From:	[redacted]
To:	[redacted]
CC:	European Data Protection Supervisor <EDPS@edps.europa.eu>; HoRAU <HoRAU@frontex.europa.eu>; [redacted]; dpo <dpo@frontex.europa.eu>; [redacted]
Sent at:	02/07/15 11:38:08
Subject:	RE: [2015-0346] draft prior check opinion on PeDRA for your comments // comments requested by 2 July

Dear [redacted]

Thank you for your good habit to pre-consult with us the draft wording of the EDPS future prior-checking opinion.
Please see attached the draft opinion on PeDRA with some small proposals of enrichments/corrections by the relevant internal actors in our Agency.

Best regards

[redacted]

FRONTEX
www.frontex.europa.eu
Plac Europejski 6, 00-844 Warsaw, Poland · Tel: +48 22 205 9500 · Fax: +48 22 205 9501

From: [redacted]
Sent: 22 June 2015 17:37
To: [redacted]; dpo
Cc: European Data Protection Supervisor; HoRAU;[redacted]
Subject: [2015-0346] draft prior check opinion on PeDRA for your comments // comments requested by 2 July

Dear colleagues,

Please find enclosed the draft opinion on PeDRA for your comments by 2 July 2015 (10 days). According to Article 27(4) of Regulation 45/2001, the two months period in which the EDPS must give his opinion is suspended.

Please note that your comments should focus only on practical aspects and factual inaccuracies in the attached draft and not serve as an occasion to provide feedback on the actual implementation relating to the substance of our recommendations. If no feedback is received within 10 days, the EDPS will proceed with the adoption of the opinion.

We remind you that the EDPS policy is to publish prior-checking Opinions. The section on Security will however be removed before publication. Should you have any legitimate reasons for which all or part of the opinion should not be published, please inform us

accordingly. This is without prejudice to the application of Regulation EC 1049/2001.

Please answer this e-mail with the EDPS functional mailbox in cc. (edps@edps.europa.eu) as the date of the receipt of your answer to the EDPS mailbox will be the only date taken into account to lift the suspension of the deadline within which the EDPS must render his opinion. Please make a reference in the subject of your message to the case file number 2015-0346

Best regards,

[redacted]

[redacted]
Legal Officer
Supervision & Enforcement
[redacted]
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
@EU_EDPS www.edps.europa.eu

Opinion on a notification for Prior Checking received from the Data Protection Officer of Frontex regarding the Processing of Personal Data for Risk Analysis (PeDRA)

Brussels, date (2015-0346)

1. Proceedings

On 15 April 2015 the European Data Protection Supervisor (EDPS) received a notification for prior checking relating to the Processing of Personal Data for Risk Analysis (PeDRA) from the Data Protection Officer (DPO) of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex).

Questions were raised on 07 and 11 May 2015, to which Frontex replied on 14 May 2015. The draft Opinion was sent to the DPO for comments on 22 June 2015. The EDPS received a reply on XX XX 2015.

2. The Facts

The PeDRA project serves to implement Article 11c of Council Regulation (EC) 2007/2004[1] ("the Frontex Regulation"), as amended.

Frontex will receive certain information on persons suspected of being involved in facilitation of illegal immigration, human trafficking, or other cross-border criminal activities from Member States. It will then use these data for two purposes (further explained below):

- Risk analyses, the results of which will be depersonalised;
- Preparation of "personal data packages" (PDPs) for onward transfer to Europol.

Data subjects are persons suspected by the competent authorities of Member States of being involved in facilitation of illegal immigration, human trafficking, or other cross-border criminal activities. Victims of human trafficking and smuggled migrants are explicitly excluded from being data subjects. This information will initially be provided in the form of narrative interview reports collected in the context of Frontex-coordinated operations[2] but other data sources will be added as processes mature. A non-exhaustive list of data categories that may be included in these reports was provided as follows:

- Name(s) of subject, nickname
- Gender
- Nationality/ies
- Names of known accomplices
- Organised crime group
- Registered business
- Personal address
- Safe house address

[1] OJ L 349/01, 25/11/2004

[2] Joint operations, pilot projects, rapid interventions

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel: +32 2-283 19 00 - Fax: +32 2-283 19 50

- Means of communications (telephone number, social media handles...)
- Means of transportation (vehicle registration, boat name...)
- Weapon
- Photograph(s)
- Non-offence event[3]
- Offence event
- Ethnicity[4]
- Sexual orientation[5]

For the future development of PeDRA, a move to more structured formats of providing the information is foreseen.

The initial source of these reports will be debriefings of migrants intercepted at the external border of the Union. These debriefings are conducted by the competent Member State authorities. This information will then be forwarded to Frontex through a secure messaging channel on the initiative of the transmitting Member State (further information on security measures below).

Member States' Intelligence Officers (the contact points who submit reports to PeDRA; one per Member State and joint operation) will receive training on how to use the tool in order to make sure that it is used in accordance with its legal basis; instances of reports that fail the legality check will be recorded to give feedback to the submitting Member States and the individual submitting Intelligence Officers (contact points). Additionally, Frontex plans to establish an "intelligence officers network" in order to facilitate dissemination of best practices.

Upon arrival at Frontex, the message will be authenticated and will go through a legality check conducted by a senior PeDRA analyst to check if it meets the criteria for transmission to Frontex defined in Article 11c(2) of the Frontex Regulation. Messages that fail the legality check will be temporarily stored until legality is confirmed; Frontex may ask the submitting Member State for further information. Messages that finally fail the legality check will be deleted and the submitting Member State informed. Reports that are obviously out of the mandate will be refused without requests for clarification.

Accepted messages may be used for one or both of purposes mentioned above and explained in greater detail below:

a) Risk analyses
   Personal data transmitted using the channel is used for risk analyses by Frontex. In the results of these risk analyses, no personal data will be included.

b) Preparation of "personal data packages" (PDPs) for onward transfer to Europol
   Frontex will collate personal data received from the Member States in thematic folders, grouped by criteria such as location, crime or organised crime group. These collections may be enriched with context documents such as already existing Frontex risk analyses or other information (e.g. maps, statistics) and explanatory text. The precise criteria when and how PDPs are extracted and transferred to Europol appear to differ slightly between different parts of the supporting documentation:

   The business case for transmission to Europol states that "[a]ccording to the Frontex regulation transmissions to Europol will take place on a case by case basis which is to

[3] Frontex explained that this refers to events that are not in and of themselves crimes as referred to in the scope for PeDRA, but linked to such crimes, e.g. movements between safe houses.
[4] Frontex explained that this information would be necessary in order to uncover connections between traffickers/smugglers, as they sometimes mostly smuggle/traffic persons of their own ethnic group ("homophily").
[5] Frontex explained that migrants are routinely sexually abused by smugglers/traffickers.

say, not systematically or automatically but following a decision in line with data protection principles of proportionally and necessity".

According to the PeDRA business case, a PDP is extracted and sent to Europol either when there is a useful quantity of items in such a folder, or when the oldest personal data in there was received by Frontex 90 days prior.

In its reply to a request for clarification, Frontex stated that its aim was to forward PDPs to Europol within 48 hours; it expects to forward all reports received to Europol.

PDPs will contain both the data as submitted by the Member States and explanatory and background material provided by Frontex.

Personal data will be kept for 90 days following the conclusion of the legality check at Frontex.[6] After this period, the information in the active system will be sanitised.[7] Personal data will, however, also be kept in an inert encrypted archive. The conservation period for this archive is planned to be three years.[8] The notification mentioned "historical and audit purposes" as the reason for this archive; Frontex later clarified that the purpose of this archive was to be able to clarify details during possible subsequent judicial proceedings and to be able to reply to requests from data subjects. Access to this archive will be limited.

No transfers to third countries or international organisations are foreseen. Europol is the only third party that is currently intended to receive personal data from PeDRA; the risk analyses may be distributed more widely, but will not contain personal data.

Frontex does not plan to proactively provide information about the processing to data subjects.

Concerning the rights of access, rectification, blocking, erasure and objection, Frontex stated that it would assess requests on a case-by-case basis, noting that restrictions under Article 20 of the Regulation may apply.

Frontex provided a description of the security measures to be used for PeDRA, which can be summarised as follows:

According to Frontex, the non-functional requirements, security requirements and Annex 1 of the Business Requirements Document (BRD) were compiled based on the PeDRA business case. Analysis of the requirements was made at that stage, in consultation with the Frontex technical stakeholders i.e. RAU, ICT and FSC. During the analysis, business processes were identified and documented in the BRD together with the business rules and use cases. Frontex foresees a subsequent phase of PeDRA where a detailed analysis will be performed aiming to mitigate the threats and vulnerabilities to the system. Furthermore, in the completed notification form, Frontex has described control objectives and high-level security controls that will be implemented for this system. Frontex stated that it would neither use contractors nor allow teleworking for PeDRA: everything will be done in-house.

PeDRA as notified refers to the whole implementation of Article 11c, the first operational component of which is a Pilot Exercise designed to test procedures. The Pilot Exercise is planned to be followed by a gradual rollout to all joint operations.

[6] Frontex justified this starting point (as opposed to message validation as starting point) with the argument that Member States may take a certain amount of time to reply to questions for clarification in the legality check, which would unduly reduce the time the data would be available for analysis. Frontex also noted that the problem of delays for replying would appear to be bigger in cases of increased influx of migrants, i.e. at the very same moment that more PeDRA-relevant information is likely to be received.

[7] Removing references to specific persons, addresses, telephone numbers etc., while keeping information about events. This is planned to happen automatically as far as possible; free-text documents that contain personal data will be tagged with a data for sanitisation and be sanitised manually.

[8] With a possibility for further extension depending on the severity of the crime; Frontex plans to align these periods with those applied by Europol (i.e. the only recipient of these data).

3. Legal Analysis

3.1. Prior Checking

Article 27(2) of the Regulation lists a number of conditions under which processing operations are subject to prior checking by the EDPS.

Point (a) of this Article mentions the processing of certain sensitive categories of data, including data on (suspected) offences as grounds for prior checking. As indicated in the notification and obvious from its purpose, PeDRA will process personal data related to (suspected) offences and is thus subject to prior checking.

According to Article 27(4) of the Regulation, the EDPS shall render his Opinion within a period of two months, not counting suspensions for further information. The case has been notified on 15 April 2015 and has been suspended from 07 to 14 May 2015. From 22 June to XX 2015, it has been suspended for comments on the draft Opinion. The EDPS thus has to render his Opinion by XX XX 2015.

3.2. Lawfulness of the Processing

Personal data may only be processed if grounds can be found in Article 5 of the Regulation.

Point (a) mentions processing "necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof". This means that (1) these tasks need find a basis in Union law and (2) the processing envisaged must be necessary for fulfilling these tasks.

Article 11c of the Frontex Regulation reads as follows (emphases added):

> "1. Without prejudice to the competence of Member States to collect personal data in the context of joint operations, pilot projects and rapid interventions, and subject to the limitations set out in paragraphs 2 and 3, **the Agency may further process personal data collected by the Member States during such operational activities and transmitted to the Agency in order to contribute to the security of the external borders of the Member States.**
>
> 2. **Such further processing** of personal data by the Agency **shall be limited to personal data regarding persons who are suspected, on reasonable grounds, by the competent authorities of the Member States** of involvement in cross-border criminal activities, in facilitating illegal migration activities or in human trafficking activities as defined in points (a) and (b) of Article 1(1) of Council Directive 2002/90/EC of 28 November 2002 defining the facilitation of unauthorised entry, transit and residence.
>
> 3. Personal data referred to in paragraph 2 shall be further processed by the Agency **only for the following purposes**:
>
> > (a) the **transmission**, on a **case-by-case basis**, to Europol or other Union law enforcement agencies, **subject to Article 13**;
> >
> > (b) the use for the **preparation of risk analyses** referred to in **Article 4**. In the **result** of the risk-analyses, data shall be **depersonalised**.
>
> 4. The personal data **shall be deleted as soon as they have been transmitted** to Europol or other Union agencies **or used for the preparation of risk analyses** referred to in Article 4. The term of **storage shall in any event not exceed three months** after the date of the collection of those data.
>
> 5. The processing of such personal data shall respect the principles of necessity and proportionality. The personal data **shall not be used by the Agency for** the

purpose of **investigations**, which remain under the responsibility of the competent authorities of the Member States.

In particular, it **shall be strictly limited to those personal data which are required for the purposes referred to in paragraph 3**.

6. Without prejudice to Regulation (EC) No 1049/2001, **onward transmission** or other communication of such personal data processed by the Agency **to third countries or other third parties shall be prohibited**.

7. This Article shall be applied in accordance with the measures referred to in Article 11a."

Concerning paragraph 1, Frontex confirmed that only data collected by Member States in the context of joint operations, pilot projects and rapid interventions would be transferred to the Agency; data collected during other routine border control activities would be excluded.

As regards paragraph 2, Frontex confirmed that only personal data related to suspects of smuggling /trafficking in human being or of other cross-border criminal activities /cross-border criminalswould be processed and that personal data e.g. about asylum seekers would fail the legality check and thus not be further processed for the purposes of PeDRA.

Paragraph 3 point a) about transmission to Europol authorises transfers on "case-by-case basis". Frontex explained that it did not expect to withhold personal data submitted to it from further transfer to Europol and that it would aim to transfer reports received within 48 hours.

Concerning the transmission of personal data to Europol, Article 13, second subparagraph of the Frontex Regulation, referred to in Article 11c(3) is relevant as well:

"Onward **transmission** or other communication of personal data processed by the Agency **to other Union agencies** or bodies shall be **subject to specific working arrangements** regarding the exchange of personal data and subject to the **prior approval** of the European Data Protection Supervisor."

Frontex has so far only negotiated and agreed such an arrangement with Europol, which; will probably be therefore the only Union Agency allowed to receive personal data from PeDRA. The text of the arrangement has been provided to the EDPS prior to signature. The EDPS found no objections to the arrangement and provided prior approval subject to some conditions.[9]

While the formal aspects of this transfer (i.e. the arrangement with Europol) do not require further explanation, the element of "on a case-by-case basis" in Article 11c(3)(a) merits further exploration:

This element means that data should not be pushed on to Europol as a matter of general policy, but only after human intervention and evaluation. Such transfers should only take place if, based on the information available to Frontex, there is an added value from the connections made between the different reports received and the additional background information provided by Frontex.

The explanations provided by Frontex in the different parts of the supporting documentation sometimes differ slightly, as noted in section 2 above.

The description as quoted from the business case for transmission to Europol ("transmissions to Europol will take place on a case by case basis which is to say, not systematically or automatically but following a decision in line with data protection principles of proportionally and necessity") appears to fulfil this "case-by-case" requirement. Pushing all received reports onwards at the latest shortly before they expire (as explained in the PeDRA business case

[9] EDPS case 2015-0129

document) would not meet this criterion. Frontex' stated aim (in its replies of 14 May 2015) to transfer information to Europol within 48 hours also casts doubts on whether a true case-by-case assessment would be carried out. **Frontex should**, in line with Article 11c of its Regulation, **only transfer personal data to Europol when this is necessary and proportionate on a case-by-case basis.**[10] Pushing on all information would not be on a case-by-case basis. **Frontex should define a methodology for assessing the necessity and proportionality of transfers to Europol and update the other relevant documents accordingly.**

Article 11c (3)(b) refers to risk analyses in accordance with Article 4 of the Frontex Regulation, which reads read as follows:

> "The Agency shall develop and apply a common integrated risk analysis model.
>
> It **shall prepare both general and tailored risk analyses** to be submitted to the Council and the Commission.
>
> [...]
>
> For the purposes of this Article, **Member States shall provide the Agency with all necessary information** regarding the situation and possible threats at the external borders. […]"

As mentioned above, no personal data shall be included in the results of these risk analyses.

While Article 11c(4) of the Frontex Regulation refers to erasure of the data "as soon as they have been transmitted […] or used for the preparation of risk analyses", Frontex submitted that these two purposes should not be seen as mutually exclusive, i.e. either for transfer to Europol *or* for use in risk analyses. The reason given was that having such an either/or use would greatly reduce the utility of the system. The EDPS agrees and notes furthermore that if such an either/or view were to be adopted, Frontex would have to decide which use would be more valuable, requiring a more in-depth analysis which may approach investigatory activities, which are clearly excluded from the scope of PeDRA by Article 11c(5) of the Frontex Regulation. A single report submitted by a MS may thus be used both for transmission to Europol and for risk analyses. Further considerations regarding conservation of data follow in section below.

In conclusion, the planned processing of personal data in PeDRA as described is covered under Article 5(a) of the Regulation, subject to the recommendations contained in this Opinion, notably the recommendation on "case-by-case" transfers above.

3.3. Processing of special categories of data

Article 10 of the Regulation contains special rules for certain sensitive categories of data. Frontex stated that data on (suspected) offences, ethnicity and sexual orientation may be processed in PeDRA and fall under Article 10.

The processing of data relating to ethnicity and sexual orientation is only allowed in the cases enumerated in Article 10(2) of the Regulation.

Article 10(2) contains a number of situations in which such special categories may be processed. None of the cases mentioned there appears to apply for PeDRA. Article 10(4) allows the Union legislator to lay down additional exceptions.[11]

[10] For the safeguards for the transfer as such, see also section 3.6 below.

[11] The same Article also allows the EDPS to lay down such additional exceptions "if necessary"; this is to be understood as a transitory measure, meant for situations where the Union legislator has not yet laid down such exception following the entry into force of the Regulation. The EDPS no longer grants such authorisations; see

Article 11c(1) of the Frontex Regulation states that "the Agency may further process personal data collected by the Member States during such operational activities and transmitted to the Agency".

This authorises Frontex to further process personal data received from the Member States in the context of PeDRA.[12] These personal data need to have been lawfully collected by the submitting Member State under the applicable national law, which presumably includes safeguards for the processing of such special data.

In those cases where Member States have lawfully collected such special data, this provision could thus also be seen to cover their further processing by Frontex, provided that there are appropriate safeguards to exclude discrimination based on ethnicity.[13]

For increased legal certainty, the **best solution would be to amend the Frontex Regulation accordingly in line with the standards of Article 10(4) of the Regulation** so as to provide a clear legal basis for the processing of such data. Pending this, Article 11c(1) of the Frontex Regulation can be seen as a legal basis for processing this special category of data as well**, provided that appropriate safeguards against discrimination are in place.**

Concerning data on "**sexual orientation**", Frontex explained that migrants are often sexually abused by smugglers/traffickers during the migration process and that therefore such information about smugglers/traffickers may be needed by Europol to conduct its further investigations. The EDPS considers that information about such abuse is in fact information about a (suspected) offence, not about the sexual orientation of the (suspected) offender and should therefore be assessed under Article 10(5) of the Regulation and not under Article 10(2).

There seems to be no need for the processing of personal data on sexual orientation in PeDRA. Therefore, **Frontex should not process personal data on sexual orientation in PeDRA**, taking into account that information on sexual abuse of migrants by smugglers/traffickers is to be considered as data related to an offence, not to sexual orientation.

The processing of data relating to offences, criminal convictions or security measures is, according to Article 10(5) of the Regulation, only allowed if it is authorised by the Treaties or other legal instruments adopted on the basis thereof.

Article 11c(3) of the Frontex Regulation, quoted in section 3.2 above, provides such an authorisation. This special category of personal data may thus be processed in PeDRA for the purposes and under the conditions listed in that Article.

3.4. Data Quality

According to Article 4(1)(c) of the Regulation, personal data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed. This principle is reaffirmed by Article 11c(5) of the Frontex Regulation, which refers to the principles of necessity and proportionality. According to Article 4(1)(d) of the Regulation, their accuracy has to be ensured.

Frontex explained that "non-offence events" referred to events that are not in and of themselves breaches of local law, e.g. information on transport within the third country, but which are linked to the cross-border crimes targeted by PeDRA; including such information appears to be relevant and not excessive.

[12] For more details and the allowed purposes, see section above above.

[13] In this context it has to be noted as well that Europol, as the intended recipient of personal data from PeDRA, is also subject to strict rules on the processing of personal data relating to Ethnicity, see Articles 10(3), 14(1) and 16(1) of Council Decision 2009/917/JHA.

Frontex explained that the responsibility for collecting and providing data, including their accuracy, lies with the Member States. That being said, Member States' Intelligence Officers (contact points) will receive training on how to use the uploading tool; instances of reports that fail the legality check will be recorded to give feedback to the submitting Member States and the individual submitting Intelligence Officers. Additionally an "Intelligence Officers network" is planned in order to facilitate dissemination of best practices. Both in the network and in the trainings, data protection aspects, notably on the need for accuracy, should be addressed. These measures should help to ensure appropriate data quality in the system. **Frontex should ensure adequate monitoring of data quality and follow-up on any issues detected.** This could for example take the form of regular internal reports on data submitted to Frontex by Member States (e.g. numbers and percentages of submission that passed/failed the legality check). The reports to be supplied by Europol to Frontex (e.g. numbers and percentages of PDPs that passed/failed the mandate check at Europol) can contribute to this exercise as well.

The data categories mentioned in the notification do not in principle appear to be excessive (subject to the remarks made in section above). The list was indicated as being non-exhaustive, notably because the reports will at least initially be provided as free-text narrative reports. In order to ensure data quality, it should be ensured that only relevant, adequate and non-excessive personal data are included. To this end, adequate training of the staff providing the initial reports should be ensured, bearing in mind that these are Member States' officials. On Frontex' side, the legality check should also contribute to ensuring data quality.

In order to ensure data quality and allow for easier monitoring, the planned move towards a more structured format appears to be a valuable enterprise. Any future templates or similar should be designed with the data quality principle in mind.

3.5. Conservation of data

According to Article 4(1)(e) of the Regulation, personal data may only be kept for as long as is necessary for the task for which they have been collected or further processed.

Article 11c(4) of the Frontex Regulation established that the conservation period "shall in any event not exceed three months after the date of the collection of those data."

Frontex interprets this conservation period as starting from the moment the data have passed the legality check.

The EDPS understands the term "collection" in this Article as referring to collection *by Frontex*, i.e. the moment when a Member State transfers personal data to Frontex and the message authentication check is passed, not the initial recording of the debriefing by Member States' competent authorities, nor the passing of the legality check.

While it is true that, as Frontex submits, Member States may require a certain amount of time to reply to requests for clarification, this would appear to be an issue for that specific Member State to address.

The **EDPS therefore recommends starting the 90 days conservation period from the authentication of the message received**.

At the end of this period, Frontex will delete certain parts of the information processed to anonymise it. Identifiers such as names, telephone numbers etc. will be removed but the resulting depersonalised information be kept.

The EDPS stresses that simply removing obvious identifiers may not be enough to anonymise the data.[14] **Frontex should ensure that this sanitisation completely anonymises the data**. If

[14] See also the Article 29 Working Party Opinion on the concept of personal data, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

data subjects remain indirectly identifiable, the information is still to be considered personal data. If Frontex cannot ensure irreversible anonymisation, it should instead simply delete the information concerned.

Frontex also intends to keep an archive of all the data processed in PeDRA for a period of - according to current planning - three years. The reason given by Frontex for this period was alignment with conservation periods at Europol. While it initially mentioned "historical and audit purposes" as the reason for the archive, Frontex later clarified that the two purposes were to be able to reply to data subject requests (e.g. for access) and to provide information should it be required in subsequent judicial proceedings.

The uses indicated for the archive do indeed not seem to be of a historical nature. In any case, further processing for historical purposes is subject to specific safeguards, notably that the data must not be used in support of measures or decisions regarding any particular individual (see Article 4(1)(b) of the Regulation).

Concerning data subject requests (e.g. for access), it should be noted that as a general rule, personal data should not be stored for longer than necessary for the purposes for which they have been processed simply to be able to reply to data subject access requests. Indeed, the right of access implies the right to access existing data and should not serve as a justification for further conservation.

For **judicial proceedings**, it should be noted that the original data provided by the Member States are forwarded to Europol as part of the PDPs. For this reason, it would appear more likely that any requests for clarification in subsequent judicial procedures would be addressed to Europol or the relevant Member State. Taking this into account, it does not appear clear why Frontex should also keep this archive for the purpose of answering to requests for clarification. In order to prove that a specific PDP has been sent to Europol, it may not be necessary to keep a full record of all personal data included.

Auditing is a different purpose than providing assistance in judicial proceedings and should be clearly distinguished. For audit purposes, the length of the conservation period would appear to be excessive; it is also not immediately obvious that all data would be necessary.[15] Frontex would need to show which information would be necessary for how long for auditing purposes.

In both cases, purpose limitation is key: the data may be accessed if and only if necessary for (one of) those two purposes.

In any case, **Frontex should further explain the necessity for this archive, especially in the light of the clear conservation period established by Article 11c(4) of the Frontex Regulation**.

3.6. Transfer of data

One main purpose of PeDRA is to generate PDPs for transmission to Europol. Frontex confirmed that otherwise, no transfers to external third parties were foreseen.

Given that Europol is not subject the Regulation, transfers to it fall under Article 9 of the Regulation.[16] It should be noted that the requirements of this Article are cumulative to the

[15] If the aim would e.g. to prove that at a certain point in time a certain PDP was transferred to Europol, it may not be necessary to keep the content of the PDP for this purpose - keeping a hash value may be enough.

[16] While Europol is an agency of the European Union, it is not subject to the Regulation, but to its own special regime. The EDPS interprets Article 9 to cover transfers to recipients that are neither subject to the Regulation, nor to national implementations of Directive 95/46/EC. See page 24 of the EDPS position paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies (position paper), available on the EDPS website.. [

other requirements of the Regulation - a transfer needs to be lawful under Article 5 *and* comply with the safeguards in Article 9.

That Article offers several possibilities for legitimising such transfers. According to Article 9(1), such transfers may occur "if an adequate level of protection is ensured" in the recipient's jurisdiction and "the data are transferred solely to allow tasks covered by the competence of the controller to be carried out".

For the adequacy criterion, this needs to be assessed "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country or recipient international organisation, the rules of law, both general and sectoral, in force in the third country or international organisation in question and the professional rules and security measures which are complied with in that third country or international organisation". Further guidance on how to assess adequacy has been provided by the EDPS[17] and the Article 29 Working Party.[18]

Frontex has carried out and documented an adequacy assessment for Europol, coming to the conclusion that it offers adequate protection.

For the second criterion, Article 11c(3)(a) of the Frontex Regulation provides a clear legal basis for transfers to Europol; they are thus in principle within Frontex' (i.e. the controller's) competence.

However, it needs to be assessed whether the transfer can be considered as happening on a case-by-case as demanded in 11c(3)(a) of the Frontex Regulation, as discussed in section above.

3.7. Information to the data subject

Article 12 of the Regulation sets out the information obligations of the controller in situations where the data have not been collected from the data subject, as is the case for PeDRA. Article 12(2) allows controllers to abstain from providing individual information under certain conditions, notably if this would involve a disproportionate effort or is impossible, or where recording or disclosure are expressly laid down by Union law. In such cases, the controller shall provide appropriate safeguards after consulting the EDPS.

Frontex explained that it would not provide direct information to data subjects on its own, noting that it was not competent to carry out investigations and that it would not be in direct contact with the data subjects (not even competent national authorities are likely to be). It is important to repeat here that the personal data to be processed in PeDRA are those of suspected human smugglers/traffickers or other suspected criminals, not those of migrants.

It may very well be that provided individual information to data subjects would be impossible for Frontex or require a disproportionate effort. For example, contact information may not be available. As Frontex' role clearly excludes investigations, it should not search for additional information e.g. contact information about data subjects.

In those cases where Frontex would be able to provide individual information to data subjects, it should also be noted that data subjects in PeDRA are likely to be subject to criminal

[17] Position paper referred in the preceding footnote, pages 10-13.

[18] The Article 29 Working Party consists of the data protection authorities of the EU Member States, the EDPS and the EC. It has interpreted Articles 25 and 26 of Directive 95/46/EC, which contain the corresponding provisions for processing in the Member States. See Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf

investigations by competent Member State authorities and that informing them individually might tip them off about the Member State's investigation. This may justify applying a restriction under Article 20(1)(a) in these cases.

That being said, to provide a minimum level of transparency, **Frontex should provide a privacy statement covering the elements of Article 12 of the Regulation on its website**.

3.8. Right of access and rectification

According to Articles 13 and 14 of the Regulation, data subjects have the right to access their data and to have it rectified.

Frontex stated that it would apply its standard approach to dealing with access and rectification requests, noting that exceptions under Article 20 may be applied.

Restricting data subject rights should only happen on a case-by-case basis, not as a general policy. In case Frontex makes use of such restrictions, this **should be documented internally, including the reasons for the restriction**.

3.9. Security measures

According to Article 22, the need for measures has to be analysed in light of the **risks** represented by the processing of personal data by the EU institution, the nature of the personal data processed and the type of processing operations. This analysis must cover all processing operations, and all factors that are relevant for risks. Measures shall in particular concern confidentiality, integrity and availability[19]. The specific context of the processing could be a relevant factor for the assessment of the risk represented by the processing.

The requirements analysis process Frontex is following will include a detailed analysis of threats and vulnerabilities to the system followed by the definition of detailed security controls that would mitigate the risks to a level acceptable by Frontex is in principle appropriate to ensure a level of security appropriate to the risks. However, as the detailed analysis to mitigate the threats and vulnerabilities is still to be performed, **Frontex should provide this detailed analysis to the EDPS as soon as it is available, with a description of the measures to be implemented**.

This detailed analysis should include (but not be limited to) elements relating to

- the protection of personal data from system administrators (i.e. preventing that the system administrators unduly read, copy or alter personal data stored in the system or its backups), and
- the protection of logs from system administrators (i.e. preventing that the system administrators unduly consult, erase or change logs for the system)

Finally, this **detailed analysis should consider all points made in the notification and further detail what security measures would be implemented to limit the risks to a level acceptable by Frontex management.**

4. Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing that the recommendations in this Opinion are fully taken into account. To recall, Frontex should (in the context of PeDRA):

[19] Article 22(1): "Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing"

1. only transfer personal data to Europol [20] when this is necessary and proportionate on a case-by-case basis;
2. define a methodology for assessing the necessity and proportionality of transfers to Europol and update the other relevant documents accordingly;
3. pending an amendment of the Frontex Regulation in line with the standards of Article 10(4) of the Regulation so as to provide a clear legal basis for the processing of data on ethnic origin, provide appropriate safeguards against the use of ethnic data for discrimination;
4. not process personal data on sexual orientation;
5. ensure adequate monitoring of data quality and follow-up on any issues detected;
6. start the 90 days conservation period from the authentication of the message received;
7. ensure that this sanitisation completely anonymises the data;
8. further explain the necessity for the archive, especially in the light of the clear conservation period established by Article 11c(4) of the Frontex Regulation;
9. provide a privacy statement covering the elements of Article 12 of the Regulation on its website;
10. document internally all cases in which a restriction under Article 20 of the Regulation is applied, including the reasons for the restriction.
11. provide the detailed security requirements analysis to the EDPS as soon as it is available, with a description of the measures to be implemented; this detailed analysis should consider all points made in the notification and further detail what security measures would be implemented to limit the risks to a level acceptable by Frontex management.

Frontex should report on these recommendations within three months of the date of this Opinion.

Done at Brussels, date

[20] Or other EU law enforcement agencies as specified in Article 11c(3a)