FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

50th DCP meeting: discussion topic 2 “Implementation of the EDPS recommendations on FAR” – outcomes

Recommendation No. 3	**When would be the best time to provide the returnees with a data protection notice?**	**Which form should this data protection notice take?**	**How do you fulfil this obligation under the GDPR? Could these two procedures be combined?**	**What challenges do you foresee in the implementation of this recommendation?**	**How could Frontex best support Member States in the implementation of this recommendation?**
	- MS **not in favour of providing a briefing or leaflets in the waiting room at the airport**: it could give the returnees a pretext for raising unnecessary discussions, may cause unrest among the returnees, may put in disadvantage the violent returnees that are forbidden to receive anything (as they are e.g. in body cuffs) - One MS suggested it could be handed out together with information on the Complaints Mechanism - Another MS suggested migrants could be informed about possible data processing within	- The best solution would be to join the distribution of the **notice with the distribution of return decision and other documents** by MS - It could be **either as part of the decision itself or via a leaflet** to be added to the RD (does not have to be linked to specific action, but could maybe cover data processing in a more hypothetical, general manner to fulfil at least the an obligation to inform about the *possibility* of data processing, e.g. “be aware your personal data, in case of Frontex involvement, might be processed for the	- SWE: asylum seekers are informed that they will be investigated and might receive negative decision – why not inform them of legal system re data processing at this moment? (“In case of negative decision, your personal data might be processed…”) - NOR: incorporated in national law, a change would have to go through the Ministry of Justice - DNK: via direct contact with the concerned person after issuance of return decision - AUT: via notice posted	- On **scheduled flights**, only the return decision may address properly cases of persons returning via voluntary departures, i.e. on their own - **Translation of the text** would be an issue. Earlier distribution may address this problem, as then it will be less of an issue to receive it in the MS official language, as are all the other documents distributed to the returnees - Early information/notice may lead to higher **risk of absconding** - Processing of personal data of **other**	- Put the **notice in FAR** to ensure returnees are informed - Produce an **informal paper/ fact sheet**, publish it in FAR for MS to hand it over to returnees during the pre-departure phase - **Monitor access to FAR**; lay down data protection rules and decide, most likely on a case-by-case basis, on the right of access - Develop a **backup plan** for cases when returnees disappear before they are informed

	the EU when arriving in Europe or at least at the beginning of a return procedure - In general, **MS would prefer to decide on their own** accord when such notice should be handed over to the returnee	purpose of…”) - The MS were rather in favour of **generic text, that would cover both national data processing notice and the one Frontex one** or even indicate the involvement of third country - Some MS would prefer to prepare the generic text themselves, others suggested **Frontex should create a unified notice and its translation into other languages** (the notice could be used independently of Frontex involvement in an operation)	on the official website	**participants** of return operations - Cases when a returnee **objects** to the processing of their data - **Feasibility** of linking the notice to the return decision (e.g. another authority/court issuing the decision) - Informing returnees whose data is initially in FAR and then is deleted or changed - Frontex should be prepared to take legal responsibility as FAR is separate from national systems	
Recommendation No. 9	**What measures are in place in Member States (IT environment) to ensure secure use and access to FAR?**	**What is the baseline level of security that you would find relevant and possible to achieve (guarantee) from your perspective?**	**What measures are possible and should be added, in your view, to ensure the integrity and confidentiality of the data on your work stations during and after access to FAR?**	**How can Frontex best support the Member States in the implementation of this recommendation?**	**Other remarks**
	- ESP: protection from work stations only; if accessed outside of the office (e.g. at night) or	- MS stated that they have **very good security features already in place**	- An **app with limited functionalities** (e.g. regarding data	- Application allowing **secure access through mobile**	- IRMA access management (COM → national-level IRMA managing authority →

	even on mobile phone – personal responsibility - SWE: FAR outside of the office, only accessible via work laptop, no access from private devices - CHE: secured with personal smart card – not possible to log in through insecure wireless connections	**regarding access to official equipment** (including smart-card protection, access policies, credentials) but the persons present did not have deep knowledge about specific security features - There are data protection officers in MS who deal with access also to national systems, so Frontex systems are under national policies as well	extraction from FAR) - **Automatic logout time** (due to inactivity of user), e.g. 5 or 10 minutes - Implementation in FAR **automated tool for verification of FAR user’s browser and antivirus validity** (if both are updated) - The MS generally recognize existence of threats of using mobile solutions	**devices** - Address **people responsible for developing security systems** - Define exact **procedures, safeguards and solutions**, also on the rules of responsibility for data (e.g. system developer? User?); first **procedural policy** level, then practical/technical solutions - **Provide support**, also **technical**, to MS which do not have advanced security system in place - Perform a **regular check** on who is granted a**ccess to FAR**, verify and update the list of persons with access granted - A **questionnaire** can solve the question on collecting the information about security features in place, it could be answered by technical	FAR access management) - Is data in FAR very sensitive? (names and nationalities only)

				staff	