EXECUTIVE SUMMARY

This Supervisory Opinion is issued in response to a request for prior consultation from the European Union Agency for Law Enforcement Cooperation (Europol). The request concerns the proposal of ‘information alerts’ in the Schengen Information System (SIS) – a new type of processing that will involve the collection, transmission and storage of personal data, including biometric data (fingerprints and facial images) of third-country nationals suspected of terrorist offences or other serious crimes.

The SIS is the EU’s largest information system for border control and law enforcement. Historically Europol has only been able to query the SIS. Now, the proposed ‘information alert’ mechanism would enable Europol to propose the insertion of new alerts, while the final decision to enter an alert remains with the competent national authority.

Europol’s DPIA identified two principal risks: (i) the risk that personal data transmitted to Member States becomes inaccurate or outdated, and (ii) the risk that an erroneous threat assessment leads to the wrongful proposal of an alert. Both risks were assessed as high impact with a moderate likelihood. The mitigation measures described to mitigate these risks are deemed by the EDPS to be insufficiently detailed to demonstrably lower the likelihood.

In addition, the EDPS identified four further risk areas that are not fully addressed in the DPIA. First, Member States could keep the intelligence package even when no alert is issued, which would go against the principle of purpose limitation. Second, the ‘overall assessment’ test for proposing an alert lacks a clear framework, opening the door to inconsistent and potentially disproportionate use. Third, the method for choosing the responsible Member State - particularly the terms ‘taking into account previous proposals’ and ‘consecutively’ - is ambiguous and need to be interpreted in a way which does not create the risk of ‘alert shopping’. Finally, the overlap between the criteria to propose SIS information alert and the criteria to feed information into the ETIAS watchlist creates uncertainty about how these two processes would practically overlap.

To remedy these gaps, the EDPS issues five recommendations, three of which are deemed necessary to ensure compliance with the data protection framework.