PeDRA Data Protection ACTION TABLE as recommended by the EDPS

Action	Implemented YES/NO	Remarks
1. Only transfer personal data to Europol when this is necessary and proportionate on a case-by-case basis;	***YES***	***This is well-recognised in all PeDRA documentation, in the draft Implementing Measures (sent already for consultation to the EDPS) and is elaborated further under point 2 of this response.***
2. Define a methodology for assessing the necessity and proportionality of transfers to Europol and update the other relevant documents accordingly;	***YES***	***Article 15 of the draft Implementing Measures[1] contains the methodology for ensuring the necessity of transmissions to Europol, and the relevant project documents have been updated accordingly[2]. Article 15(1) lists the legal requirements of any transmission of personal data to a recipient agency, while para. 3 reminds us that the Data Controller shall be required to make an evaluation of the necessity of the transfer. This evaluation will be partially based on added-value, but will also be informed by explicit requests for certain categories of personal data made in advance by Europol and listed in each Operational Plan. Any personal data that fall outside of the explicit request from Europol at the beginning of each operation, shall not be transmitted to Europol.*** ***Although this complies with the data protection principle, we feel compelled to communicate to the EDPS that this is very likely to lower the efficacy of the personal data in a law enforcement environment, where the most useful data are very often unforeseen.*** ***Frontex regards the issue of proportionality to be of low risk for several reasons. First, it should be recognised that the personal data will be used to prevent criminal offences that result in decreased internal security within the European Union and often result in considerable loss of life, for example in the Mediterranean. This means that the purposes for processing under PeDRA will always be very important compared with the data protection rights of the suspects.***

[1] Draft MB Decision adopting Implementing Measures for the processing of personal data collected during joint operations, pilot projects and rapid interventions

[2] Business Case for Transmission of personal data to Europol v3; PeDRA Full business case v6

		Secondly, the collection of the personal data by Member States is done manually in the field, and is very labour intensive. There may in the future be the possibility of inspecting the mobile phones of migrants to look for personal data relating to human traffickers or smugglers, but apart from this we do not foresee any other electronic collection of personal data. Hence, Frontex does not expect to receive large quantities of personal data that were automatically collected via electronic or any other means, and so there is little risk of PeDRA involving volumes of personal data disproportionate to the purposes for which they are collected. ***Thirdly, very large numbers of irregular migrants are often facilitated by a small number of individuals, and so we expect that even after the detection of a large and overcrowded boat, most migrants will be providing data relating to the same data subjects. Migrants, asylum seekers and victims always vastly outnumber suspects and so the number of data subjects is expected to be low compared to the number of sources.*** ***Finally, collection of the personal data will mostly take place as a result of direct contact with individual migrants. When few migrants are detected the volume of personal data will be greatly diminished, but so will the need for the personal data as there would be fewer crimes being committed. In contrast when large numbers of migrants arrive, the volume of collected personal data will likely increase, but so will the need. Hence, we consider the proportionality to be, to a great extent self-regulated.***
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;	***YES***	***Article 9 of the draft Implementing Measures is specifically about special categories of data. Para. 2 lists the conditions where processing data on ethnicity is permissible: where ethnicity is much more appropriate than nationality in analysing a certain crime or identifying an individual.*** ***There do not exist any possibilities of using ethnicity for the purpose of discrimination, as all ethnicities will be treated equally in the analytical process. As an additional safeguard, it will not be possible to search the PeDRA database using just ethnicity as the only query term. Using logs from the archive the Agency it will be able to test for any signs of discriminative analyses.***
4. Not process personal data on sexual orientation;	***YES***	***Article 9 (1) of the draft Implementing Measures specifically prohibits processing data on sexual orientation.***

5. Ensure adequate monitoring of data quality and follow-up on any issues detected;	***YES***	***There are two issues here: firstly, that personal data are transmitted by the nominated Member State representatives using pre-agreed and secure channels, and secondly that the data are legal and of high quality. These requirements are addressed in several places in the draft Implementing Measures and will be specifically outlined in all Operational Plans.*** ***For example, Article 5(3)a reminds Member States that their Intelligence Officers are responsible for ensuring that only personal data that comply with the Data Protection Regulation, the Frontex Regulation, the Implementing Measures and the specific Operational Plan are transmitted to Frontex, whereas Article 10(1) states that transmissions received from inappropriate channels will be logged for monitoring purposes.*** ***Article 14(8) relates to the authentication process and states that in the case of a transmission failing a component of the authentication process, Frontex shall contact the Intelligence Officer in the sending Member State and inform about the failure and the reason for the decision.*** ***Finally Article 21(a) relates to the monitoring and evaluation of data quality issues, in terms of the quality of data transmitted to Frontex by host Member States, and Article 21(c) refers to the efficacy of the same personal data once it has been further processed by Europol.***
6. Start the 90 days conservation period from the authentication of the message received;	***YES***	***We agree that this is the most appropriate time to start the conservation period and this is reflected in Article 11(1) and (2) of the draft Implementing Measures.***
7. Ensure that this sanitisation completely anonymises the data;	***YES***	***Article 11(3) recognises the difference between deletion/anonymisation, which completely depersonalises the data for placing in risk analysis reports, and pseudonymisation which codifies personal data but leaves the individual still identifiable.*** ***Article 11(4) covers these aspects and also ensures that personal data are deleted/anonymised from original data files, additional files, and also from backups.***
8. further explain the necessity for the archive, especially in the light of the clear conservation	***YES***	***Article 12 covers the processes involved in archiving the personal data and logs encrypted, away from operational systems and with limited access.*** ***The encrypted archive will serve to protect the Agency and individual data processors from liability in case of security***

period established by Article 11c(4) of the Frontex Regulation;		***breaches. There have been examples in Member States of security leaks whereby law enforcement data were found in the hands of unauthorised users or even criminals. In this case encrypted archives and logs were used in defence of the authorities and individual processors. Under PeDRA the same personal data will be processed (often simultaneously) by Member States, Frontex and Europol. It would produce an unacceptable institutional risk if during a security breach Frontex was the only organisation without an archive of its actions.*** ***In a law-enforcement environment it is considered best practice to keep a detailed record of what has been done to the data and by whom, so that the organisation and the individual processor can defend against accusations of inappropriate or inept processing of personal data. This is important when testing for prejudiced analytical behaviour of individual analysts that may for example, only be analysing the behaviour of certain ethnicities in a discriminate way. It is also important to show, in the face of acquisitions to the contrary, that the Agency as a whole operates an objective analytical environment.*** ***This archive is also required in case of judicial proceedings which require confirmation of data processing that took place in Frontex. Judicial or Data Protection authorities may be able to approach the sending Member States for the 'original' data, but where there is a sudden influx of migrants at the border the personal data may not be stored or processed at the national level. It is not unreasonable to assume that, at periods of peak activity at the border, the flow of personal data to Frontex may not be replicated to national authorities in the sending Member State, especially as Frontex is automatizing the import of data into analytical systems, a task which may have to be done manually in the sending Member State.*** ***In many cases Europol transmits personal data back to Member States. In the event that Member States receive their own data back again but in a modified form, it may be necessary to reconstruct the flow and processing of the data. In most cases if Frontex modifies the personal data, both the original and the modified form will be transmitted to Europol. However, the reason for the modification may not be immediately apparent without detailed logs from the archive.*** ***The duration that logs and personal data are kept in the encrypted archive will not exceed the retention period in recipient agencies.***
9. Provide a privacy statement covering the elements of	***YES***	***The statement is being prepared and will be put on the Frontex website in advance of the Pilot Exercise which is scheduled for (Feb 2016).***

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.	***YES***	***Article 17 of the draft Implementing Measures foresees that the application of Article 12(1) and Articles 15 – 17 of the Data Protection Regulation are permanently restricted. Application of Articles 13 and 14 may be restricted by the decision of the Data Controller on individual basis, documented internally, including the reason for 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.	***YES***	***The security analysis is attached to this document.***