Digital information exchange in terrorism cases

2021/0393(COD) - 12/07/2023 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 623 votes to 26, with 4 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2018 /1727 of the European Parliament and of the Council and Council Decision 2005/671/JHA as regards the exchange of digital information in terrorist cases.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amends the Commission proposal as follows:

Eurojust's competence

Eurojust should assist in investigations and prosecutions involving only a Member State and a third country, or a Member State and an international organisation, provided that a cooperation agreement has been concluded with that third country or international organisation or that, in a particular case, there is an essential interest in providing such assistance.

The amended text clarifies that the decision as to whether and how Member States provide legal assistance to a third country or an international organisation remains the exclusive competence of the competent authority of the Member State concerned, subject to applicable national, Union or international law.

National correspondent for Eurojust

Each Member State should designate a competent national authority as a national correspondent for Eurojust on terrorism matters. This correspondent should be empowered to collect this information and to transmit it to Eurojust, in accordance with national criminal procedural law and applicable data protection rules.

Exchange of information on terrorism cases

As regards terrorist offences, the competent national authorities should inform their national members of any ongoing or concluded criminal investigations supervised by judicial authorities as soon as the case is referred to the judicial authorities in accordance with national law, in particular national criminal procedural law, of any ongoing or concluded prosecutions and court proceedings, and of any court decisions on terrorist offences.

That obligation should apply to all criminal investigations related to terrorist offences regardless of whether there is a known link to another Member State or a third country unless the criminal investigation, due to its specific circumstances, clearly affects only one Member State.

Terrorist offences for the purpose of this Article are offences referred to in Directive (EU) 2017/541 of the European Parliament and of the Council on combating terrorism.

The information transmitted should include the **operational personal data and non-personal data** set out in Annex III. Such information may include personal data in accordance with Annex III, point (d), but only if such personal data are held by or can be communicated to the competent national authorities in accordance with national law and if the transmission of those data is necessary to identify reliably a data subject.

Secure digital communication and information exchange between national competent authorities and Eurojust

Communication between the competent national authorities and Eurojust under this Regulation should be carried out through the decentralised IT system. The case management system should be connected with a network of IT systems and **interoperable e-CODEX access points**, which operate under the individual responsibility and management of each Member State and Eurojust, enabling the secure and reliable cross-border exchange of information.

The decentralised IT system should allow secure exchanges of data between the competent national authorities and Eurojust, without any Union institution or body intervening in the content of these exchanges. The decentralised IT system should comprise the IT backbone systems of the Member States and Eurojust which are interconnected by interoperable access points. The access points of the decentralised IT system should be based on e-CODEX.

Case management system

Eurojust should establish a case management system for the processing of operational personal data listed in Annex II, data listed in Annex III and non-personal data.

Where Eurojust has been granted access to data from other EU information systems established under other Union legal acts, it may use the case management system to connect to such systems for the purpose of retrieving and processing information, including personal data, provided that it is necessary for the performance of its tasks.

Retention of data

Eurojust may not retain operational personal data transmitted in accordance with the Regulation beyond five years after the date on which the judicial decision of the last of the Member States involved in the investigation or prosecution has become final, or three years in the event of withdrawal of the indictment, acquittal or a final decision not to prosecute.

Annex III

The amended text provided for:

- adding the following information to the list of information identifying the suspected, accused, convicted or acquitted person: place of residence; business name; legal form; telephone numbers; IP addresses; e-mail addresses; details of bank accounts held with banks or financial institutions, as well as:

- adding to the list of information relating to the terrorist offence information concerning legal persons involved in the preparation or commission of a terrorist offence.