EDPS RECOMMENDATION N. 9

ADOPTION AND IMPLEMENTATION OF A PLAN TO OBTAIN BETTER KNOWLEDGE OF THE SECURITY MEASURES APPLIED BY MEMBER STATES AND TO AGREE ON BASELINE SECURITY MEASURES

Background

In order to address the EDPS recommendation on security of processing and risk assessment, ECRet has:

-   consulted Member States on the recommendation and next steps, and

-   created a joint working group together with Frontex ICT with the aim of developing the requested implementation plan.

Outcome of discussions with Member States

Member States have been asked to comment and provide their feedback on the implementation of this recommendation for the meeting of the Direct Contact Points on Return and the Pre-Return Assistance Network (DCP/PRAN meeting) which took place in Warsaw on 4-5 December.

Member States were specifically asked to discuss:

-   the measures in place to ensure secure use of FAR and Frontex systems;

-   the baseline level of security that would be possible for Member States to achieve and guarantee;

-   what measures should be added to ensure the integrity and confidentiality of the data on workstations;

-    Frontex support to Member States in the implementation of this recommendation.

Overall, Member States already have a number of security features in place regarding access to official equipment (including smart-card protection, access policies, credentials), but the level of these security measures differ from country to country. In addition, FAR often has to be accessed from devices other than office workstations due to business needs outside regular working hours, and rules for access to these devices are also diverse.

Additional security measures to be introduced could include:

- the development of an application with limited functionalities regarding data extraction from FAR;

- an automatic logout time (due to inactivity of user), e.g. 5 or 10 minutes;

- the implementation in FAR of an automated tool for verification of the user's browser and antivirus validity (to check if both are updated).

While Member States generally recognise the existence of threats in the use of mobile solutions, they are adamant that any new security measures must not hamper operationality. In order to continue to be useful, FAR ought to remain a user friendly platform that does not give Member States additional burdens.

Frontex support to Member States in implementing this recommendation could include:

- the development of a secure application for mobile devices,

- the creation of a network of ICT security officers,

- the development of procedures, safeguards and solutions regulating the responsibility for data (e.g. system developer, user),

- the provision of any necessary technical support;

- regular review of the FAR access list.

Conclusion and next steps:

- Member States recognise the need to ensure secure access to data in FAR but on the condition that security measures do not hamper operationality;

- Member States remain open to dialogue with Frontex on new solutions;

- Frontex will develop a questionnaire for Member States so as to obtain additional information on existing security measures and practicable baseline security measures;

- Frontex will develop a detailed policy on security and access to FAR.

Joint Working Group

The ECRet and ICT Joint Working Group is working to find solutions to update the security measures in FAR. By bringing together FAR managers/users with system administrators and the ICT Security Officer, the group will be able to offer viable solutions from both the operational and the IT point of view.

A current proposal includes asking SharePoint Administrators to enable logging the user agent (browser version, operating system version) of the FAR users over 1 month, in order to obtain information on Member States' upgrades.

The Joint Working Group is also responsible for developing the above-mentioned questionnaire for Member States which will assess:

- Existing security measures applied at Member States' level, and

- The feasibility of developing specific baseline security measures.