POLAND

Polish position as regards amendments to 2016/794 Regulation under block 4: enabling Europol to enter data into the Schengen Information System

1) Do you agree that there is an operational need to make verified third-country sourced information on terrorists and other criminals available to frontline officers (border guards and police officers) in order to detect those persons when they seek to cross EU external borders or when they are being checked within the EU?

Poland is of the opinion that the defined security gap has to be adequately addressed and information about any potential threats to the security of EU should be available to law enforcement officers. Bearing in mind that protecting Europeans from terrorism and organised crime is one of our strategic priorities, the instruments providing access to that information to frontline officers seem to be the most effective and increasing the probability of identifying/controlling the person posing the risk.

2) If so, do you agree that the Schengen Information System is the right tool to make this information available to frontline officers (border guards and police officers)? If not, what alternative solution would you propose?

Poland generally supports the direction of changes proposed in the SIS in relation to Europol. The extension of the SIS to alerts entered by Europol is in line with the EU's efforts to date in the area of redesigning the architecture of large-scale EU information systems to support the security of citizens of the Member States. In the opinion of our experts, possibly SIS is the best available tool to make information available to frontline officers.

At the same time, we believe that a balanced approach to changes in SIS is necessary, emphasizing in particular the need to maintain the supporting role of Europol and the need to assess the added value that these changes can bring in relation to the costs and practical consequences for SIS end users. To this end:

1) The added value of the new category of the SIS alert will depend to a large extent on the quality of information provided by third countries to Europol, therefore it is of utmost importance to set effective verification mechanism in terms of credibility, accuracy, complexity and respect of fundamental rights of individuals. The question is, if Europol has resources to conduct such verification in an appropriate manner, in case of large quantity of data and necessity to check every information case-by-case.

2) The disclosure of information based on a hit should depend on the type of crime and only after obtaining the consent of the Member State that owns the alert. From an operational point of view, it is also important to precisely define the actions to be taken after the hit on the basis of the alert.

3) We believe that the effective implementation of possible changes requires that the European Commission, eu-LISA and Europol coordinate activities in this area so that any changes for national users do not require the launch of separate sub-projects carried out in individual bodies and services. The implementation of the changes related to Europol coincides with the SIS Recast projects already carried out by eu-LISA and the implementation of interoperability of large-scale systems.

There are also a number of connections between this draft Regulation and other EU legislation on large-scale EU information systems. In particular, an evaluation of the provisions at Union level relating to the VIS and ETIAS is necessary to determine whether the new category of SIS alerts should be processed automatically in ETIAS and VIS.

In technical terms, we have to bear in mind risks such as: the relationship between the preparations that eu-LISA has to make for the Central SIS and the preparations Europol has to conduct for establishing the technical interface for transmitting data to the SIS; potential problems that eu-LISA might face in managing the changes presented in this proposal due to the other changes currently being introduced (e.g. introduction of the Entry / Exit System, ETIAS and updates of SIS, VIS and Eurodac); the lack of ICT resources, which results in delays in making the necessary changes and upgrades to the main system.