

Legislation on Information Alerts in SIS Passed

Thomas Wahl

News

On 6 July 2022, the European Parliament and the Council passed new legislation that establishes the category of “information alerts” for entries into the Schengen Information System (SIS). The respective [Regulation \(EU\) 2022/1190](#) amending Regulation (EU) 2018/1862 was published in the Official Journal L 185 of 12 July 2022, p. 1.

“Information alerts” target third country nationals who are suspected to be involved in terrorist offences or other serious crime (listed in Annex I of the Europol Regulation 2016/794). The aim is to monitor their movement, and to make all information on the suspect directly and in real time available to front-line officers in Member States. Since the information on third country nationals is frequently provided by third countries or international organisations only to Europol, Europol will play a crucial role in the process of entering information alerts into the SIS.

According to the Regulation, Europol will propose to Member States to enter information alerts into the SIS in the following situations:

- Where there is a factual indication that a person intends to commit or is committing any of the mentioned offences;
- Where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to believe that that person may commit an offence mentioned above.

In addition, Europol must establish that the information alert is necessary and justified, i.e. Europol must be sure that the information received is reliable and accurate and that no other alert on the person concerned in the SIS already exists.

Other obligations for Europol include:

- Sharing all of the information that it holds on the case and the assessment of the person concerned;
- Informing Member States without delay if Europol has relevant additional or modified data in relation to its proposal to enter an information alert into SIS or evidence suggesting that data included in its proposal are factually incorrect or have been unlawfully stored
- Transmitting information to the issuing Member State “as soon as possible” if Europol has evidence suggesting that data entered into SIS as information alert are factually incorrect or have been unlawfully stored (e.g. if third countries provide the information for politically motivated reasons).

AUTHOR

Thomas Wahl

Senior Researcher
Max Planck Institute for the
Study of Crime, Security and
Law

ISSN: 1862-6947



Member States must also meet several obligations, such as:

- Issuing Member States must inform other Member States and Europol if – after an own verification of the information received – the information alert is entered into the SIS. To this end, Member States must put in place a periodic reporting mechanism;
- Executing Member States must collect and communicate certain information about the third country national to the issuing Member State in the event of a hit;
- Member States must inform Europol about any hit on information alerts or the location of the suspect who is subject to an information alert on the territory of the issuing State;
- The issuing Member State must review the need to maintain the information alert after the retention of one year. Following a thorough individual assessment, the information alert can be kept longer than the review period.

Europol and the Member States now need to adopt the technical and procedural arrangements to implement the Regulation. The Commission will then set the date when Member States can start entering, updating and deleting information alerts in the SIS. Europol's new role in the SIS comes shortly after Regulation 2022/991 set up the new mandate of Europol. It entered into force on 28 June 2022 (→ related link).

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.

All news items are freely accessible at: <https://eucrim.eu/news/>

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.

The project is co-financed by the [Union Anti-Fraud Programme \(UAFP\)](#), managed by the [European Anti-Fraud Office \(OLAF\)](#).



**Co-funded by
the European Union**