Council of the European Union

Brussels, 6 April 2022
(OR. en)

7986/22

Interinstitutional File: 2021/0393(COD)

LIMITE

JAI 463
COPEN 121
EUROJUST 33
CT 63
ENFOPOL 188
COTER 93
CODEC 463

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	7554/22
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 - Revised text by the Presidency

At its meeting on 1 April 2022, the COPEN Working Party resumed the examination of the draft Regulation on the basis of a second revised draft submitted by the Presidency (7554/22).

In the light of the comments presented the Member States and the Commission, the Presidency has revised the draft text, see attached.

Changes compared to the text of the Commission proposal have been indicated by **bold** characters, or by ~~strikethrough~~; new changes that have not yet been discussed are in put in **bold** and underlined characters.

ANNEX

Proposal for a

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 85 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Acting in accordance with the ordinary legislative procedure[1],

Whereas:

(1) Regulation (EU) 2018/1727 of the European Parliament and of the Council[2] established Eurojust and sets out its tasks, competence and functions.

---

1 […].

2 Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (OJ L 295, 21.11.2018, p. 138).

(2) Council Decision 2005/671/JHA[3] sets out that in order to combat terrorism it is essential to have the fullest and most up-to-date information possible. It obliges Member States' competent national authorities to provide Eurojust with information on prosecutions and convictions for terrorist offences, which affect or may affect two or more Member States.

(3) Inconsistencies in the interpretation of Decision 2005/671/JHA cause that information is not shared at the right time, not the appropriate information is shared or information is not shared at all. Eurojust needs to receive sufficient information to identify links between cross-border investigations.

(4) Assisting the competent authorities of the Member States in ensuring the best possible coordination of investigations and prosecutions, including the identification of links, is an important task of Eurojust under Regulation (EU) 2018/1727. It enables Eurojust to take a more proactive approach and provide better services to the Member States, for example suggesting the initiation of investigations, identifying coordination needs, potential cases of *ne bis in idem* and prosecution gaps.

(5) In September 2019, Eurojust has set up the European Judicial Counter-Terrorism Register based on Decision 2005/671/JHA with the specific objective to identify potential links between judicial proceedings against suspects of terrorist offences and possible coordination needs stemming from these.

(6) As the register has been set up after Regulation (EU) 2018/1727 had already been adopted, the European Judicial Counter-Terrorism Register is neither technically well integrated at Eurojust nor legally well integrated in Regulation (EU) 2018/1727. Therefore, it is necessary to remedy that.

---

[3] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences (OJ L 253, 29.09.2005, p. 22).

(7) To combat terrorism effectively, efficient exchange of information for investigation or prosecution of terrorist offences between competent authorities and Union agencies is crucial. It is essential to have the most complete and updated information possible. The persistence of the terrorist threat and the complexity of the phenomenon raise the need for an ever greater exchange of information.

(8) As terrorist organisations are increasingly involved in other forms of serious crimes, such as trafficking in human beings, drug trafficking or money laundering, it is also necessary to cross-check judicial proceedings against such serious crimes.

(9) In order to enable Eurojust to identify cross-links between cross-border judicial proceedings against suspects of terrorist offences as well as cross-links between judicial proceedings against suspects of terrorist offences and information processed at Eurojust relating to other cases of serious crimes, it is essential that Eurojust receives sufficient information to enable Eurojust to cross-check this data.

(10) The competent authorities need to know exactly what kind of information they have to transmit to Eurojust, at what stage of the national proceedings and in which cases, in order to provide such data. This is expected to increase the information Eurojust receives significantly.

(11) Directive (EU) 2017/541 of the European Parliament and of the Council[4] is the reference point for national authorities to define terrorist offences as implemented in national law.

[4] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

(12) For the identification of cross-links between terrorism investigations and judicial proceedings against suspects of terrorist offences, reliable identification data is crucial. Due to the uncertainties regarding alphanumerical data especially for third country nationals, it should be possible to exchange biometric data **when such data, according to national law, are held by or can be transmitted to the competent national authorities**. Due to the sensitive nature of biometric data and the impact processing of biometric data has on the respect for private and family life and the protection of personal data, as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, **these data may only be transmitted in cases where it is necessary for the reliable identification of the data subject.** ~~a strict necessity test should be applied by the competent authorities and Eurojust in each case.~~

(13) As information about existing cross-links to other judicial proceedings is most useful at an early stage of the investigation, it is necessary that the competent authorities provide information to Eurojust as soon as **the case is referred to a judicial authority in accordance with national law** ~~judicial authorities are involved~~. **Depending on the applicable national provisions, the moment where the case is referred to a judicial authority may for example correspond to the moment when such authority is informed of an ongoing investigation, when it authorises or orders an investigation [measure] or when it decides on prosecution.** If the competent national authorities are already aware of cross-links, they should inform Eurojust accordingly.

(14) In order to ensure the accuracy of the data in the European Judicial Counter-Terrorism Register, to identify cross-links early and to ensure time limits are respected, the competent national authorities should **keep the information provided up-to-date** ~~update the information provided regularly~~. Such updates should include new information relating to the person under investigation, judicial decisions such as pre-trial detention or opening of the court proceedings and judicial cooperation requests or identified links with other jurisdictions.

(15) Given the sensitive nature of judicial proceedings against suspects of terrorist offences, it is not always possible for the competent national authorities to share the information on terrorist offences at the earliest stage. Such derogations from the obligation to provide information should remain an exception.

(16) For the purposes of exchanging and processing sensitive data between competent national authorities and Eurojust for protecting such data against unauthorised disclosure and cyber attacks, and without prejudice to future technological developments, secure communication channels, such as the secure communication connections referred to in Article 9 of Council Decision 2008/976/JHA[5] or the decentralised IT system as defined in Regulation (EU) […/…] of the European Parliament and of the Council[6] [*Regulation on the digitalisation of judicial cooperation*] should be used. In order to exchange data securely and protect the integrity of the communication and data exchange, the case management system should be connected to such secure communication systems and meet high cybersecurity standards.

---

5 Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (OJ L 348, 24.12.2008, p. 130).

6 Regulation (EU) […/…] of the European Parliament and of the Council on the digitalisation of judicial cooperation and access to justice in civil, commercial and criminal law cases (OJ L…).

(17) In order to ensure uniform conditions for the implementation of this Regulation as regards the establishment and use of the decentralised IT system for the cases not covered by Regulation (EU) […/…] of the European Parliament and of the Council[7] [*Regulation on the digitalisation of judicial cooperation*], implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[8].

(18) The transmission of unstructured data makes manual intervention necessary, creates additional administrative burden, and reduces the quality of the results of cross-checking. Therefore, national competent authorities should transmit the data in a structured manner while respecting minimal interoperability requirements as defined in the European Interoperability Framework[9]. In addition, the transfer of data should be automated as much as possible to lessen the administrative burden of national authorities and to ensure the necessary data is provided regularly and quickly.

(19) A modernized case management system is necessary for Eurojust to process the sensitive personal data securely. The new system needs to integrate and enable the functionalities of the European Judicial Counter-Terrorism Register and improve the capacities of Eurojust regarding link detection.

---

7 Regulation (EU) […/…] of the European Parliament and of the Council on the digitalisation of judicial cooperation and access to justice in civil, commercial and criminal law cases (OJ L…).

8 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

9 https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework.

(20) It is important to maintain the control and responsibility of the national members for the data, which they receive from the national competent authorities. No operational personal data should be shared with another Member State by default. Operational personal data should only be shared in as far as national competent authorities authorise the exchange of data. In order to digitalise and speed up the follow up on potential links while ensuring full control over the data, handling codes should be introduced.

(21) Terrorist activities **very** often affect two or more Member States. Terrorism already had a strong transnational component in the past. However, with the use and availability of electronic communication, transnational collaboration between terrorist offenders has increased significantly. ~~Therefore, terrorist offences should be considered per se transnational in their nature~~. **However, the transnational character of a terrorist offence might not be known at the moment when the case is referred to a judicial authority. This transnational character may be revealed through the cross-checking by Eurojust. This is why terrorism requires coordination and cooperation between prosecuting authorities or a prosecution on common grounds, as provided for in Article 85 TFEU. As a consequence, information on terrorim cases should be exchanged with Eurojust, unless** ~~if~~ the specific circumstances of the case ~~do not~~ clearly indicate a purely national character.

(22) Investigations and prosecutions in terrorism cases are often impeded by the lack of information exchange between national investigation and prosecution authorities. **Therefore it is necessary to extend the time limits for storing data in the European Judicial Counter-Terrorism Register**. **In addition,** ~~In order to be able~~ **the possibility** to cross check new terrorist investigations also with previous investigations ~~and~~ **may** establish potential links **and that there is a need of cooperation. It can reveal that a person suspected or prosecuted in an oingoing case in a Member State was suspected or prosecuted in a concluded case in another Member State. It may also establish links between ongoing investigations or prosecutions which could have been hidden otherwise. This is also the case when previous investigations ended in a acquittal. This is the reason why** it is necessary to store the data on any previous investigations, not only on convictions ~~and to extend the time limits for storing data in the European Judicial Counter-Terrorism Register~~. However, it is necessary to ensure that such data is processed for prosecution purposes only. The information may not be used for anything else but identifying links with ongoing investigations and prosecutions and for the support of those investigations and prosecutions.[10]

(23) Eurojust has concluded twelve cooperation agreements with third countries, which allow for the transfer of operational personal data and the secondment of a third country liaison prosecutor to Eurojust. Moreover, the Trade and Cooperation Agreement between the European Union and the United Kingdom[11] allows for the secondment of a liaison prosecutor. In March 2021, the Council gave the Commission a mandate[12] to negotiate further cooperation agreements on the cooperation between Eurojust and thirteen further third states.

---

10 This recital may be amended if option 2 of Article 27(5) is chosen.

11 Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (OJ L 149, 30.4.2021, p.10).

12 Council Decision (EU) 2021/7072 of 16 March 2021.

(24) While Regulation (EU) 2018/1727 provides a legal basis for the cooperation and exchange of data with third countries, it does not contain any rules on the formal and technical aspects of the cooperation with third country liaison prosecutors seconded to Eurojust, in particular their access to the case management system. In the interest of legal certainty, Regulation (EU) 2018/1727 should provide an explicit legal basis for the cooperation between Eurojust and the third country liaison prosecutors and their access to the Eurojust case management system. Eurojust should ensure adequate safeguards and security measures for the protection of data and fundamental rights through the technical setup and internal rules.

(25) In the interest of clarity, the relationship between the exchange of information between national competent authorities on terrorism cases with Eurojust under Decision 2005/671/JHA and Regulation (EU) 2018/1727 should be clarified. Therefore, the relevant provisions should be deleted from Decision 2005/671/JHA and be added to Regulation (EU) 2018/1727.

(26) While some Member States' competent national authorities are already connected to secure telecommunication connection as referred to in Article 9 of Council Decision 2008/976/JHA[13], many competent authorities are not yet connected to secure telecommunication connection or secure communication channels. In order to ensure that the Member States have sufficient time to provide such a connection for the competent authorities, a transitional period for implementation should be granted.

[13] Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network, (OJ L 348, 24.12.2008, p. 130).

(27) [In accordance with Articles 1, 2 and 4a(1) of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.] OR [In accordance with Article 3 and Article 4a(1) of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Ireland has notified [, by letter of …,] its wish to take part in the adoption and application of this Regulation.]

(28) In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(29) The European Data Protection Supervisor was consulted in accordance with Article 42 of Regulation (EU) 2018/1725 and delivered an opinion on 26 January 2022,

HAVE ADOPTED THIS REGULATION:

Article 1

Amendments to Regulation (EU) 2018/1727

Regulation (EU) 2017/1727 is amended as follows:

(1) in Article 3, paragraph 5 is replaced by the following:

"5. Eurojust may also assist with investigations and prosecutions that only affect a Member State and a third country or a Member State and an international organisation, provided that a cooperation agreement or arrangement establishing cooperation pursuant to Article 52 has been concluded with that third country or that international organisation, or provided that in a specific case there is an essential interest, in providing such assistance.

The decision whether or not to provide judicial assistance remains solely with the competent authority of the [14] Member State(s) concerned.

(2) Article 20 is amended as follows:

(a) the following paragraph 2a is inserted:

"2a. Each Member State shall designate a competent national authority as Eurojust national correspondent for terrorism matters. This national correspondent for terrorism matters shall be a judicial or other competent authority. Where the national legal system requires, more than one authority can be designated. The national correspondent for terrorism matters shall have access to all relevant information in accordance with Article 21a(1). It shall be competent to collect such information and to send it to Eurojust.";

[14] Clarification inserted further to a suggestion by CZ.

(b) in Article 20(8), the first sentence is replaced by the following:

"In order to meet the objectives referred to in paragraph 7, the persons referred to in paragraph 3, points (a), (b) and (c), shall be connected to the case management system in accordance with this Article and with Articles 23, 24, 25 and 34."

(3) Article 21 is amended as follows:

(a) paragraph 9 is replaced by the following:

"9. This Article shall not affect other obligations regarding the transmission of information to Eurojust.";

(b) paragraph 10 is **replaced by the following** : ~~deleted;~~

"10. The competent national authority shall not be obliged to provide such information where it has already been transmitted to Eurojust in accordance with other provisions of this Regulation.";

(4) the following Article 21a is inserted:

"*Article 21a*

Exchange of information on terrorism cases

1. The competent national authorities shall inform their national members of any ongoing or concluded criminal investigations supervised by judicial authorities, prosecutions, court proceedings and court decisions on terrorist offences as soon as **the case is referred to the judicial authorities, in accordance with national law** ~~judicial authorities are involved~~. **This obligation shall apply to all terrorist offences regardless whether there is a known link to another Member State or a third country, unless the case, due to its specific circumstances, clearly affects only one Member State.**

2. Paragraph 1 shall not apply where :

a) the sharing of information would jeopardise current investigations or the safety of an individual ; or

b) the sharing of information would be contrary to essential interests of the security of the Member State concerned.

3~~2~~. 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*. ~~The obligation referred to in paragraph 1 shall apply to all terrorist offences regardless whether there is a known link to another Member State or third country, unless the case, due to its specific circumstances, clearly affects only one Member State.~~

* Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).";

4~~3~~. 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, if such personal data are held by or can be communicated**[15] **to the competent national authorities in accordance with national law and if their transmission is necessary to identify a data subject under Art. 27(5) reliably.**

[15] Some delegations expressed the wish to delete "or can be communicated to". However, the term is retained because it covers all possible national situations and has no binding consequences for the Member States since the transmission of biometric data is optional.

5~~4~~. **Subject to paragraph 2,** the competent national authorities shall inform their national member without delay about any ~~relevant~~ changes **to the information transmitted under paragraph 1** ~~in the national proceeding~~.

~~Without prejudice to the first subparagraph, the national authorities shall review and provide an update on the information transmitted under paragraph 1 at least every three months.~~

~~5. Paragraph 1 shall not apply where the sharing of information would jeopardise current investigations or the safety of an individual, or when it would be contrary to essential interests of the security of the Member State concerned.~~

6. The competent national authority shall not be obliged to provide such information where it has already been transmitted to Eurojust ~~**in accordance with Decision 2005/671/JHA**~~**.**[16]

_____

[16] The reference to data transmitted in accordance with Council Decision 2005/671/JHA, as previously proposed, has been deleted in order to cover all situations in which data may be transmitted to Eurojust.

(5) the following Articles 22a, 22b and 22c are inserted:

"Article 22a

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

1. The communication between the competent national authorities and Eurojust under this Regulation shall be carried out through the decentralised IT system as defined in Regulation (EU) [.../…] of the European Parliament and of the Council* [*Regulation on the digitalisation of judicial cooperation*].

2. Where exchange of information in accordance with paragraph 1 is not possible due to the unavailability of the decentralised IT system or due to exceptional circumstances, it shall be carried out by the swiftest, most appropriate alternative means. Member States and Eurojust shall ensure that the alternative means of communication are reliable and provide an equivalent level of security.

3. The competent national authorities shall transmit the information in accordance with Articles 21 and 21a to Eurojust in a semi-automated manner from national registers and in a structured way determined by **the Commission, pursuant to Articles 22b and 22c** ~~Eurojust~~.

_____

* [*Regulation (EU) […/…] of the European Parliament and of the Council on the digitalisation of judicial cooperation*](OJ L…).

Article 22b

Adoption of implementing acts by the Commission

1. The Commission shall adopt the implementing acts necessary for the establishment and use of the decentralised IT system for communication under this Regulation, setting out the following:

   (a) the technical specifications defining the methods of communication by electronic means for the purposes of the decentralised IT system;

   (b) the technical specifications for communication protocols;

   (c) the information security objectives and relevant technical measures ensuring minimum information security standards and a high level of cybersecurity standards for the processing and communication of information within the decentralised IT system;

   (d) the minimum availability objectives and possible related technical requirements for the services provided by the decentralised IT system;

   (e) the establishment of a steering committee comprising representatives of the Member States to ensure the operation and maintenance of the decentralised IT system in order to meet the objectives of this Regulation.[17]

2. The implementing acts referred to in paragraph 1 shall be adopted by [*2 years after entry into force*] in accordance with the examination procedure referred to in Article 22c(2).

[17] The Presidency is considering the deletion of this litt. (e), for reasons of consistency with the horizontal proposal on digitalization of judicial cooperation. Delegations are invited to share their opinion, if any.

Article 22c

Committee Procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council*.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

   Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and Article 5(4), third subparagraph, of Regulation (EU) No 182/2011 shall apply.

---

* Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).";

(6) Articles 23, 24 and 25 are replaced by the following :

"*Article 23*

Case Management System

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

2. The purposes of the case management system shall be to:

   (a) support the management and coordination of investigations and prosecutions for which Eurojust is providing assistance;

   (b) ensure secure access to and exchange of information on on-going investigations and prosecutions;

   (c) allow for the cross-checking of information and establishing cross-links;

   (d) allow for the extraction of data for operational and statistical purposes;

   (e) facilitate monitoring to ensure that the processing of operational personal data is lawful and complies with this Regulation and the applicable data protection rules.

3. The case management system may be linked to the secure telecommunications connection referred to in Article 9 of Council Decision 2008/976/JHA* and other secure communication channel(s) in accordance with applicable Union law.

4. In the performance of their duties, national members may process personal data on the individual cases, on which they are working, in accordance with this Regulation or other applicable instruments.

   They shall allow the Data Protection Officer to have access to the personal data processed in the case management system.

5. For the processing of operational personal data, Eurojust may not establish any automated data file other than the case management system.

The national members may, however, temporarily store and analyse personal data for the purpose of determining whether such data are relevant to Eurojust's tasks and can be included in **the case management system** ~~operational data management system~~. That data may be held for up to three months.

Article 24

Management of the information in the case management system

1. The national member shall store the information transmitted to him or her in accordance with this Regulation or other applicable instruments in the case management system.

The national member shall be responsible for the management of the data processed by that national member.

2. The national member shall decide, on a case-by-case basis, whether to keep access to the information restricted or to give access to it or to parts of it to other national members, to liaison prosecutors seconded to Eurojust, to authorised Eurojust staff or to any other person working on behalf of Eurojust who has received the necessary authorisation from the Administrative Director.

3. The national member shall indicate, in general or specific terms, any restrictions on the further handling, access and transfer of the information if a cross-link referred to in Article 23(2), point (c), has been identified.

Article 25

Access to the case management system at national level

1. **Persons referred to in Article 20(3), points (a), (b) and (c), shall at most have access to:** ~~In so far as they are connected to the case management system, persons referred to in Article 20(3) shall only have access to:~~

   (a) data controlled by the national member of their Member State~~, unless the national member, who has decided to introduce the data in the case management system, expressly denied such access~~;

   (b) data controlled by national members of other Member States and to which the national member of their Member State has received access, unless the national member who controls the data ~~expressly~~ denied such access.

2. The national member shall, within the limitations provided for in paragraph 1 of this Article, decide on the extent of access, which is granted to the persons referred to in Article 20(3)**, points (a), (b) and (c), in their Member State** ~~in so far as they are connected to the case management system~~.

3. Data provided in accordance with Article 21a may only be accessed at national level by national correspondents for Eurojust in terrorism matters as referred to in Article 20(3), point (c).

4. Each Member State may decide, after consultation with its national member, that persons referred to in Article 20(3), points (a), (b) and (c), may, within the limitations provided for in paragraphs 1 to 3, enter information in the case management system concerning their Member State. Such contribution shall be subject to the validation by the respective national member. The College shall lay down the details of the practical implementation. Member States shall notify Eurojust and the Commission of their decision regarding the implementation of this paragraph. The Commission shall inform the other Member States thereof.

~~3. Each Member State shall decide, after consultation with its national member, on the extent of access, which is granted in that Member State to the persons referred to in Article 20(3) in so far as they are connected to the case management system.~~

~~Member States shall notify Eurojust and the Commission of their decision regarding the implementation of the first subparagraph. The Commission shall inform the other Member States thereof.~~

_____

* Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (OJ L 348, 24.12.2008, p. 130).";

(7) Article 27 is amended as follows:

(a) paragraph 4 is replaced by the following:

"4. Eurojust may process special categories of operational personal data in accordance with Article 76 of Regulation (EU) 2018/1725. Where such other data refer to witnesses or victims within the meaning of paragraph 2 of this Article, the decision to process them shall be taken by the national members concerned.";

(b) the following paragraph 5 is added:

"5. Where operational personal data is transmitted in accordance with Article 21a, Eurojust may process the operational personal data listed in Annex III of the following persons:

(a) persons to whom, in accordance with the national law of the Member State concerned, there are serious grounds for believing that they have committed or are about to commit a criminal offence in respect of which Eurojust is competent;

(b) persons who have been convicted of such offence.

[18] OPTION 1 : Furthermore, Eurojust may continue to process the operational personal data related to an acquitted person, in order to identify cross-links between the proceedings concluded by an acquittal and other ongoing or future investigations or prosecutions.[19]

---

18 During the Working Party of 1 April 2022, a very slight preference for option 1 was noted by the Presidency. But some delegations were not represented and some others put a scrutiny reservation. For this reason, the position of the Working Party was particularly unclear. The Presidency feels the need to discuss again about the two proposed options. If needed, a tour de table will be organized during the meeting on 11 April.

19 The proposed modifications have several objectives. The first one is to focus exclusively on the data of acquitted persons. In case where proceedings are concluded for another reason, the current rules are not supposed to be modified. However, some delegations indicated that a judicial decision not to prosecute should be treated like an acquittal decision. There is a common point between both decisions, the lack of evidence. But while each acquittal decision may become final, this is not always the case for a decision not to prosecute. For instance, in some legal orders, the public ministry can withdraw at any time its decision not to prosecute. In accordance with article 29, in case of an acquittal, the data have to be deleted when the decision becomes final. The absence of the final character of at least certain decisions not to prosecute might therefore impede the application of the same rules for these decisions as for acquittal decisions. This questions merits further reflections and the delegations are invited to share their views.
The second one is to make it clearer that an acquitted person is presumed to be innocent. Therefore the reference to point (a) has been deleted.
The third one is to identify with more precision the cases where it might be useful to allow a cross-checking of information with data related to an acquitted person. The proposed text allows for the cross-checking of data only with ongoing investigations or prosecutions. In the Commission's proposal, the cross-checking of information with other concluded investigations and prosecutions was also permitted. But it was not in line with recital 22 where it is indicated that "the information may not be used for anything else but identifying links with ongoing investigations and prosecutions and for the support of those investigations and prosecutions". In this way, it is clearer in the text that the goal of processing of data related to acquitted person is only to reveal a possible coordination need between the Member States concerned, without affecting the presumption of innocence.

OPTION 2: Furthermore, Eurojust may be authorised by the competent national authority to continue to process the operational personal data related to an acquitted person, if there is a need for the cross-checking of information and establishing cross-links between the proceedings concluded by an acquittal and other ongoing or future investigations or prosecutions.[20]

The previous subparagraph also applies to the operational personal data related to a person who has been the subject of a final decision of non prosecution.[21]

~~Eurojust may continue to process the operational personal data referred to in point (a) of the first subparagraph also after the proceedings have been concluded under the national law of the Member State concerned, even in case of an acquittal. Where the proceedings did not result in a conviction, processing of personal data may only take place in order to identify links with other ongoing or concluded investigations and prosecutions as referred to in Article 23(2), point (c).";~~

[20] The difference with the first option is that the possibility to process data of acquitted persons is not automatic but subject to the evaluation of a need on a case-by-case basis. This option 2 stresses the exceptional character of the processing of such data and allows flexibility to each Member State according to the specificities of its criminal procedure and each case. In particular, the grounds for the acquittal (lack of evidence or proof of innocence) may be taken into account by the national member in his assessment.

[21] Some delegations expressed the wish to specify that the treatment reserved for data of acquitted persons would also be applied to data of persons who are the subject of a decision not to prosecute. The proposed addition would complete option 1 or option 2. The Presidency would like underline that, according to the current rules, deriving from art. 27 §1, Eurojust is not prevented to continue to process the data after a final decision not to prosecute. If this addition is made, an *a contrario* interpretation might come to the conclusion that for the data processed under art. 27 §1, Eurojust is not allowed to process the data after a final decision not to prosecute.

(8) Article 29 is amended as follows:

(a) the following paragraph 1a is inserted:

"1a. Eurojust shall not store operational personal data transmitted in accordance with Article 21a beyond the first applicable date among the following dates:

(a) the date on which prosecution is barred under the statute of limitations of all the Member States concerned by the investigation and prosecutions;

(b) 5 years after the date on which the judicial decision of the last of the Member States concerned by the investigation or prosecution became final, **[3][22]** years in case of an acquittal[23].

OR

(b) the date on which Eurojust is informed that the person has been acquitted and the judicial decision became final if Eurojust is not authorised by the competent national authority to continue to process the operational personal data related to an acquitted person pursuant to article 27 §5 ; [3] years after the date on which the judicial decision became final if Eurojust authorised by the competent national authority to continue to process the operational personal data related to an acquitted person pursuant to article 27 §5 ; the Member State concerned shall inform Eurojust accordingly without delay after the decision became final ;

(c) 5 years after the date on which the judicial decision of the last of the Member States concerned by the investigation or prosecution became final.[24]

---

22 Some delegations indicated that they were considering a shorter deadline.
23 If option 1 is retained for article 27(5).
24 If option 2 is retained.

(b) paragraphs 2 and 3 are replaced by the following:

"2. Observance of the storage deadlines referred to in paragraphs 1 and 1a of this Article shall be reviewed constantly by appropriate automated processing conducted by Eurojust, particularly from the moment in which Eurojust ceases to provide support.

A review of the need to store the data shall also be carried out every three years after they were entered.

If operational personal data referred to in Article 27(4) are stored for a period exceeding five years, the EDPS shall be informed thereof.

3. Before one of the storage deadlines referred to in paragraphs 1 and 1a expires, Eurojust shall review the need for the continued storage of the operational personal data where and as long as this is necessary to perform its tasks.

It may decide by way of derogation to store those data until the following review. The reasons for the continued storage shall be justified and recorded. If no decision is taken on the continued storage of operational personal data at the time of the review, those data shall be deleted automatically.";

(9) in Section III, the following Article 54a is inserted:

"*Article 54a*

Third country liaison prosecutors

1. A liaison prosecutor from a third country may be seconded to Eurojust based on a cooperation agreement concluded before 12 December 2019 between Eurojust and that third country or an international agreement between the Union and the third country pursuant to Article 218 TFEU allowing for the secondment of a liaison prosecutor.

2. The rights and obligations of the liaison prosecutor shall be set out in the cooperation agreement or international agreement referred to in paragraph 1 or working arrangement concluded in accordance with Article 47(3).

3. Liaison prosecutors seconded to Eurojust shall be granted access to the case management system for the secure exchange of data.

Transfers of operational personal data to third country liaison prosecutors through the case management system may only take place under the rules and conditions set out in this Regulation, the agreement with the respective country or other applicable legal instruments.

Article 24(1), the second sentence and Article 24(2) shall apply *mutatis mutandis* to liaison prosecutors.

The College shall lay down the detailed conditions of access.";

(10) In Article 80, the following paragraphs 8, 9 and 10 are added:

"8. Eurojust may continue to use the case management system composed of temporary work files and of an index until [*the first day of the month following the period of two years after the adoption of this Regulation*], if the new case management system is not in place yet.

9. The competent authorities and Eurojust may continue to use other channels of communication than referred to in Article 22a(1) until [*the first day of the month following the period of two years after the adoption of the implementing act referred to in Article 22b of this Regulation*], if those channels of communication are not available for direct exchange between them yet.

10. The competent authorities may continue to provide information in other ways than semi-automatically in accordance with Article 22a(3) until [*the first day of the month following the period of two years after the adoption of the implementing act referred to in Article 22b of this Regulation*], if the technical requirements are not in place yet.";

(11) the following Annex III is added:

"Annex III:

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

For a natural person :

– surname (family name);

– first names (given name, ~~**alias**~~)

– **alias;**

– date of birth;

– place of birth (town and country);

– nationality or nationalities;

– identification document,

– gender;

– **place of residence;**

For a legal person :[25]

[25] In the previous draft proposal, it was proposed under litt. b of annex III to transmit "*information concerning legal persons associated to the terrorist offence*". Several delegations stressed the broad and imprecise nature of this wording. The proposal has been made to transmit the information only in cases where the legal person is "*directly*" associated to the terrorist offence. This wording could be interpreted as providing for the transmission of information when the legal person itself is suspected, prosecuted or convicted. Several delegations and the Commission indicated that it would be appropriate to provide for the disclosure of information relating to the legal persons involved. Therefore the presidency suggests to add information concerning such legal persons under litt. a.

– **business name;**

– **legal form;**

– **place of head office;**

For both :

– **telephone numbers;**

– **email addresses;**

– **details on bank accounts held with banks ~~of~~ or 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;**~~[26]

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

– brief summary of the case;

[26] It is proposed to delete this indent, as a consequence of the addition of a reference to legal persons in point (a). The consequence of the deletion would be that information relating to a legal person involved in the terrorist offence without being investigated or procesuted or without having committed an offence would not be transmitted. Delegations are invited to indicate whether they agree.

(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.".

Article 2

Amendments to Decision 2005/671/JHA

Decision 2005/671/JHA is amended as follows:

(1) in Article 1 point (c) is deleted.

(2) Article 2 is amended as follows:

(a) paragraph 2 is deleted;

(b) paragraph 3 is replaced by the following:

"3. Each Member State shall take the necessary measures to ensure that at least the information referred to in paragraph 4 concerning criminal investigations for terrorist offences which affect or may affect two or more Member States, gathered by the relevant authority, is transmitted to Europol, in accordance with national law and with Regulation (EU) 2016/794 of the European Parliament and of the Council *.[27]

_____

* Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) (OJ L 135, 24.5.2016, p. 53).";

(c) paragraph 5 is deleted.

Article 3

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

---

[27] It will be necessary to ensure that this Regulation enters into force before the Directive amending Council Decision 2005/671/JHA as regards its compliance with the Union's rules on the protection of personal data. This Directive will indeed amend the 2005 Decision on the basis of this new version of Article 2.