From:	European Data Protection Supervisor
To:	<Fabrice.Leggeri@frontex.europa.eu>
CC:	[redacted]
Sent at:	08/12/15 16:41:56
Subject:	Our ref. 2015-0346 & 0786 D-2274

Dear Sir,

Please find attached a scanned version of a letter (+annex) sent to you by regular mail today.

Best regards,

EDPS Secretariat

Tel. +32 2 283 19 00 | Fax +32 2 283 19 50

edps@edps.europa.eu

European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1040 Brussels

@EU_EDPS www.edps.europa.eu

EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr Fabrice LEGGERI
Executive Director
Frontex
Plac Europejski 6
00-844 Warsaw
POLAND

Brussels, 08 December 2015
WW/OL/sn/D(2015)2274 **C 2015-0346/-0786**
Your ref.: 14891 + 11100a/02.10.2015
Please use edps@edps.europa.eu for all correspondence

Dear Mr Leggeri,

Thank you for your letter of 21 September 2015 and also for Mr Arias' letter of 2 October 2015, both of which provided information on the follow-up given to the EDPS prior check opinion on PeDRA, issued 3 July 2015.

As the consultation on implementing rules for PeDRA is closely linked to the follow-up to the prior-check opinion on PeDRA, the EDPS provides its comments on the draft implementing rules in the parts dealing with the relevant recommendations from the opinion.

Please find attached a table with our assessment of the information provided. Overall, Frontex has made very good progress. As you will see, the closure of several recommendations is dependent on the adoption of draft Implementing Rules for PeDRA, so please communicate them to us once they are adopted.

Wojciech Rafał WIEWIÓROWSKI

Cc: [redacted]

Recommendation	Frontex Action	EDPS Assessment
1. Only transfer personal data to Europol when this is necessary and proportionate on a case-by-case basis;	Detailed rules explained in draft implementing measures, Article 15.	Ok, although the **approach described could possibly be simplified**. For example, the detailed list of areas of interest included in Article 15(4) and (5) of the draft Implementing Rules could be replaced by greater reliance on proportionality: in the current version, the necessity assessment risks becoming a matter of ticking a box, meaning both that there would possibly not be a substantive evaluation of necessity, while also creating a risk of relevant information being excluded from transfer to Europol due to not fitting in any of the predefined boxes. With a greater emphasis on proportionality, a more substantive assessment could be carried out in specific cases, ensuring both that only relevant data are transferred, while also avoiding that relevant data would be withheld for formal reasons. The EDPS would have no objection to such a less formalistic approach - Frontex has a certain margin of manoeuvre here. **Recommendation to be closed once draft Implementing Measures have been adopted.** It is assumed that the rest of PeDRA documentation will be brought in line with the approach described in the draft Implementing Measures, once adopted.
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,	Frontex stated that the search functionality in PeDRA will not allow querying by ethnicity. Detailed rules are laid down in Article 9 of the draft Implementing Measures.	As explained in the opinion, data on sexual orientation should not be processed, while for data on ethnicity, the EDPS prior check opinion required additional safeguards. This is to be seen against the background that Frontex could only process such data where they have been provided by a Member State, which is presumed to have lawfully collected them under its own national rules. The EDPS understands that there will be no systematic collection of such data, but that it may incidentally be included in the information provided by Member States. As concerns the actual safeguards provided by the proposed Article 9, paragraph 5 restates the principle that such data may not be used for discrimination; not having the possibility to search by ethnicity contributes to ensuring this. **Compliance with the rules on special categories of data should be part of the data quality**

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

Recommendation	Frontex Action	EDPS Assessment
provide appropriate safeguards against the use of ethnic data for discrimination;		**check during the authentication process in Article 14(5)(b) of the draft implementing rules.** It is currently implied by the reference to Article 4 of the draft implementing rules, but should be made more explicit.
4. Not process personal data on sexual orientation;	Forbidden by Article 9(1) of draft Implementing Measures	Ok, **recommendation to be closed once draft Implementing Measures have been adopted.**
5. Ensure adequate monitoring of data quality and follow-up on any issues detected;	Detailed in several Articles of draft Implementing Measures, e.g. Article 5, 14 and 21.	Ok, **recommendation to be closed once draft Implementing Measures have been adopted.**
6. Start the 90 days conservation period from the authentication of the message received;	Defined accordingly in Article 11(1) and (2) of draft Implementing Measures	Ok, **recommendation closed.**
7. Ensure that sanitisation completely anonymises the data;	Article 11 of the draft Implementing Measures.	Article 11(3) explains the difference between anonymisation and pseudonymisation. This Article could be made clearer by focusing on anonymisation, which is the more relevant concept here. As currently drafted, it explains why pseudonymised data are not anonymised, but does not explain what "anonymised" means and how it will be *ensured* that the sanitisation process will completely anonymise the data. **Frontex should provide further information on how the sanitisation process will work.**
8. further explain the necessity for the archive, especially in the light of the	Frontex explained that the archive was necessary for two purposes: a) providing a clear trail of	The EDPS notes that while these risks may be real, they are not part of the risk assessment provided under recommendation 11. Certain controls may be necessary, but should be based on a risk assessment. For example, if non -repudiation of transfers is the target, then PeDRA business logs together with hash values of the

Recommendation	Frontex Action	EDPS Assessment
clear conservation period established by Article 11c(4) of the Frontex Regulation;	what happened for information security purposes; b) providing information on processing by Frontex in judicial proceedings. Otherwise, Frontex would see a risk of not being able to defend itself against accusations of inept or inappropriate processing of data. This archive would be kept separate from the operational logs with additional security measures and would only be accessed for the two purposes mentioned above.	PDPs transferred could possibly be sufficient and would not necessarily entail the processing of personal data. **Frontex should provide an assessment of the specific risks it intends to mitigate with the archive and justify the proposed controls including an explanation of how purpose limitation will be ensured, keeping in mind that Article 11c(4) of the Frontex Regulation creates a strict upper limit for the conservation of personal data received from the Member States.**
9. Provide a privacy statement covering the elements of Article 12 of the Regulation on its website;	Under preparation, to be published before pilot exercise (scheduled for February 2016)	Ok, **recommendation to be closed once published.**
10. Document internally all cases in which a restriction under	Article 17 of draft Implementing Rules restricts the rights under Article 12(1) and 15 to 17 of	The **blanket restriction of the rights under Articles 12(1) and 15 to 17 of Regulation (EC) 45/2001 is not justified.** Please note that restrictions should only occur on a case-by-case basis. The right to erasure under Article 16 of Regulation (EC) 45/2001 basically applies only when the processing was unlawful (e.g. personal data of a victim being processed). Similarly, the right to

Recommendation	Frontex Action	EDPS Assessment
Article 20 of the Regulation is applied, including the reasons for the restriction.	Regulation (EC) 45/2001; it also notes that the rights under Articles 13 and 14 of Regulation (EC) 45/2001 may be restricted on a case-by-case where justified under Article 20(1)(a) of the same Regulation. In this case, this has to be documented internally, including the reasons for the restriction.	object under Article 15 of Regulation (EC) 45/2001 can only be invoked under certain circumstances, which would appear to be unlikely for PeDRA. Article 17 is ancillary to these rights. While the EDPS cannot exclude that a restriction to these rights may be necessary in specific cases when data subject want to exercise them, it is not appropriate to impose a blanket restriction. As concerns Article 12(1), please note that paragraph 2 of the same Article excludes cases where informing the data subject is impossible or would require a disproportionate effort. In this situation, Frontex does not need to invoke Article 20 in order not to inform the data subject. The recommended publication of a privacy statement can act as a safeguard here. **Ok for possibility to restrict the application of Articles 13 and 14** of Regulation (EC) 45/2001. Such restrictions have to be documented, as recognised in Article 17(1)(b) of the draft Implementing Rules.
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	Frontex provided a security analysis, containing identified risks and mitigation measures for some of them. This analysis focused on the systems development for PeDRA.	The risk analysis (using Microsoft's STRIDE methodology) provided by Frontex only covers systems development. STRIDE is focused on software elements and aims at preventing IT attacks to that software. This is of course part of the analysis that should be performed but does not cover all risks relating to the processing of personal data and to the system as a whole. For example, Frontex has identified several threats to the organisation in its discussion of Recommendation 8 that do not appear in the analysis provided for this recommendation. E.g. if there is a risk that Frontex analysts are accused of inappropriately or ineptly processing personal data, then a description of the risks and corresponding security measures to be implemented should be included in the risk analysis In order to have a full picture of the risks and necessary controls, the assessment should cover the entire lifecycle - development, operations, decommissioning - of PeDRA, as well as taking the environment in which it will operate into account. Additionally, according to the developer of the methodology and the tool that seems to have been used by Frontex, "You should analyze your threat model with your team to ensure you have addressed all potential security pitfalls".

Recommendation	Frontex Action	EDPS Assessment
acceptable by Frontex management.		**Frontex should define an appropriate risk assessment methodology that would cover all risks relating to the processing of personal data performed in light of the notification that was provided to the EDPS**. For inspiration, Frontex could look at the following methodologies (non-exhaustive list): • Magerit[1] • EBIOS [2] • Octave [3] These methodologies offer information related to threats Frontex might consider in the context of PeDRA. **If Frontex has performed a risk analysis that cover risks to Frontex in a more generic manner (i.e. a baseline risks analysis that is valid for all processing of personal data performed in Frontex), and in addition that risk analysis bridges the gap between the EDPS request and the STRIDE analysis provided to the EDPS, then this baseline risk analysis can be provided to the EDPS in order to fulfil the recommendation 11.** In terms of controls to consider (*after* the risk analysis is performed), Frontex can take inspiration from ISO 27002.

[1] http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en#.VjHuoUbCfw0
[2] http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
[3] http://www.cert.org/resilience/products-services/octave/