthalten die Ergebnisse dieser Risikoanalysen keine personenbezogenen Daten.

Während Artikel 11c Absatz 4 der Frontex-Verordnung auf die Löschung von Daten „sobald diese übermittelt [...] oder für die Erstellung von Risikoanalysen verwendet wurden“ verweist, erklärte Frontex, dass nicht gelten sollte, dass sich diese zwei Zwecke nicht gegenseitig ausschließen, d. h., entweder für die Übermittlung an Europol *oder* für die Verwendung bei Risikoanalysen. Begründet wurde dies damit, dass eine solche entweder/oder-Verwendung den Nutzen des Systems erheblich verringern würde. Der EDSB stimmt dieser Meinung zu und stellt ferner fest, dass sich Frontex im Falle einer derartigen entweder/oder-Verwendung entscheiden müsse, welche Verwendung von größerem Nutzen sei. Dies würde wiederum eine ausführlichere Analyse erfordern, die Ermittlungsaktivitäten gleichkommen könnte, die jedoch gemäß Artikel 11c Absatz 5 der Frontex-Verordnung ausdrücklich vom Tätigkeitsbereich von PeDRA ausgenommen sind. Ein einzelner Bericht, der von einem MS vorgelegt wird, kann daher sowohl für die Weiterleitung an Europol als auch für die Erstellung von Risikoanalysen verwendet werden. Weitere Überlegungen zur Datenaufbewahrung folgen in Abschnitt 3.5 unten.

Schlussendlich fällt die geplante Verarbeitung personenbezogener Daten im Rahmen von PeDRA wie beschrieben unter Artikel 5a der Verordnung, vorbehaltlich der Empfehlungen, die in dieser Stellungnahme enthalten sind, insbesondere der Empfehlungen zu Übermittlungen von „Fall zu Fall.“

### **3.3. Verarbeitung besonderer Datenkategorien**

Artikel 10 der Verordnung enthält spezielle Regeln für bestimmte Kategorien sensibler Daten. Laut Frontex können Daten über (mutmaßlichen) Straftaten, ethnische Herkunft sowie sexuelle Ausrichtung im Rahmen von PeDRA verarbeitet werden und fallen unter Artikel 10.

Die Verarbeitung von Daten, aus denen die ethnische Herkunft oder sexuelle Ausrichtung hervorgehen, ist nur in den Fällen erlaubt, die unter Artikel 10 Absatz 2 der Verordnung aufgeführt sind.

---

<sup>10</sup> Siehe auch Abschnitt 3.6 unten für Sicherheitsvorkehrungen hinsichtlich der Übermittlung als solche.

Artikel 10 Absatz 2 beschreibt eine Reihe von Situationen, in denen derartige besondere Kategorien verarbeitet werden dürfen. Keiner der genannten Fälle scheint PeDRA zu betreffen. Gemäß Artikel 10 Absatz 4 kann der Unionsgesetzgeber weitere Ausnahmen festlegen.<sup>11</sup>

Gemäß Artikel 11c Absatz 1 der Frontex-Verordnung „kann die Agentur personenbezogene Daten weiterverarbeiten, die von den Mitgliedstaaten im Rahmen solcher operativer Maßnahmen erfasst und der Agentur übermittelt wurden.“

Somit ist Frontex zur Weiterverarbeitung von personenbezogenen Daten ermächtigt, die von einem Mitgliedstaat im Rahmen von PeDRA übermittelt wurden.<sup>12</sup> Diese personenbezogenen Daten mussten vom übermittelnden Mitgliedstaat rechtmäßig nach den geltenden nationalen Rechtsvorschriften erhoben werden. Hierzu zählen vermutlich Sicherheitsvorkehrungen zur Verarbeitung solcher besonderer Daten.

Bei Fällen, in denen die Mitgliedstaaten solche besonderen Daten rechtmäßig erhoben haben, könnte somit aufgrund dieser Regelung die Weiterverarbeitung ohne Erlaubnis von Frontex fortgeführt werden, vorausgesetzt, es ist für angemessene Maßnahmen zur Bekämpfung von Diskriminierung aufgrund von ethnischer Herkunft gesorgt.<sup>13</sup>

Für eine erhöhte Rechtssicherheit wäre eine entsprechende **Änderung der Frontex-Verordnung im Einklang mit den Vorschriften des Artikels 10 Absatz 4 der Verordnung die beste Lösung**, um eine eindeutige Rechtsgrundlage für die Verarbeitung solcher Daten zu schaffen. Bis dahin kann Artikel 11 c Absatz 1 der Frontex-Verordnung als Rechtsgrundlage für die Verarbeitung dieser besonderen Datenkategorie erachtet werden, **sofern angemessene Maßnahmen zur Bekämpfung von Diskriminierung getroffen wurden**.

Hinsichtlich Daten über die „**sexuelle Ausrichtung**“ erklärte Frontex, dass Migranten während des Migrationsprozesses häufig von Schleusern/Menschenhändlern sexuell missbraucht würden und dass aus diesem Grund derartige Informationen über Schleuser/Menschenhändler von Europol für die weiteren Ermittlungen benötigt werden könnten. Der EDSB erachtet Informationen über derartige Missbrauchsfälle tatsächlich als Informationen über eine (mutmaßliche) Straftat und nicht über die sexuelle Ausrichtung des (mutmaßlichen) Täters. Aus diesem Grund sollten sie gemäß Artikel 10 Absatz 5 der Verordnung beurteilt werden und nicht gemäß Artikel 10 Absatz 2.

Im Rahmen von PeDRA erscheint eine Verarbeitung personenbezogener Daten über die sexuelle Ausrichtung nicht nötig. Aus diesem Grund **sollte Frontex im Rahmen von PeDRA keine personenbezogenen Daten über die sexuelle Ausrichtung verarbeiten**, wobei zu berücksichtigen ist, dass Informationen zu sexuellem Missbrauch von Migranten durch Schleuser/Menschenhändler als Daten in Zusammenhang mit einer Straftat erachtet werden und nicht als Daten in Zusammenhang mit der sexuellen Ausrichtung.

Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßnahmen betreffen, darf gemäß Artikel 10 Absatz 5 der Verordnung nur erfolgen, wenn sie durch die Verträge oder andere auf der Grundlage dieser Verträge erlassene Rechtsakte genehmigt wurde.

---

<sup>11</sup> Derselbe Artikel erlaubt es auch dem EDSB, derartige weitere Ausnahmen „falls notwendig“ festzulegen. Dies ist als Übergangsmaßnahme für Situationen zu betrachten, in denen der Unionsgesetzgeber noch keine derartige Ausnahme nach Inkrafttreten der Verordnung festgelegt hat. Die Erteilung solcher Genehmigungen fällt nicht mehr in den Zuständigkeitsbereich des EDSB; siehe EDSB Fall 2013-0717

<sup>12</sup> In Abschnitt 3.2 werden weitere Einzelheiten und die zulässigen Zwecke beschrieben.

<sup>13</sup> In diesem Zusammenhang muss außerdem erwähnt werden, dass Europol, als vorgesehener Empfänger der personenbezogenen Daten von PeDRA, ebenfalls strengen Regeln zur Verarbeitung personenbezogener Daten hinsichtlich ethnischer Herkunft unterworfen ist, siehe Artikel 10 Absatz 3, Artikel 14 Absatz 1 und Artikel 16 Absatz 1 des Beschlusses 2009/917/JHA des Rates.



Artikel 11c Absatz 3 der Frontex-Verordnung, der in Abschnitt 3.2 oben zitiert wurde, erteilt eine solche Genehmigung. Diese besondere Kategorie personenbezogener Daten kann deshalb im Rahmen von PeDRA für die Zwecke und unter den Voraussetzungen, die in diesem Artikel aufgeführt werden, verarbeitet werden.

### **3.4. Qualität der Daten**

Gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung müssen personenbezogene Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen. Dieses Prinzip wird in Artikel 11c Absatz 5 der Frontex-Verordnung, der auf die Prinzipien der Erforderlichkeit und der Verhältnismäßigkeit verweist, noch einmal bestätigt. Gemäß Artikel 4 Absatz 1 Buchstabe d der Verordnung muss deren Richtigkeit gewährleistet sein.

Laut Frontex bezieht sich der Begriff „Nicht-Straftaten“ auf Vorfälle, die an sich keine Verstöße gegen örtliches Recht darstellen, z. B. Informationen zum Transport innerhalb eines Drittstaates, die jedoch in Verbindung mit grenzüberschreitenden Verbrechen stehen, die im Rahmen von PeDRA verfolgt werden, einschließlich solcher Informationen, die dafür erheblich erscheinen und nicht darüber hinausgehen.

Laut Frontex liegt die Zuständigkeit für die Erhebung und Bereitstellung von Daten, einschließlich deren Richtigkeit, bei den Mitgliedstaaten. Unabhängig davon erhalten die Ermittlungsbeamten der Mitgliedstaaten (die Kontaktstellen) Schulungen zur Handhabung des Upload-Tools. Fälle, bei denen sich die Berichte als nicht rechtmäßig herausstellen, werden für die übermittelnden Mitgliedstaaten und den einzelnen übermittelnden Ermittlungsbeamten zum Zwecke der Rückmeldung erfasst. Außerdem ist der Aufbau eines „Ermittlungsbeamtennetzwerkes“ vorgesehen, um die Verbreitung bewährter Verfahren zu erleichtern. Sowohl innerhalb des Netzwerks als auch während der Schulungen sollten Datenschutzaspekte, insbesondere die Notwendigkeit der Richtigkeit, angesprochen werden. Diese Maßnahmen sollten zur Sicherstellung angemessener Datenqualität innerhalb des Systems beitragen. **Frontex sollte eine angemessene Kontrolle der Datenqualität gewährleisten und allen aufgedeckten Mängeln nachgehen.** Dies könnte beispielsweise in Form einer regelmäßigen internen Berichterstattung über Daten erfolgen, die von den Mitgliedstaaten an Frontex übermittelt werden (z. B. Zahlen und Prozentwerte zu Übermittlungen, die als rechtmäßig/nicht rechtmäßig erachtet wurden). Berichte, die von Europol an Frontex übermittelt werden sollen (z. B. Zahlen und Prozentwerte zu PDPs, die die Mandatsprüfung bei Europol bestanden/nicht bestanden haben), können ebenfalls zur Bewältigung dieser Aufgabe beitragen.

Im Prinzip scheint die in dieser Meldung genannte Anzahl an Datenkategorien nicht übermäßig zu sein (vorbehaltlich der Anmerkungen in Abschnitt 3.3 oben). Diese Liste wurde als nicht erschöpfend bezeichnet, insbesondere da die Berichte zumindest vorerst als beschreibende Freitextdokumente zur Verfügung gestellt werden. Zur Sicherstellung der Datenqualität sollte gewährleistet sein, dass ausschließlich personenbezogene Daten, die den Zwecken entsprechen, die erheblich sind und die nicht über das erforderliche Maß hinausgehen, verwendet werden. Daher besteht die Notwendigkeit, für angemessene Schulungsmaßnahmen für das Personal zu sorgen, das die ersten Berichte zur Verfügung stellt. Es sollte jedoch berücksichtigt werden, dass es sich hierbei um Beamte der Mitgliedstaaten handelt. Bei Frontex sollte die Kontrolle der Rechtmäßigkeit ebenfalls zur Sicherstellung der Datenqualität beitragen.

Zur Sicherstellung der Datenqualität sowie zur besseren Überwachung scheint der geplante Schritt in Richtung eines besser strukturierten Formats ein wichtiges Vorhaben zu sein. In Zukunft sollten Vorlagen und Ähnliches stets im Einklang mit dem Grundsatz der Datenqualität erstellt werden.

### **3.5. Datenaufbewahrung**

Gemäß Artikel 4 Absatz 1 Buchstabe e der Verordnung dürfen personenbezogene Daten nur so lange, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, gespeichert werden.

Nach Artikel 11c Absatz 4 der Frontex-Verordnung darf die Speicherzeit „keinesfalls länger sein als drei Monate nach Erhebung dieser Daten.“

Für Frontex beginnt die Speicherzeit ab dem Zeitpunkt, zu dem die Daten als rechtmäßig erachtet wurden.

Für den EDSB bezieht sich der Begriff „Erhebung“ in diesem Artikel auf die Erhebung *durch Frontex*, d. h. auf den Zeitpunkt, zu dem ein Mitgliedstaat personenbezogene Daten an Frontex übermittelt und die Nachricht die Authentifizierungskontrolle bestanden hat. Es geht weder um die ersten von den zuständigen Behörden der Mitgliedstaaten vorgenommenen Befragungsaufzeichnungen, noch geht es darum, ob die Nachricht als rechtmäßig erachtet wurde.

Laut Frontex benötigen die Mitgliedstaaten in der Tat eine gewisse Zeit, um auf Bitten um Klarstellung zu antworten. Hierbei handle es sich jedoch um ein Problem, das der betroffenen Mitgliedstaat selbst lösen müsse.

**Daher empfiehlt der EDSB, dass die 90-tägige Aufbewahrungszeit ab dem Zeitpunkt der Authentifizierung der erhaltenen Nachricht beginnt.**

Am Ende dieses Zeitraums wird Frontex bestimmte Teile der verarbeiteten Informationen löschen, um diese zu anonymisieren. Identifikatoren wie Namen, Telefonnummern etc. werden entfernt, die verbleibenden anonymisierten Informationen werden jedoch aufbewahrt.

Der EDSB betont, dass die bloße Entfernung offensichtlicher Identifikatoren nicht ausreichen könnte, um die Daten zu anonymisieren.<sup>14</sup> **Frontex sollte sicherstellen, dass die Daten durch Schwärzung vollständig anonymisiert werden.** Für den Fall, dass die betroffenen Personen indirekt identifizierbar bleiben, sind diese Informationen weiterhin als personenbezogene Daten zu erachten. Für den Fall, dass Frontex eine unumkehrbare Anonymisierung nicht gewährleisten kann, sollten der Einfachheit halber alle betroffenen Informationen gelöscht werden.

Nach derzeitiger Planung beabsichtigt Frontex außerdem, alle Daten, die im Rahmen von PeDRA verarbeitet wurden, für einen Zeitraum von drei Jahren in einem Archiv aufzubewahren. Frontex wählte diesen Zeitraum, um sich den Aufbewahrungszeiten von Europol anzupassen. Während anfänglich „historische Zwecke und Prüfungszwecke“ als Grund für das Archiv angegeben wurden, stellte Frontex später klar, dass das Archiv zwei andere Zwecke erfüllen soll. Zum einen soll auf die Anträge von betroffenen Personen geantwortet werden können (z. B. auf Zugang), zum anderen sollen Informationen für mögliche anschließende Gerichtsverfahren zur Verfügung gestellt werden können.

Die angegebenen Verwendungszwecke für das Archiv scheinen in der Tat keinen historischen Charakter zu haben. In jedem Fall unterliegt die Weiterverarbeitung für historische Zwecke bestimmten Sicherheitsvorkehrungen, um insbesondere sicherzustellen, dass die Daten nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen Betroffenen verwendet werden (siehe Artikel 4 Absatz 1 Buchstabe b der Verordnung).

---

<sup>14</sup> Siehe auch Artikel 29 der Stellungnahme der Datenschutzgruppe zum Begriff „personenbezogene Daten“ unter: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_de.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf)

Hinsichtlich möglicher Anträge von betroffenen Personen (z. B. auf Zugang), ist darauf hinzuweisen, dass personenbezogene Daten generell, sobald der Zweck, für den sie erhoben wurden, erreicht wurde, gelöscht werden sollten, schlicht, um auf Zugangsanträge von betroffenen Personen antworten zu können. Das Zugangsrecht impliziert das Recht, auf bestehende Daten zuzugreifen, und sollte nicht als Grund dienen, Daten weiterhin aufzubewahren.

Hinsichtlich **Gerichtsverfahren** ist darauf hinzuweisen, dass die ursprünglichen Daten, die von den Mitgliedstaaten zur Verfügung gestellt wurden, als Teil der PDPs an Europol weitergeleitet werden. Aus diesem Grund erscheint es wahrscheinlicher, dass Bitten um Klarstellung in späteren Gerichtsverfahren an Europol oder den betreffenden Mitgliedstaat gerichtet werden. Angesichts dieser Tatsache ist nicht ersichtlich, aus welchem Grund Frontex ebenfalls über dieses Archiv verfügen sollte, um auf Bitten um Klarstellung antworten zu können. Um beweisen zu können, dass ein bestimmtes PDP an Europol gesendet wurde, muss es nicht erforderlich sein, über eine vollständig Sammlung aller personenbezogenen Daten zu verfügen.

**Überprüfungen** werden nicht zum Zweck der Rechtshilfe in Gerichtsverfahren durchgeführt und sollten deutlich unterschieden werden. Für Prüfungszwecke erscheint die Dauer der Aufbewahrungszeit übermäßig. Außerdem ist nicht unmittelbar erkennbar, dass alle Daten notwendig wären.<sup>15</sup> Frontex müsste zeigen, wie lange bestimmte Informationen für Prüfungszwecke notwendig wären.

In beiden Fällen ist die Eingrenzung des Verwendungszwecks der Schlüssel: Auf die Daten kann nur dann zugegriffen werden, wenn sie für einen oder beide Zwecke erforderlich sind.

In jedem Fall **sollte Frontex die Notwendigkeit des Archivs näher erläutern, insbesondere angesichts der in Artikel 11c Absatz 4 der Frontex-Verordnung festgelegten, eindeutigen Aufbewahrungszeit.**

### **3.6. Datenübermittlung**

Ein Hauptzweck von PeDRA ist die Erstellung von PDPs zur Weiterleitung an Europol. Frontex bestätigte, dass darüber hinaus keine Übermittlungen an andere Dritte vorgesehen seien.

Da Europol nicht der Verordnung unterliegt, fallen Übermittlungen an Europol unter Artikel 9 der Verordnung.<sup>16</sup> Es sei darauf hingewiesen, dass die Voraussetzungen dieses Artikels kumulativ für andere Voraussetzungen dieser Verordnung sind - eine Übermittlung muss *sowohl* nach Artikel 5 rechtmäßig sein *als auch* die Sicherheitsvorkehrungen in Artikel 9 erfüllen.

Der Artikel bietet mehrere Möglichkeiten, solche Übermittlungen zu legitimieren. Gemäß Artikel 9 Absatz 1 finden solche Übermittlungen nur dann statt, „wenn ein angemessenes Schutzniveau in dem Land des Empfängers gewährleistet ist“ und „die Daten ausschließlich die Wahrnehmung von Aufgaben ermöglichen sollen, die in die Zuständigkeit des für die Verarbeitung Verantwortlichen fallen.“

---

<sup>15</sup> Wenn es beispielsweise darum ginge zu zeigen, dass zu einem bestimmten Zeitpunkt ein bestimmtes PDP an Europol übermittelt wurde, muss es nicht erforderlich sein, den Inhalt des PDP für diesen Zweck aufzubewahren. Das Aufbewahren eines Hashwerts könnte ausreichen.

<sup>16</sup> Obwohl Europol eine Agentur der Europäischen Union ist, unterliegt sie nicht der Verordnung, sondern einer eigenen Sonderregelung. Der EDSB versteht Artikel 9 in dem Sinne, dass dieser Übermittlungen an Empfänger abdeckt, die weder der Verordnung noch den nationalen Umsetzungen der Richtlinie 95/46/EG unterworfen sind. Siehe Seite 24 des EDSB-Positionspapiers zur Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch EU-Organe und -Einrichtungen (Positionspapier), erhältlich auf der EDSB-Website.. [

Die Angemessenheit ist „anhand aller Umstände einer Datenübermittlung oder einer Reihe von Datenübermittlungen zu beurteilen. Besonders zu berücksichtigen sind dabei die Art der Daten, der Zweck und die Dauer des geplanten Verarbeitungsvorgangs oder der geplanten Verarbeitungsvorgänge, das Drittland oder die internationale Organisation der Endbestimmung, die in dem betreffenden Drittland oder der betreffenden internationalen Organisation geltenden allgemeinen und sektoriellen Rechtsvorschriften sowie die in diesem Land oder in dieser internationalen Organisation geltenden Landesregeln und Sicherheitsmaßnahmen.“ Weitere Leitlinien zur Beurteilung der Angemessenheit werden vom EDSB<sup>17</sup> sowie in Artikel 29 der Stellungnahme der Datenschutzgruppe zur Verfügung gestellt.<sup>18</sup>

Frontex hat für Europol eine Angemessenheitsbeurteilung durchgeführt und dokumentiert und ist zu dem Schluss gekommen, dass angemessener Schutz geboten wird.

Für das zweite Kriterium bietet Artikel 11c Absatz 3 Buchstabe a der Frontex-Verordnung eine eindeutige Rechtsgrundlage für Übermittlungen an Europol. Daher fallen sie prinzipiell in den Zuständigkeitsbereich von Frontex (d. h. in den Zuständigkeitsbereich des für die Verarbeitung Verantwortlichen).

Nichtsdestotrotz ist zu beurteilen, ob die Übermittlungen von Fall zu Fall stattfinden, wie in Artikel 11c Absatz 3 Buchstabe a der Frontex-Verordnung gefordert, und in Abschnitt 3.2 oben dargelegt.

### **3.7. Informationspflicht gegenüber der betroffenen Person**

In Artikel 12 der Verordnung werden die Informationspflichten des für die Verarbeitung Verantwortlichen dargelegt, wenn die Daten, wie im Fall von PeDRA, nicht bei der betroffenen Person erhoben wurden. Gemäß Artikel 12 Absatz 2 muss der für die Verarbeitung Verantwortliche unter bestimmten Bedingungen einzelne Informationen nicht zur Verfügung stellen, insbesondere wenn dies einen unverhältnismäßigen Aufwand erfordert, unmöglich ist, oder die Speicherung oder Weitergabe durch Rechtsvorschriften der Union ausdrücklich vorgesehen ist. In solchen Fällen stellt der für die Verarbeitung Verantwortliche nach Absprache mit dem EDSB angemessene Sicherheitsvorkehrungen zur Verfügung.

Frontex erklärte, dass sie selbst keine direkten Informationen an betroffene Personen herausgäbe, dass das Anstellen von Ermittlungen nicht in ihren Aufgabenbereich falle und dass sie nicht in direktem Kontakt mit den betroffenen Personen stünde (vermutlich haben nicht einmal die zuständigen nationalen Behörden direkten Kontakt). An dieser Stelle ist es wichtig, nochmals darauf hinzuweisen, dass es sich bei den im Rahmen von PeDRA zu verarbeitenden personenbezogenen Daten um Daten von mutmaßlichen Schleusern/Menschenhändlern oder anderen Personen handelt, die grenzüberschreitender krimineller Handlungen verdächtigt werden, und nicht um Daten von Migranten.

Es mag durchaus sein, dass es Frontex unmöglich ist, den betroffenen Personen die einzelnen Informationen zukommen zu lassen oder dass dies einen unverhältnismäßigen Aufwand erfordert. So ist es beispielsweise möglich, dass keine Kontaktinformationen erhältlich sind. Da Ermittlungen ausdrücklich nicht in den Aufgabenbereich von Frontex fallen, sollte nicht

---

<sup>17</sup> Positionspapier, auf das in der vorangegangenen Fußnote verwiesen wurde, Seiten 10-13.

<sup>18</sup> Artikel 29 der Stellungnahme der Datenschutzgruppe umfasst die Datenschutzbehörden der EU-Mitgliedstaaten, den EDSB und die EG. Darin wurden Artikel 25 und 26 der Richtlinie 95/46/EG ausgelegt, die entsprechende Bestimmungen für die Verarbeitung in den Mitgliedstaaten enthalten. Siehe Arbeitsdokument: Übermittlungen personenbezogener Daten an Drittländer: Nach Artikel 25 und 26 der EU-Datenschutzrichtlinie, erhältlich unter [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf)

nach zusätzlichen Informationen, wie z. B. Kontaktinformationen über betroffene Personen, gesucht werden.

In den Fällen, in denen Frontex in der Lage wäre, direkte Informationen an betroffene Personen herauszugeben, ist zudem darauf hinzuweisen, dass die betroffenen Personen in PeDRA einem Strafverfahren durch die zuständigen Behörden der Mitgliedstaaten unterliegen könnten und die Informationen ihnen Hinweise zu den Ermittlungen der Mitgliedstaaten geben könnten. Für diese Fälle könnte eine Einschränkung im Sinne von Artikel 20 Absatz 1 Buchstabe a gerechtfertigt sein.

Um für ein Mindestmaß an Transparenz zu sorgen, **sollte Frontex allerdings auf ihrer Website eine Datenschutzerklärung abgeben, die die Bestandteile des Artikels 12 der Verordnung abdeckt.**

### **3.8. Auskunftsrecht und Berichtigung**

Gemäß Artikel 13 und 14 der Verordnung haben die betroffenen Personen das Recht, auf ihre Daten zuzugreifen und diese berichtigen zu lassen.

Frontex erklärte, dass Auskunfts- oder Berichtigungsanfragen nach ihrer Standardmethode bearbeitet würden, dass jedoch Ausnahmen nach Artikel 20 angewandt werden könnten.

Eine Einschränkung der Rechte der betroffenen Person ist nur von Fall zu Fall zu beschließen und nicht als generelles Prinzip anzuwenden. Für den Fall, dass sich Frontex solcher Einschränkungen bedient, **sollte dies intern dokumentiert werden, einschließlich der Gründe für die Einschränkung.**

### **3.9. Sicherheitsmaßnahmen**

[...]

## **4. Schlussfolgerung:**

Es gibt keinen Grund zu der Annahme, dass die Bestimmungen der Verordnung (EG) Nr. 45/2001 missachtet werden, vorausgesetzt, die Empfehlungen, die in der vorliegenden Stellungnahme enthalten sind, werden in vollem Umfang berücksichtigt. Zur Erinnerung: Frontex sollte (im Rahmen von PeDRA):

1. nur dann personenbezogene Daten an Europol übermitteln<sup>19</sup> wenn dies von Fall zu Fall notwendig und verhältnismäßig ist;
2. eine Vorgehensweise zur Bewertung der Erforderlichkeit und der Verhältnismäßigkeit von Übermittlungen an Europol definieren und alle anderen relevanten Dokumente entsprechend aktualisieren;
3. Bis zu einer Änderung der Frontex-Verordnung im Einklang mit den Vorschriften des Artikels 10 Absatz 4 der Verordnung zur Bereitstellung, um einer eindeutigen Rechtsgrundlage für die Verarbeitung von Daten über die ethnische Herkunft und für angemessene Sicherheitsmaßnahmen gegen die Verwendung von Daten über die ethnische Herkunft zur Diskriminierung sorgen;
4. keine personenbezogenen Daten über die sexuelle Ausrichtung verarbeiten;
5. eine angemessene Kontrolle der Datenqualität gewährleisten und allen aufgedeckten Mängeln nachgehen;

---

<sup>19</sup> Oder andere Strafverfolgungsbehörden der EU gemäß Artikel 11c Absatz 3 Buchstabe a

6. die 90-tägige Aufbewahrungszeit zu dem Zeitpunkt beginnen lassen, zu dem die eingegangene Nachricht authentifiziert wurde;
7. sicherstellen, dass die Daten durch die Schwärzung vollständig anonymisiert wurden;
8. die Notwendigkeit des Archivs näher erläutern, insbesondere angesichts der in Artikel 11c Absatz 4 der Frontex-Verordnung festgelegten, eindeutigen Aufbewahrungszeit;
9. auf ihrer Website eine Datenschutzerklärung abgeben, die die Bestandteile des Artikels 12 der Verordnung abdeckt;
10. intern alle Fälle dokumentieren, bei denen eine Einschränkung im Sinne des Artikels 20 der Verordnung vorgenommen wird, einschließlich der Gründe für die Einschränkung.
11. [...]

Frontex sollte innerhalb von drei Monaten nach dem Datum dieser Stellungnahme über diese Empfehlungen berichten.

Geschehen zu Brüssel am Freitag, den 3. Juli 2015

**(unterzeichnet)**

Wojciech Rafał WIEWIÓROWSKI