



Brussels, 16 February 2023  
(OR. en)

6502/23

---

---

**Interinstitutional File:**  
**2021/0393(COD)**

---

---

COPEN 40  
EUROJUST 2  
CT 24  
ENFOPOL 70  
COTER 33  
JAI 171  
CODEC 199

**NOTE**

---

From:	General Secretariat of the Council
To:	Delegations

---

No. prev. doc.:	16095/22 + 16096/22
No. Cion doc.:	14458/21 + ADD 1

---

Subject:	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 - Letter sent to the European Parliament
----------	---

---

At its meeting on 20 December 2022, the Permanent Representatives Committee (Part 2)

- a) confirmed the agreement on the compromise text of the above-mentioned draft Regulation, as it was reached between the negotiating parties on 14 December 2022 and as it is contained in 16096/22; and
- b) authorised the Presidency to address the habitual offer letter to the European Parliament.

The letter as it was sent to the European Parliament is set out in the Annex.

This information is provided in accordance with point 1 h) of note 9493/20 on ‘Strengthening legislative transparency’.



**Council of the European Union**  
General Secretariat

SGS 22 / 05981

Brussels, 20 December 2022

Mr. Juan Fernando López Aguilar  
Chair of the Committee on Civil Liberties, Justice and Home Affairs  
European Parliament  
Bât. ALTIERO SPINELLI  
14G305  
60, rue Wiertz / Wiertzstraat 60  
B-1047 BRUSSELS

**Subject:** 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

Dear Mr. López Aguilar,

Following the informal meeting between the representatives of the three institutions, a draft compromise text was agreed by the Permanent Representatives Committee today.

I am therefore now in a position to confirm that, should the European Parliament adopt its position at first reading, in accordance with Article 294 paragraph 3 of the Treaty, in the form of the text set out in the Annex to this letter (subject to revision by the lawyer-linguists of both institutions), the Council would, in accordance with Article 294, paragraph 4 of the Treaty, approve the European Parliament's position and the act shall be adopted in the wording which corresponds to the European Parliament's position.

On behalf of the Council I wish to thank you for your close cooperation, which should enable us to reach agreement on this file at first reading.

Yours faithfully,

E. HRDÁ  
Chair of the  
Permanent Representatives Committee

Copy: Mr Didier Reynders, Member of the European Commission  
Mr Patryk Jaki, Rapporteur for the European Parliament

Rue de la Loi/Wetstraat 175 - B-1048 Bruxelles/Brussel - Belgique/België  
Tel. +32 2 281 54.83 - [www.consilium.europa.eu](http://www.consilium.europa.eu)



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<sup>1</sup>,

Whereas:

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

---

<sup>1</sup> [...].

<sup>2</sup> 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<sup>3</sup> 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.

<sup>3</sup> 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.
- (8) Terrorist organisations are increasingly involved in other forms of serious crimes, and often form part of organised networks. This concerns serious crimes such as trafficking in human beings, drug trafficking, financial crime and money laundering. It is therefore 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 from the competent authorities as soon as possible, in accordance with the relevant provisions of this Regulation, the information that is necessary to enable Eurojust to cross-check this data and to identify those cross-links.
- (10) The competent authorities need to know exactly what kind of information they have to transmit to Eurojust, at what stage of the national criminal proceedings and in which cases, in order to provide such data. The competent national authorities should transmit information to Eurojust in a structured, organised, systematic and semi-automated manner. A semi-automated manner is one in which the mode used to transmit information is partly automated and partly controlled by a human. This is expected to significantly increase the quality and relevance of the information Eurojust receives.
- (10a) Sharing, storing and cross-checking data will significantly increase the amount of data processed at Eurojust. These elements should be taken into account when determining, within the habitual procedures and frameworks, the financial, human and technical resources that Eurojust needs.

- (11) Directive (EU) 2017/541 of the European Parliament and of the Council<sup>4</sup> is the reference point for national authorities to define terrorist offences as implemented in national law.
- (12) The exchange of reliable identification data is crucial for the identification of cross-links between terrorism investigations and judicial proceedings against suspects of terrorist offences, as well as to possess and store a set of data that ensures that individuals that are subject to such terrorism investigations or judicial proceedings can reliably be identified. The use of biometric data is therefore important, taking into account the uncertainties regarding alphanumerical data, especially for third country nationals, the fact that suspects sometimes use fake and double identities, and that such data are often the only link to suspects in the investigative phase. Therefore, where, under national law on criminal proceedings or on procedural rights in criminal proceedings, the competent national authorities store and collect biometric data and are permitted to transmit them, they should be able to exchange such data, when available, with Eurojust. 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, such data should be transmitted in a way that strictly complies with the principles of necessity, proportionality and purpose limitation and only for the purpose of identifying individuals that are subject to criminal proceedings related to terrorism offences.

---

<sup>4</sup> 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).

- (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. A case should be considered to have been referred to a judicial authority where, for instance, the judicial authority is informed of an ongoing investigation, approves or orders an investigation measure, or decides to prosecute, depending on the applicable national law. If a competent national authority is already aware of cross-links between criminal proceedings in its Member State and the criminal proceedings in another Member State, it should inform Eurojust accordingly.
- (13a) Taking into account the fact that in some legal traditions and systems of the Member States a judicial authority does not supervise investigations and is only involved at later stages of proceedings, nothing in this Regulation should prevent competent national authorities from providing information on terrorism investigations to their national members at Eurojust already at an earlier stage in accordance with their national law.
- (14) In order to ensure the accuracy of the data in the European Judicial Counter-Terrorism Register, to identify cross-links or ascertain the identity of a suspect as early as possible in an investigation and to ensure time limits are respected, the competent national authorities should provide updated information. Such updates should include new information relating to the person under investigation, judicial decisions such as pre-trial detention, opening of the court proceedings, acquittals and final decisions not to prosecute, as well as judicial cooperation requests or identified links with other jurisdictions.



- (15) The competent national authorities should not be obliged to share information on terrorist offences with Eurojust at the earliest stage where it would jeopardise ongoing investigations or the safety of an individual or where it would be contrary to essential interests of the security of the Member State concerned. Such derogations from the obligation to provide information should only be applied in exceptional circumstances and on a case-by-case basis. When considering whether or not to derogate from that obligation, due account should be taken of the fact that Eurojust treats the information provided by national authorities in compliance with Union law on data protection while also considering the confidentiality of the judicial proceedings.
- (16) For the purposes of exchanging and processing sensitive data between competent national authorities and Eurojust, and 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 Council Decision 2008/976/JHA or a decentralised IT system should be used.
- (16a) 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. Such secure communication channels may also be used to connect the case management system with other EU information systems to the extent that the legal acts establishing those systems provide for access by Eurojust.
- (16b) The decentralised IT system should enable secure data exchanges between competent national authorities and Eurojust, without any of the Union institutions being involved in the substance of those exchanges. The decentralised IT system should be comprised of IT back-end systems of Member States and Eurojust, and interoperable access points, through which they are interconnected. The access points of the decentralised IT system should be based on e-CODEX.

- (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 covered by this Regulation, 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.<sup>5</sup>
- (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<sup>6</sup>. 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 the detection of cross-links while taking, as a rule, full advantage of mechanisms for comparing biometric data which already exist and are already in place at national and Union level.
- (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.

<sup>5</sup> 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).

<sup>6</sup> <https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework>.

- (21) Present-day terrorism and serious and organised crime are very dynamic and globalised phenomena, often affecting 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. The transnational character of a terrorist offence might not be known at the moment at which the case is referred to a judicial authority. Nevertheless, it is possible for the transnational character of a terrorist offence to be revealed by Eurojust cross-checking data. The investigation or prosecution of terrorist offences therefore requires coordination and cooperation between prosecuting authorities or a prosecution on common bases, as provided for in Article 85 TFEU. Information on terrorism cases should be exchanged with Eurojust in a timely manner, unless the specific circumstances of the case 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. In order to be able to cross check new terrorist investigations also with previous investigations and establish potential links, it is necessary to ensure that a retention period for data on any previous investigations and convictions is adequate for operational activities. Therefore, it is necessary to extend the time limits for storing data in the European Judicial Counter-Terrorism Register. The possibility to cross-check new terrorist investigations also with previous investigations could establish potential links and entail the need for cooperation. Such cross-checking might reveal that a person suspected or prosecuted in an ongoing case in a Member State was suspected or prosecuted in a case that has been concluded in another Member State. It might also establish links between ongoing investigations or prosecutions which could have been otherwise hidden. That is the case even where previous investigations ended in an acquittal or in a final decision not to prosecute. It is therefore necessary to store the data on any previous investigations where appropriate, not only on convictions.

- (22a) 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. Unless the competent national authority decides otherwise, on a case-by-case basis, Eurojust should be able to continue to process such operational data. Where, after the decision to acquit or not to prosecute becomes final, the competent national authority decides that it is not necessary to process the data of acquitted or non-prosecuted persons, including due to the specificities of the case or due to the grounds for the acquittal or non-prosecution, that data should be deleted.
- (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<sup>7</sup> allows for the secondment of a liaison prosecutor. In March 2021, the Council gave the Commission a mandate<sup>8</sup> to negotiate further cooperation agreements on the cooperation between Eurojust and thirteen further third states.

<sup>7</sup> 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).

<sup>8</sup> 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 implement adequate safeguards and security measures for the protection of data and fundamental rights through the updated technical setup and strict internal rules.
- (24a) When processing personal operational data in accordance with this Regulation, Eurojust should ensure a high level of data protection. For the processing of operational personal data, Eurojust is subject to Article 3 and Chapter IX of Regulation (EU) 2018/1725, as well as specific rules on processing of operational data provided for in Regulation (EU) 2018/1727 as amended by Regulation (EU) 2022/838 and this Regulation. These provisions apply to the processing of all operational personal data processed by Eurojust. In particular, they apply to all operational personal data processed in the case management system, whether they are processed by national members, national correspondents, liaison prosecutors or other authorised persons in accordance with Regulation (EU) 2018/1727.
- (24b) Decisions on whether and how Eurojust should support the coordination and cooperation between investigating and prosecuting authorities should remain solely with the competent authorities of the Member State(s) concerned, subject to applicable national law, international law, comprising conventions or other international agreements on mutual assistance in criminal matters, or Union law.
- (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<sup>9</sup>, 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.
- (27) In accordance with Articles 1 and 2 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 (TEU) and the Treaty on the Functioning of the European Union (TFEU), 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.
- (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:

---

<sup>9</sup> Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network, (OJ L 348, 24.12.2008, p. 130).

*Article 1*

**Amendments to Regulation (EU) 2018/1727**

Regulation (EU) 2018/1727 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 and how to provide judicial assistance remains solely with the competent authority of the Member State(s) concerned, subject to applicable national, international or Union law.”

(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, in compliance with national and Union law, in particular national criminal procedural law and applicable data protection rules.”;

(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:

“10. The competent national authorities shall not be obliged to provide information as referred to in this Article 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, in particular national criminal procedural law. That obligation shall 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.
2. Paragraph 1 shall not apply where:
  - (a) the sharing of information would jeopardise a current investigation or the safety of an individual; or
  - (b) the sharing of information would be contrary to essential security interests of the Member State concerned.

3. 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\*.

\* 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. The information transmitted in accordance with paragraph 1 shall include the operational personal data and non-personal data listed in Annex III. That information may only include personal data in accordance with Annex III, point d, if such personal data are held by or can be communicated to the competent national authorities in accordance with national law and if their transmission is necessary to identify reliably a data subject under Article 27(5).
5. Subject to paragraph 2, the competent national authorities shall inform their national member without undue delay about any changes to the information transmitted under paragraph 1 and, if possible, no later than 10 working days after the relevant change.
6. The competent national authority shall not be obliged to provide such information where it has already been transmitted to Eurojust.
7. The national competent authority may at any stage request the support of Eurojust in the follow-up action as regards cross-links identified on the basis of information provided under this Article.”

- (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. The case management system referred to in Article 23 of this Regulation shall be connected with the decentralised IT system.
2. The decentralised IT system means a network of IT systems and interoperable e-CODEX access points, operating under the individual responsibility and management of each Member State and Eurojust that enables the secure and reliable cross-border exchange of information.
3. 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 and data protection.
4. The competent national authorities shall transmit the information referred to in Articles 21 and 21a to Eurojust in a semi-automated manner from national registers and in a structured way, which shall be determined by the Commission, in consultation with Eurojust, in an implementing act, in accordance with Article 22b. In particular, that implementing act shall determine the format of the data transmitted pursuant to Annex III, point d and the necessary technical standards with respect to transmitting such data, as well as setting out the digital procedural standards as defined in Article 3(9) of Regulation (EU) 2022/850.

5. The Commission shall be responsible for the creation, maintenance and development of reference implementation software which Member States and Eurojust may choose to apply as their back-end system. This reference implementation software should be based on a modular setup, meaning that the software is packaged and delivered separately from the e-CODEX components needed to connect it to the decentralised IT system. This setup should enable Member States to reuse or enhance their existing national judicial communication infrastructures for the purpose of cross-border use and Eurojust to connect its case management system to the decentralized IT system.
6. The Commission shall provide, maintain and support on a free-of-charge basis the reference implementation software. The creation, maintenance and development of the reference implementation software shall be financed from the general budget of the Union.
7. Member States and Eurojust shall bear their respective costs for establishing and operating an authorised e-CODEX access point as defined in Article 3(3) of Regulation (EU) 2022/850 of the European Parliament and of the Council, and for establishing and adjusting their relevant IT systems to make them interoperable with the access points.

*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.
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).

#### *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.
- 3a. Where Eurojust has been granted access to data in or from other EU IT systems established under other Union legal acts, it may use the case management system to access data in or to connect to such IT systems for the purpose of retrieving and processing information, including personal data, provided that it is necessary for the performance of its tasks and is in line with the Union legal acts establishing such IT systems.

- 3b. Paragraphs 3 and (3a) do not extend the access rights granted to Eurojust to other EU information systems under the respective Union legal acts.
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. 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 consultation with the national authorities, 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:
  - (a) data controlled by the national member of their Member State,
  - (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 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.
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.

\* 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.

Unless the competent national authority decides otherwise, on a case-by-case basis, 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 shall take place only in order to identify cross-links between ongoing, future or concluded investigations and prosecutions as referred to in Article 23(2), point (c). That also applies to operational personal data related to a person who has been the subject of 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) five years after the date on which the judicial decision of the last of the Member States concerned by the investigation or prosecution became final; this time-period shall be two years in the case of an acquittal or final decision not to prosecute;
- (c) the date on which Eurojust is informed of the decision of the competent national authority pursuant to Article 27(5)”;

(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. In accordance with Articles 45 and 46, Eurojust shall remain liable for the processing of personal data by liaison prosecutors in the case management system

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 9, 10 and 11 are added:

- “9. 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.
10. 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.
11. 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;
- date of birth;
- place of birth (town and country);
- nationality or nationalities;
- identification document (type and number);
- gender;
- place of residence;

For a legal person:

- business name;
- legal form;
- place of head office;

For both:

- telephone numbers;
- email addresses;
- details of bank accounts held with banks or financial institutions;

(b) information on the terrorist offence:

- information concerning legal persons involved in the preparation or commission of a 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;
  - type of terrorism, such as jihadist, separatist, left-wing or 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:
- 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 \*.

---

\* 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*  
*The President*

*For the Council*  
*The President*