Council of the European Union

Brussels, 10 March 2022
(OR. en)

7079/22

Interinstitutional File:
2021/0393(COD)

LIMITE

JAI 323
COPEN 87
EUROJUST 27
CT 42
ENFOPOL 121
COTER 69
CODEC 269

PUBLIC

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. Cion doc.:	14458/21 + ADD 1
Subject:	Draft Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1727 of the European Parliament and the Council and Council Decision 2005/671/JHA, as regards the digital information exchange in terrorism cases - Non-paper by the Commission services

Delegations will find attached a non-paper by the Commission services on the transmission of biometric data.

ANNEX

PUBLIC

Non-paper from the Commission services on the transmission of biometric data for the CTR at eurojust[1]

This explanatory note provides additional information on the Commission's proposal to transmit biometric data incl. fingerprints as set out in Article 21a(3) and Annex III of the Eurojust Regulation. It also presents the alternatives, which the Commission services considered during the drafting process and explains the reasons, why these were discarted.

I. Commission proposal: obligation to transmit biometric data incl. fingerprints, only where available

In the consultations, the Commission services received the feedback that biometric data would enhance the capability of link detection between judicial cases in the CTR, and guarantee that a hit is reliable when it comes to establishing the identity of a person. A link between cases based on the biometric information of a suspected/accused terrorist is more accurate since it uniquely identifies a person, whereas a link based e.g. on a name and surname might not be relevant at all. Without biometric data, more manual checks/human resources and additional time will be required to confirm the relevance of hits. In the view of Commission services, the transmission of biometric data would allow to limit the other data shared with Eurojust and therefore reduce administrative burden on the side of national competent authorities. As some Member States expressed their concern in the consultation process that the regulation would create an obligation to change their national system, the provision does not set out a flat obligation to provide the data. Instead, it only applies where biometric data is available. There is no obligation to change national law to make the information available to the judicial authorities when this is not the case.

[1] This non-paper has not been adopted or endorsed by the European Commission. Any views expressed may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the entities to which it is addressed for the purpose of facilitating discussions and may contain confidential and/or privileged material.

In addition, biometric data would enable synergies with other legislative projects and improve the connectivity of databases in the JHA area. Biometric data is and will be included in the ECRIS-TCN and SIS databases. Eurojust has access to these systems, therefore also needs to be able to process biometric data in order to use these systems effectively. In the context of ECRIS-TCN, Eurojust will be receiving requests from third countries as a contact point and might receive requests containing fingerprint data in that context.

That biometric data is already transmitted to Europol does not replace the need to send the information to Eurojust. Europol cannot fulfil the purpose of the CTR, which is to detect links with other judicial CTR cases. Furthermore, Eurojust will not receive the information directly from Europol. Also, if Eurojust does not receive biometric data in the CTR, (biometric) hits with Europol data will not be possible.

Therefore the Commission proposal opted for the obligatory transmission of biometric data including fingerprints.

II. Alternative 1: obligatory transmission of photographs and optional transmission of fingerprints, incl. strict necessity test

Another option would have been to set out only an obligation to transmit photographs, but to transmit fingerprints only in cases where such data is necessary e.g. as the suspect is not reliably identified.

There are practical and legal differences between photographs and fingerprints. Pictures are usually included in the judicial case file, they are accessible to the judicial authorities and can therefore be easily transmitted to Eurojust's CTR. Moreover, unlike fingerprints, it is also possible to compare photographs without additional technology. Even if photographs were not cross-checked systematically with other photographs to identify new links, they allow to corroborate links based on other identity data. Photographs therefore enable in any case a more accurate review of pre-identified links.

PUBLIC

There is also a substantial difference between photographs and fingerprints in terms of data protection. While fingerprints will always be considered as special category of personal data (Article 76 of Regulation 2018/1725), hence subject to additional appropriate safeguards, the processing of photographs on the other hand, according to recital 29 of the same Regulation should not systematically be considered to be special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

This option would still have allowed to maintain fingerprint and photographs as part of the CTR, but not to cross-check such data systematically and establish links of higher quality as with the Commission proposal.

Therefore, if fingerprint data are not transmitted systematically, it would be necessary to transmit additional information in Annex III to ensure Eurojust has sufficient information to identify links. In particular, telephone numbers, email addresses, place of residence, details of accounts held with banks or other financial institutions and information concerning legal persons associated to the terrorist offence would need to be provided.

This option would have still allowed to create synergies with other legislative initiatives, which are based on biometric data in order to improve the accuracy of identification of suspects, especially in cases involving third country nationals. However, this option was considered less effective and would at the same time not reduce the administrative burden on national authorities as much as the Commission proposal.

Art. 21(3) Eurojust Regulation:

"The information transmitted in accordance with paragraph 1 shall include the operational personal data and non-personal data listed in Annex III. **National competent authorities may provide personal data in accordance with Annex III point d, [subject to a strict necessity test/ if such personal data is necessary to identify a data subject under Art. 27(5) reliably]."**

PUBLIC

"Annex III:

(a) information to identify the suspect, accused, convicted or acquitted person:

surname (family name);
first names (given name, alias);
date of birth;
place of birth (town and country);
nationality or nationalities;
identification document;
gender,
photographs,
place of residence;
telephone numbers;
email addresses;
details on bank accounts held with banks of financial institutions,

(b) information on the terrorist offence:

legal qualification of the offence under national law;
applicable form of serious crime from the list referred to in Annex I;
affiliation with terrorist group;
information concerning legal persons associated to the terrorist offence;
type of terrorism, such as jihadist, separatist, left-wing, right-wing;
brief summary of the case;

(c) information on the national proceedings:

status of the national proceedings;
responsible public prosecutor's office;
case number;
date of opening formal judicial proceedings;
links with other relevant cases;

PUBLIC

(d) **additional** information to identify the suspect~~, where available, for the national competent authorities~~:

- fingerprint data that have been collected in accordance with national law during criminal proceedings.
- ~~photographs~~".

PUBLIC

III. Alternative 2: optional transmission of biometric data and strict necessity test

Another option would have been to introduce only the option to transmit photographs and fingerprints in cases where such data is necessary as the identity of the suspect is not reliably clarified. This might be e.g. in cases involving third country nationals or where alias are used. Again, his would still allow to maintain such data as part of the CTR, but not to cross-check such data systematically and establish links of higher quality as set out under the Commission proposal.

In addition, the information mentioned above would also be needed, if all biometric data are not transmitted systematically. This option would still allow to create synergies with the other legislative initiatives, which are based on biometric data in order to improve the accuracy of identification of suspects, especially in cases involving third country nationals. However, this option was considered less effective and would at the same time not reduce the administrative burden on national authorities as the Commission proposal.

Art. 21(3) Eurojust Regulation:

"The information transmitted in accordance with paragraph 1 shall include the operational personal data and non-personal data listed in Annex III. **National competent authorities may provide personal data in accordance with Annex III point d, [subject to a strict necessity test/ if such personal data is necessary to identify a data subject under Art. 27(5) reliably]."**

"Annex III:

(a) information to identify the suspect, accused, convicted or acquitted person:

surname (family name);
first names (given name, alias);
date of birth;
place of birth (town and country);
nationality or nationalities;

identification document;

gender,

place of residence;

telephone numbers;

email addresses;

details on bank accounts held with banks of financial institutions.

(b) information on the terrorist offence:

legal qualification of the offence under national law;

applicable form of serious crime from the list referred to in Annex I;

affiliation with terrorist group;

information concerning legal persons associated to the terrorist offence;

type of terrorism, such as jihadist, separatist, left-wing, right-wing;

brief summary of the case;

(c) information on the national proceedings:

status of the national proceedings;

responsible public prosecutor's office;

case number;

date of opening formal judicial proceedings;

links with other relevant cases;

(d) **additional** information to identify the suspect, where available, for the national competent authorities:

- fingerprint data that have been collected in accordance with national law during criminal proceedings;
- photographs.".

PUBLIC

IV. Alternative 3: no fingerprints, but maintaining photographs

Finally, the final option considered was to transmit only photographs under Annex III. As set out above, pictures are in almost all cases included in the judicial case file, are accessible to the judicial authorities and can therefore be easily transmitted to Eurojust's CTR. Even without additional technology, they can be used to collaborate potential links and have been used to do so at Eurojust in the past. The additional information set out under Alternative 1 would be even more important.

While this option would have less impact on fundamental rights, it is also much less efficient. The transmission of fingerprint data and photographs would enhance the accuracy of link detection best and also enable the cross-checking functionalities with other agencies and databases, where necessary. In addition, the survey feedback underlined the importance of biometric data to link national investigations and proceedings.

Art. 21(3) Eurojust Regulation:

"The information transmitted in accordance with paragraph 1 shall include the operational personal data and non-personal data listed in Annex III."

"Annex III:

(a) information to identify the suspect, accused, convicted or acquitted person:

- surname (family name);
- first names (given name, alias);
- date of birth;
- place of birth (town and country);
- nationality or nationalities;
- identification document;
- gender;
- **place of residence;**
- **telephone numbers;**
- **email addresses;**

PUBLIC

– **details on bank accounts held with banks of financial institutions;**

– **photographs;**

(b) information on the terrorist offence:

– legal qualification of the offence under national law;

– applicable form of serious crime from the list referred to in Annex I;

– affiliation with terrorist group;

– **information concerning legal persons associated to the terrorist offence;**

– type of terrorism, such as jihadist, separatist, left-wing, right-wing;

– brief summary of the case;

(c) information on the national proceedings:

– status of the national proceedings;

– responsible public prosecutor's office;

– case number;

– date of opening formal judicial proceedings;

– links with other relevant cases.

(d) ~~information to identify the suspect, where available, for the national competent authorities:~~

~~– fingerprint data that have been collected in accordance with national law during criminal proceedings;~~

~~– photographs.".~~"

PUBLIC