Official Journal
of the European Union

EN
L series

2023/2131

11.10.2023

REGULATION (EU) 2023/2131 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 4 October 2023

amending Regulation (EU) 2018/1727 of the European Parliament and of the Council and Council Decision 2005/671/JHA, as regards 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.

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

(3) As a result of inconsistencies in the interpretation of Decision 2005/671/JHA, in some cases the information is not shared in a timely manner, information is not shared at all, or not all relevant information is shared. 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 between such investigations and prosecutions, is an important task of Eurojust under Regulation (EU) 2018/1727. That Regulation enables Eurojust to take a more proactive approach and to provide better services to the Member States, for example by suggesting the initiation of investigations and identifying coordination needs, cases that potentially breach the principle of *ne bis in idem* and prosecution gaps.

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

(6) The European Judicial Counter-Terrorism Register was set up after the adoption of Regulation (EU) 2018/1727, and consequently that Register is not well-integrated in the technical infrastructure of Eurojust, nor is that Register referred to in Regulation (EU) 2018/1727. Therefore, it is necessary to remedy that situation.

(7) To combat terrorism effectively, efficient exchange of information for the investigation or prosecution of terrorist offences between competent national authorities and Union agencies is crucial. It is essential to have the most complete and up-to-date information possible.

([1]) Position of the European Parliament of 12 July 2023 (not yet published in the Official Journal) and decision of the Council of 18 September 2023.

([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).

([3]) Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences (OJ L 253, 29.9.2005, p. 22).

(8) Terrorist organisations are increasingly involved in other forms of serious crime and often form part of organised networks. Such involvement concerns serious crimes such as trafficking in human beings, drug trafficking, financial crime and money laundering. It is necessary to cross-check judicial proceedings against such serious crimes.

(9) In order to enable Eurojust to identify links between cross-border judicial proceedings against suspects of terrorist offences as well as 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 receive from the competent national authorities as soon as possible, in accordance with the relevant provisions of this Regulation, the information that is necessary to enable Eurojust to identify those links by means of cross-checks.

(10) In order to provide data to Eurojust, competent national authorities need to know exactly what kind of information they have to transmit, at what stage of the national criminal proceedings and in which cases. 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 under human control. That manner of transmission is expected to significantly increase the quality and relevance of the information Eurojust receives.

(11) Sharing, storing and cross-checking data will significantly increase the amount of data processed by Eurojust. Those elements should be taken into account when determining, within the existing procedures and frameworks, the financial, human and technical resources required by Eurojust.

(12) Directive (EU) 2017/541 of the European Parliament and of the Council ([4]), as transposed into national law, is the reference point for competent national authorities to define terrorist offences.

(13) It is crucial to exchange reliable identification data in order for Eurojust to identify links between terrorism investigations and judicial proceedings against suspects of terrorist offences. It is also crucial for Eurojust to possess and store a set of data that ensures that individuals 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 or double identities, and that biometric 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, those authorities should be able to exchange such data, when available, with Eurojust. Due to the sensitive nature of biometric data and the impact that 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.

(14) As information about existing links to other judicial proceedings is most useful at an early stage of the investigation, it is necessary that the competent national 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 links between criminal proceedings in its Member State and criminal proceedings in another Member State, it should inform Eurojust accordingly.

([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).

(15) Taking into account the fact that in some Member States' legal traditions and systems a judicial authority does not supervise investigations and is only involved at later stages of proceedings, this Regulation should not prevent competent national authorities from providing information on terrorism investigations to their national members at an earlier stage in accordance with their national law.

(16) In order to ensure the accuracy of the data in the European Judicial Counter-Terrorism Register, to identify links or ascertain the identity of a suspect as early as possible in an investigation and to ensure that time limits are respected, the competent national authorities should update the information they have provided. Such updates should include new information relating to the person under investigation, judicial decisions such as pre-trial detention, opening of court proceedings, acquittals and final decisions not to prosecute, as well as judicial cooperation requests or identified links with other jurisdictions.

(17) The competent national authorities should not be obliged to share information on terrorist offences with Eurojust at the earliest stage where doing so would jeopardise ongoing investigations or the safety of an individual or be contrary to essential interests of the security of the Member State concerned. Such derogations from the obligation to share 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, competent national authorities should take due account of the fact that Eurojust treats the information provided by such authorities in compliance with Union law on data protection, and of the confidentiality of the judicial proceedings.

(18) For the purposes of exchanging sensitive data between competent national authorities and Eurojust and of processing such data, secure communication channels, such as a decentralised IT system or the secure telecommunications connection referred to in Council Decision 2008/976/JHA ([5]), should be used in order to protect such data against unauthorised disclosure and cyber attacks. Such use should be without prejudice to future technological developments.

(19) In order to exchange data securely and protect the integrity of the communication and data exchange, the case management system should be connected to secure communication channels and meet high cybersecurity standards. Such secure communication channels may also be used to connect the case management system with other Union information systems to the extent that the legal acts establishing those systems provide for access by Eurojust.

(20) The decentralised IT system should enable secure data exchanges between competent national authorities and Eurojust, without any Union institution, body, office or agency being involved in the substance of such exchanges. The decentralised IT system should be comprised of IT back-end systems of Member States and Eurojust that are interconnected by interoperable access points. The access points of the decentralised IT system should be based on e-CODEX.

(21) In order to ensure uniform conditions for the implementation of this Regulation as regards the establishment and use of the decentralised IT system for 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 ([6]).

(22) The transmission of unstructured data makes manual intervention necessary, creates additional administrative burden and reduces the quality of the results of cross-checking. Therefore, competent national authorities should transmit data in a structured manner while complying with minimal interoperability requirements as defined in the European Interoperability Framework referred to in the Commission Communication of 23 March 2017 entitled 'European Interoperability Framework – Implementation Strategy'. In addition, the transfer of data should be automated as much as possible to lessen the administrative burden on competent national authorities and to ensure that the necessary data are provided regularly and quickly.

([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) 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).

(23) A modernised case management system is necessary for Eurojust to process sensitive personal data securely. The new system needs to integrate and enable the functionalities of the European Judicial Counter-Terrorism Register and improve Eurojust's ability to identify links while taking, as a rule, full advantage of existing national and Union mechanisms for comparing biometric data.

(24) It is important to maintain the control and responsibility of the national members for the data which they receive from the competent national authorities. No operational personal data should be shared with another Member State by default. Operational personal data should only be shared in so far as competent national 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.

(25) Present-day terrorism and serious and organised crime are very dynamic and globalised phenomena, often affecting two or more Member States. Although terrorism already had a strong transnational component, the use and availability of electronic communication means that transnational collaboration between terrorist offenders has increased significantly. The transnational character of a terrorist offence may not be known when the case is referred to a judicial authority but it might be revealed during the cross-checking of data by Eurojust. 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 of the Treaty on the Functioning of the European Union (TFEU). Information on terrorism cases should be exchanged with Eurojust in a timely manner, unless the specific circumstances of the case clearly indicate that it has a purely national character.

(26) 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 with previous investigations and identify potential links, it is necessary to ensure that the 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.

(27) The possibility to cross-check new terrorist investigations with previous investigations could identify 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 concluded in another Member State. It might also identify links between ongoing investigations or prosecutions which could otherwise have been 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 data on any previous investigations where appropriate, not only on convictions.

(28) It is necessary to ensure that data from investigations that ended in an acquittal or in a final decision not to prosecute are processed for prosecution purposes only. Such data may not be used for purposes other than identifying links with ongoing investigations and prosecutions and supporting 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 the grounds for acquittal or non-prosecution, those data should be deleted.

(29) Eurojust has concluded 12 cooperation agreements with third countries, which allow for the transfer of operational personal data and the secondment of third-country liaison prosecutors to Eurojust. Moreover, the Trade and Cooperation 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 ([7]) allows for the secondment of a liaison prosecutor. In March 2021, the Council gave the Commission a mandate to negotiate cooperation agreements between Eurojust and 13 further third states, namely Algeria, Argentina, Armenia, Bosnia and Herzegovina, Brazil, Colombia, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.

([7]) OJ L 149, 30.4.2021, p. 10.

(30) 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 as regards 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 for their access to the case management system. Eurojust should implement adequate safeguards and security measures for the protection of data and fundamental rights through the updated technical set-up and strict internal rules.

(31) When processing operational personal 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 of the European Parliament and of the Council ([8]), as well as specific rules on the processing of operational personal data provided for in Regulation (EU) 2018/1727 as amended by Regulation (EU) 2022/838 of the European Parliament and of the Council ([9]) and this Regulation. Those 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.

(32) 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 States concerned, subject to applicable national law, Union law or international law, comprising conventions or other international agreements on mutual assistance in criminal matters.

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

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

(35) 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 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.

(36) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark annexed to the TEU and the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(37) 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,

([8]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

([9]) Regulation (EU) 2022/838 of the European Parliament and of the Council of 30 May 2022 amending Regulation (EU) 2018/1727 as regards the preservation, analysis and storage at Eurojust of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences (OJ L 148, 31.5.2022, p. 1).

HAVE ADOPTED THIS REGULATION:

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 as to whether and how Member States provide judicial assistance to a third country or to an international organisation shall remain solely with the competent authority of the Member State concerned, subject to applicable national, Union or international law.';

(2) Article 20 is amended as follows:

(a) the following paragraph is inserted:

'2a. Each Member State shall designate a competent national authority as Eurojust national correspondent for terrorism matters. That national correspondent for terrorism matters shall be a judicial or other competent authority. Where the national legal system so requires, it shall be possible for a Member State to designate more than one competent national authority as Eurojust national correspondent for terrorism matters. 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) paragraph 8 is replaced by the following:

'8. In order to meet the objectives referred to in paragraph 7 of this Article, the persons referred to in paragraph 3, points (a), (b) and (c), of this Article shall be connected to the case management system in accordance with this Article and with Articles 23, 24, 25 and 34. The cost of connection to the case management system shall be borne by the general budget of the Union.';

(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 such information has already been transmitted to Eurojust in accordance with other provisions of this Regulation.';

(4) the following Article is inserted:

'*Article 21a*

Exchange of information on terrorism cases

1. As regards terrorist offences, the competent national authorities shall inform their national members of any ongoing or concluded criminal investigations supervised by judicial authorities as soon as the case is referred to the judicial authorities in accordance with national law, in particular national criminal procedural law, of any ongoing or

concluded prosecutions and court proceedings, and of any court decisions on terrorist offences. That obligation 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 an ongoing 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 (*).

4. The information transmitted in accordance with paragraph 1 shall include the operational personal data and non-personal data set out in Annex III. Such information may include personal data in accordance with Annex III, point (d), but only if such personal data are held by or can be communicated to the competent national authorities in accordance with national law and if the transmission of those data is necessary to identify reliably a data subject under Article 27(5).

5. Subject to paragraph 2, the competent national authorities shall inform their national members about any changes to the information transmitted under paragraph 1 without undue delay and, where possible, no later than 10 working days after such changes.

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 links identified on the basis of information provided under this Article.

(*) 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).';

(5) the following Articles are inserted:

'*Article 22a*

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

1. 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 shall be connected with a network of IT systems and interoperable e-CODEX access points, which operate under the individual responsibility and management of each Member State and Eurojust, enabling the secure and reliable cross-border exchange of information ("the decentralised IT system").

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 and data protection.

3. The competent national authorities shall transmit the information referred to in Articles 21 and 21a of this Regulation to Eurojust in a semi-automated and structured manner from national registers. The arrangements for such transmission shall be determined by the Commission, in consultation with Eurojust, in an implementing act, in accordance with Article 22b of this Regulation. In particular, that implementing act shall determine the format of the data transmitted pursuant to Annex III, point (d), to this Regulation and the necessary technical standards with regard to the transmission of such data, and shall set out the digital procedural standards as defined in Article 3, point 9, of Regulation (EU) 2022/850 of the European Parliament and of the Council (*).

4. 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. That reference implementation software shall 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. That setup shall 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 decentralised IT system.

5. The Commission shall provide, maintain and support the reference implementation software free of charge. The creation, maintenance and development of the reference implementation software shall be financed from the general budget of the Union.

6. Member States and Eurojust shall bear their respective costs for establishing and operating an authorised e-CODEX access point as defined in Article 3, point 3, of Regulation (EU) 2022/850, 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 of this Article shall be adopted by 1 November 2025 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) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (OJ L 150, 1.6.2022, p. 1).

(**) 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, 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 ongoing investigations and prosecutions;

(c) allow for the cross-checking of information and identifying 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 channels in accordance with applicable Union law.

4. Where Eurojust has been granted access to data in or from other Union information systems established under other Union legal acts, it may use the case management system to access data in or to connect to such information 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 information systems.

5. Paragraphs 3 and 4 do not extend the access rights granted to Eurojust to other Union information systems under the Union legal acts establishing those systems.

6. 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.

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

The national members may 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. Those 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 that national member 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 competent national authorities, in general or specific terms, any restrictions on the further handling, access and transfer of the information if a link as 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 have access to no more than the following data:

(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 has denied such access.

2. The national member shall, within the limitations provided for in paragraph 1 of this Article, decide on the extent to which access 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 be accessed at national level only 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, 2 and 3 of this Article, enter information in the case management system concerning their Member State. Such contribution shall be subject to validation by the respective national member. The College shall lay down the details of the practical implementation of this paragraph. 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 is added:

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

(a) persons for 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 the event of an acquittal or of a final decision not to prosecute. Where the proceedings did not result in a conviction, processing of operational personal data shall take place only in order to identify links between ongoing, future or concluded investigations and prosecutions as referred to in Article 23(2), point (c).';

(8) Article 29 is amended as follows:

(a) the following paragraph is inserted:

'1a. Eurojust shall not store operational personal data transmitted in accordance with Article 21a beyond the first of 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 or prosecution;

(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, or 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 shall be reviewed constantly by appropriate automated processing conducted by Eurojust, in particular from the moment 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) the following Article 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 concluded 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 in a 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, in the agreement with the respective country or in other applicable legal instruments.

Article 24(1), second subparagraph, 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 are added:

'9. Eurojust may continue to use the case management system composed of temporary work files and of an index until 1 December 2025, if the new case management system is not yet in place.

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

11. The competent national 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 date of entry into force of the implementing act referred to in Article 22b of this Regulation, if the technical requirements are not yet in place.';

(11) the following Annex is added:

'*ANNEX III*

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

For a natural person:

— surname (family name);

— first names (given names);

— any aliases;
— date of birth;
— place of birth (town and country);
— nationality or nationalities;
— identification document (type and document number);
— gender;
— place of residence;

For a legal person:

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

For both natural and legal persons:

— telephone numbers;
— email addresses;
— details of accounts held with banks or other 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;
— any affiliation with a 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 such proceedings;
— responsible public prosecutor's office;
— case number;
— date of opening of 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) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (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 Strasbourg, 4 October 2023.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	J. M. ALBARES BUENO