Council of the European Union

Brussels, 21 February 2023
(OR. en)

6677/23

Interinstitutional File:
2021/0391(COD)

COPEN 48
JAI 191
EUROJUST 5
CODEC 234

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	16007/22; 16106/22
No. Cion doc.:	14684/21 + ADD 1
Subject:	Regulation of the European Parliament and of the Council establishing a collaboration platform to support the functioning of Joint Investigation Teams and amending Regulation (EU) 2018/1726 - 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 13 December 2022 and as it is contained in 16106/22; 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

SGS 22 / 05982

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 establishing a collaboration platform to support the functioning of Joint Investigation Teams and amending Regulation (EU) 2018/1726

Dear Mr. López Aguilar,

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

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 set out in the compromise text contained 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 also wish to thank you for your close cooperation which should enable us to reach agreement on this dossier at first reading.

Yours faithfully,

E. HRDÁ
Chair of the
Permanent Representatives Committee

Copy to: Mr. Didier Reynders, Member of the European Commission
Mr Malik Azmani, Rapporteur for the European Parliament

Rue de la Loi/Wetstraat 175 – 1048 Bruxelles/Brussel – Belgique/België
Tél./Tel. +32 (0)2 281 61 11

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing a collaboration platform to support the functioning of Joint Investigation Teams and amending Regulation (EU) 2018/1726

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 82(1), point (d), 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,

Whereas:

(1) The Union has set itself the objective of offering its citizens a common area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured. At the same time, the Union has to ensure that that common area remains a safe place. That objective can only be achieved by a more effective, coordinated cooperation of the national and international law enforcement and judicial authorities and by means of appropriate measures to prevent and combat crime, including organised crime and terrorism.

(2) That is especially challenging where crime takes a cross-border dimension on the territory of several Member States and/or third countries. In such situations, Member States need to be able to join their forces and operations to allow for effective and efficient cross-border investigations and prosecutions for which the exchange of information and evidence is crucial. One of the most successful tools for such cross-border cooperation are Joint Investigation Teams ('JITs') that allow for direct cooperation and communication between the judicial and law enforcement authorities of several Member States and possibly third countries to organise their actions and investigations in the most efficient way. JITs are set up for a specific purpose and a limited time-period by the competent authorities of two or more Member States and possibly third countries, to carry out jointly criminal investigations with a cross-border impact.

(2a) JITs have proven instrumental in improving judicial cooperation for the prosecution of cross-border crimes, such as cybercrime, terrorism, and serious and organised crime, by eliminating time-consuming procedures and formalities between JIT members. The increased use of JITs has also enhanced the culture of international cooperation in criminal matters between judicial authorities in the Union.

(3) The Union acquis provides for two legal frameworks to set up JITs with the participation of at least two Member States: Council Framework Decision 2002/465/JHA[1] and Article 13 of the Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union[2]. Third countries can be involved in JITs as parties where there is a legal basis for such involvement, such as Article 20 of the Second Additional Protocol of the 1959 Council of Europe Convention[3] and Article 5 of the Agreement on Mutual Legal Assistance between the European Union and the United States of America[4].

---

1 Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams (OJ L 162, 20.6.2002, p. 1).

2 OJ C 197, 12.7.2000, p. 3.

3 CET No 182

4 OJ L 181, 19.7.2003, p. 34.

(3a) International judicial authorities play a crucial role in the investigation and prosecution of international crimes. Their representatives may participate in a particular JIT on invitation of the JIT members based on the JIT agreement. Therefore, the exchange of information and evidence between national competent authorities and any other court, tribunal or mechanism that aims to address crimes of concern to the international community as a whole, in particular the International Criminal Court (ICC) should be facilitated as well. This Regulation should therefore provide access for representatives of such international judicial authorities to the JITs collaboration platform in order to enhance international cooperation towards the prosecution of international crimes.

(3b) There is a pressing need for a collaboration platform for JITs to communicate efficiently and exchange information and evidence in a secure manner in order to ensure that those responsible for the gravest crimes can be swiftly held responsible. That need is underlined by the amended mandate of the European Union Agency for Criminal Justice Cooperation (Eurojust) as set out in Regulation (EU) 2022/838 of the European Parliament and of the Council[5] enabling the agency to preserve, analyse and store evidence relating to genocide, crimes against humanity, war crimes and related criminal offences and enabling the exchange of related evidence with competent national authorities and international judicial authorities, in particular the International Criminal Court (ICC).

---

5 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.).

(4) The existing legal frameworks at Union level do not set out how the entities participating in JITs exchange information and communicate. Those entities reach an agreement on such exchange and communication on the basis of the needs and available means. To fight the increasingly complex and time-sensitive cross-border crime, speed, cooperation and efficiency are crucial. However, there is currently no system to support the management of JITs, to allow for more efficient evidence searching and recording, and to secure the data exchanged between those involved in JITs. There is an evident lack of dedicated secure and effective channel to which all those involved in JITs could have recourse and through which they could promptly exchange large volumes of information and evidence or allow for secure and effective communication. Furthermore, there is no system that would support management of JITs, including the traceability of evidence exchanged among the participants. in a manner that is compliant with legal requirements before national courts, as well as the planning and coordination of JIT operations

(5) In light of the increasing possibilities of crime infiltrating Information Technology (IT) systems, the current state of play could hamper the effectiveness and efficiency of cross-border investigations, as well as jeopardise and slow down such investigations and prosecutions due to the unsecure and non-digital exchange of information and evidence, making them more costly. The judiciary and law enforcement in particular need to ensure that their systems are as modern and as safe as possible and that all JIT members can connect and interact easily, independently of their national systems.

(6) It is important for JITs' cooperation to be improved and supported by modern IT tools. The speed and efficiency of the exchanges between the entities participating in JITs could be considerably enhanced by creating a dedicated IT platform to support their functioning. Therefore it is necessary to lay down rules establishing a centralised IT platform ('JITs collaboration platform') at Union level to help JITs collaborate, securely communicate and share information and evidence.

(7) The JITs collaboration platform should only be used where one of the Union legal bases is, among others, a legal basis for the JIT. For all JITs based solely on international legal bases, the platform, financed by the Union budget and developed on basis of Union legislation, should not be used. However, where a third country is part of a JIT agreement that lists one of the Union legal bases besides an international one, its competent authorities should be considered JIT members.

(8) The use of the JITs collaboration platform should be on a voluntary basis. However, in view of its added value for cross-border investigations its use is strongly encouraged. The use or non-use of the JITs collaboration platform should not prejudice or affect the legality of other forms of communication or exchange of information and should not change the way the JITs are set up, organised or function. The establishment of the JITs collaboration platform should not impact the underlying legal bases for JITs nor the applicable national procedural legislation regarding the collection and use of the obtained evidence. Officials from other national competent authorities, such as customs, who may be members of JITs set up pursuant to the Framework Decision, should be able to have access to the JIT collaboration spaces. The platform should only provide a secure IT tool to improve cooperation, accelerate the flow of information between its users, increase the security of the data exchanged and the effectiveness of the JITs.

(9) The JITs collaboration platform should cover the operational and post-operational phases of a JIT, from the moment the relevant JIT agreement is signed by its members, until the JIT evaluation has been completed. Due to the fact that the actors participating in the JIT set-up process are different from the actors who are members of JIT once it is established, the process of setting up a JIT, especially the negotiation of the content and the signature of the JIT agreement, should not be managed by the JITs collaboration platform. However, following a need for an electronic tool to support the process of signing up a JIT, the Commission should consider covering that process by the e- Evidence Digital Exchange System (eEDES).

(10) For each JIT making use of the JITs collaboration platform, the JIT members should be encouraged to conduct an evaluation of the JIT, either during the operational phase of the JIT or following its closure, using the tools provided for by the JITs collaboration platform.

(11) The JIT agreement, including any appendices, should be a prerequisite for the use of the JITs collaboration platform. The content of all future JIT agreements should be adapted to take into account the relevant provisions of this Regulation.

(11a) The JITs Network developed a model agreement which includes appendices, to facilitate the setting up of JITs. The content of the model agreement and its appendices should be adapted to take into account the decision to use the JITs collaboration platform and the rules for access to the platform.

(12) From an operational perspective, the JITs collaboration platform should be composed of isolated JIT collaboration spaces created for each individual JIT hosted by the platform.

(13) From a technical perspective, the JITs collaboration platform should be accessible via a secure connection over the internet and should be composed of a centralised information system, accessible through a secure web portal, communication software for mobile and desktop devices, including advanced logging and tracking mechanism and a connection between the centralised information system and relevant IT tools, supporting the functioning of JITs and managed by the JITs Network Secretariat.

(14) The purpose of the JITs collaboration platform should be to facilitate the coordination and management of a JIT, ensure the exchange and temporary storage of operational information and evidence, provide secure communication, provide for evidence traceability and support the process of the evaluation of a JIT. All entities participating in JITs should be encouraged to use all functionalities of the JITs collaboration platform and to replace as much as possible the communication and data exchange channels which are currently used.

(15) The coordination and exchange of data between Justice and Home Affairs agencies and Union bodies active in judicial cooperation and JIT members is key to ensuring a coordinated Union response to criminal activities and providing crucial support to Member States in tackling crime. The JITs collaboration platform should complement existing tools allowing for secure exchange of data among judicial authorities and law enforcement, such as the Secure Information Exchange Network Application (SIENA).

(16) Communication-related functionalities of the JITs collaboration platform should be provided by state of the art software allowing for non-traceable communication stored locally at the devices of the users.

(17) A proper functionality allowing to exchange operational information and evidence, including large files, should be ensured through an upload/download mechanism designed to store the data centrally only for the limited period of time necessary for the technical transfer of the data. As soon as the data is downloaded by all addresses, it should be automatically and permanently deleted from the JITs collaboration platform.

(18) Given its experience with managing large-scale systems in the area of justice and home affairs, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) established by Regulation (EU) 2018/1726 of the European Parliament and of the Council[6] should be entrusted with the task of designing, developing and operating the JITs collaboration platform making use of the existing functionalities of SIENA and other functionalities at Europol to ensure complementarity and, where appropriate, connectivity. Therefore, its mandate should be amended to reflect those new tasks and it should be provided with the appropriate funding and staffing to meet its responsibilities under this Regulation. In that regard, rules should be established on the responsibilities of eu-LISA, as the Agency entrusted with the development, technical operation and maintenance of the JITs collaboration platform.

---

6 Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 (OJ L 295, 21.11.2018, p. 99).

(19) eu-LISA should ensure that data held by law enforcement authorities could, where necessary, be easily transmitted from SIENA to the JITs collaboration platform. To this end, a report should be submitted by the Commission to the European Parliament and to the Council assessing the necessity, feasibility and suitability of a connection of the JITs collaboration platform with SIENA, on the conditions, technical specifications and procedures for ensuring a secure and efficient connection and data exchange. The assessment should take into account a high level of data protection needed for such a connection, based on the existing Union and national data protection framework, such as Directive (EU) 2016/680 of the European Parliament and of the Council, Regulation (EU) 2018/1725 of the European Parliament and of the Council and the rules applicable to relevant Union bodies, offices or agencies in the legal acts establishing them. The protection level of data that will be exchanged through the JITs collaboration platform should be taken into account (sensitive, non-classified). The European Data Protection Supervisor should also be consulted prior to submitting the report to the European Parliament and Council with regard to the impact on the protection of individuals' rights and freedoms stemming from the envisaged processing of personal data.

(20) Since the establishment of the Network of National Experts on Joint Investigation Teams (the 'JITs Network') in accordance with Council Document 11037/05[1], the JITs Network Secretariat supports the work of the JITs Network by organising annual meetings, trainings, collecting and analysing the JIT evaluation reports and managing the Eurojust's JIT funding programme. Since 2011, the JITs Network Secretariat is hosted by Eurojust as a separate unit. To allow the JITs Network Secretariat to support users in the practical application of the JITs collaboration platform, to provide day-to-day guidance and assistance, to design and provide training modules, to raise awareness and promote the use of the JITs collaboration platform, Eurojust should be provided with appropriate staff allocated to the JITs Network Secretariat.

(21) Given the currently existing IT tools supporting operations of JITs, which are hosted at Eurojust and managed by the JITs Network Secretariat, it is necessary to connect the JITs collaboration platform with those IT tools, in order to facilitate the management of JITs. To that end, Eurojust should ensure the necessary technical adaptation of its systems in order to establish such connection. Eurojust should also be provided with the appropriate funding and staffing to meet its responsibilities in that regard as well.

(21a) During the operational phase of a JIT, Eurojust and Europol provide valuable operational support to JIT members by offering a wide range of supporting tools, including mobile offices, cross-match and analytical analyses, coordination and operational centres, the coordination of prosecution, expertise and funding.

(22) In order to ensure a clear allocation of rights and tasks, rules should be established on the responsibilities of Member States, Eurojust, Europol, the European Public Prosecutor's Office, the European Anti-Fraud Office (OLAF) and other competent Union bodies, offices and agencies, including the conditions, under which they may use the JITs collaboration platform for operative purposes.

(23) This Regulation sets out the details about the mandate, composition and organisational aspects of a Programme Management Board which should be set up by the Management Board of eu-LISA. The Programme Management Board should ensure the adequate management of the design and development phase of the JITs collaboration platform. It is also necessary to set out the details of the mandate, composition and organisation aspects of an Advisory Group to be established by eu-LISA in order to obtain expertise related to the JITs collaboration platform, in particular in the context of preparation of its annual work programme and its annual activity report.

(24) This Regulation establishes rules on access to the JITs collaboration platform and the necessary safeguards. The JIT space administrator or administrators should be entrusted with the management of the access rights to the individual JIT collaboration spaces. They should be in charge of managing access, during the operational and post-operational phases of the JIT, for JITs collaboration platform users, on the basis of the JIT agreement. JIT space administrators should be able to transfer their technical and administrative tasks to the JITs Network Secretariat, except for the verification of the data uploaded by third countries or representatives of international judicial authorities.

(25) Bearing in mind the sensitivity of the operational data exchanged among the JITs collaboration platform users, the JITs collaboration platform should guarantee a high level of security. eu-LISA should take all necessary technical and organisational measures in order to ensure the security of the exchange of data by using strong end-to-end encryption algorithms to encrypt data in transit or at rest.

(26) This Regulation establishes rules on the liability of Member States, eu-LISA, Eurojust, Europol, the European Public Prosecutor's Office, OLAF and other competent Union bodies, offices and agencies, in respect of material or non-material damage occurring as a result of any act incompatible with this Regulation. Concerning third countries and representatives of international judicial authorities, liability clauses in respect of material or non-material damage should be contained in respective JIT agreements.

(27) In addition, this Regulation provides specific data protection provisions, concerning both operational data and non-operational data, needed to supplement the existing data protection arrangements and to provide for an adequate overall level of data protection, data security and protection of the fundamental rights of the persons concerned.

(28) The processing of personal data under this Regulation should comply with the Union's legal framework on the protection of personal data. Directive (EU) 2016/680 of the European Parliament and of the Council[7] applies to the processing of personal data by competent national authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. As regards the processing by Union institutions, bodies, offices and agencies, Regulation (EU) 2018/1725 of the European Parliament and of the Council[8] should apply in the context of this Regulation. To that end, appropriate data protection safeguards should be ensured.

(28a) Each competent national authority of a Member State, and where appropriate, Eurojust, Europol, the European Public Prosecutor's Office, OLAF or any other competent Union body, office or agency should be individually responsible for the processing of operational personal data when using the collaboration platform established by this Regulation. JITs collaboration platform users should be considered joint controllers for the processing of non-operational personal data.

---

7 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

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).

(29) In accordance with the JIT agreement, it should be possible for JIT space administrators to grant access to a JIT collaboration space to third countries which are parties to a JIT agreement or to representatives of international judicial authorities participating in a JIT. In the context of a JIT agreement, any transfer of personal data to third countries or representatives of international judicial authorities, the latter being considered international organisations for that purpose, is subject to compliance with the provisions set out in Chapter V of Directive (EU) 2016/680. Exchanges of operational data with third countries or representatives of international judicial authorities should be limited to those strictly required to fulfil the purposes of the JIT agreement.

(30) Where a JIT has multiple JIT space administrators, one of them should be designated in the relevant JIT agreement as controller of the data uploaded by third countries or representatives of international judicial authorities, before the JIT collaboration space including third countries or representatives of international judicial authorities is established.

(31) eu-LISA should ensure that accessing the centralised information system and all data processing operations in the centralised information system are logged for the purposes of monitoring data integrity and security, the lawfulness of the data processing as well as for the purposes of self-monitoring. eu-LISA should not have access to the content of the JIT collaboration spaces.

(32) This Regulation imposes reporting obligations on eu-LISA regarding the development and functioning of the JITs collaboration platform in light of objectives relating to the planning, technical output, cost-effectiveness, security and quality of service. Furthermore, the Commission should conduct an overall evaluation of the JITs collaboration platform taking into account also the objectives of this Regulation, as well as the aggregated results of the evaluations of the individual JITs, two years after the start of operations of the JITs collaboration platform and every four years thereafter.

(33) While the setting up and maintenance of the JITs collaboration platform and the supporting role of Eurojust after the start of operations should be borne by the Union budget, each Member State as well as Eurojust, Europol, the European Public Prosecutor's Office, OLAF and any other competent Union body, office and agency should bear its own costs arising from their use of the JITs collaboration platform.

(34) In order to establish conditions for the technical development and implementation of the JITs collaboration platform, 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 the Council[9].

(35a) (new) The Commission should adopt the relevant implementing acts necessary for the technical development of the JITs collaboration platform as soon as possible after the entry into force of this Regulation.

(35) The Commission should determine the date of the start of operations of the JITs collaboration platform once the relevant implementing acts necessary for the technical development of the JITs collaboration platform have been adopted and eu-LISA has carried out a comprehensive test of the JITs collaboration platform, with the involvement of the Member States.

(36) Since the objective of this Regulation, namely to enable the effective and efficient cooperation, communication and exchange of information and evidence among JIT members, Eurojust, Europol, OLAF and other competent Union bodies, offices and agencies, cannot be sufficiently achieved by the Member States, but can rather, by setting out common rules, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary to achieve that objective.

---

9 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).

(37) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to 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.

(38) In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Ireland has notified, by letter of 7 April 2022, its wish to take part in the adoption and application of this Regulation.

(39) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) No 2018/1725 and delivered formal comments on 25 January 2022.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject matter

This Regulation:

(a) establishes an IT platform (the 'JITs collaboration platform'), to be used on a voluntary basis, to facilitate the cooperation of competent authorities participating in Joint Investigation Teams ('JITs') set up on the basis of Article 13 of the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union or on Framework Decision 2002/465/JHA;

(b) lays down rules on the division of responsibilities between the JITs collaboration platform users and the agency responsible for the development and maintenance of the JITs collaboration platform;

(c) sets out conditions, under which the JITs collaboration platform users may be granted access to the JITs collaboration platform;

(d) lays down specific data protection provisions needed to supplement the existing data protection arrangements and to provide for an adequate overall level of data protection, data security and protection of the fundamental rights of the persons concerned.

Article 2

Scope

This Regulation applies to the processing of information, including personal data, within the context of a JIT. That includes the exchange and storage of operational data as well as non-operational data

1a. This Regulation applies to the operational and post-operational phases of a JIT, starting from the moment the relevant JIT agreement is signed by its members until all operational and non-operational data of that JIT has been removed from the centralised information system.

This Regulation does not amend or otherwise affect the existing legal provisions on the establishment, conduct or evaluation of JITs

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'centralised information system' means a central IT system where storing and processing of JITs related data takes place;

(2) 'communication software' means software that facilitates the exchange of files and messages in text, audio or video formats between JITs collaboration platform users;

(3) 'competent authorities' means the authorities of the Member States competent to be part of a JIT that was set up in accordance with Article 1 of Framework Decision 2002/465/JHA and Article 13 of the Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union, the European Public Prosecutor's Office when acting pursuant to its competences as provided for by Articles 22, 23 and 25 of Council Regulation (EU) 2017/1939, as well as the competent authorities of a third country where they are party of a JIT agreement on the basis of an additional legal basis;

(4) 'JIT members' means representatives of the competent authorities referred to in point 3 of this Article;

(5) 'JITs collaboration platform users' means JIT members, Eurojust, Europol, OLAF and other competent Union bodies, offices and agencies or representatives of a participating international judicial authority;

(5a) 'international judicial authority' means an international body, court, tribunal, or mechanism established to investigate and prosecute serious crimes of concern to international community as a whole, namely crimes of genocide, crimes against humanity, war crimes and related criminal offences that affect international peace and security;

(6) 'JIT collaboration space' means an individual isolated space for each JIT hosted on the JITs collaboration platform;

(7) 'JIT space administrator" means Member State's JIT member, or a European Public Prosecutor's Office's JIT member, designated in a JIT agreement, in charge of the JIT collaboration space.

(8) 'operational data' means information and evidence processed by the JITs collaboration platform during the operational phase of a JIT to support cross-border investigations and prosecutions;

(9) 'non-operational data' means administrative data processed by the JITs collaboration platform, notably to facilitate the management of the JIT and cooperation between JITs collaboration platform users.

Article 4

Technical architecture of the JITs collaboration platform

The JITs collaboration platform shall be composed of the following:

(a) a centralised information system, which allows for temporary central data storage;

(b) a communication software, which allows for secure local storage of communication data on devices of the JITs collaboration platform users;

(c) a connection between the centralised information system and relevant IT tools, supporting the functioning of JITs and managed by the JITs Network Secretariat.

The centralised information system shall be hosted by eu-LISA at its technical sites.

Article 5

Purpose of the JITs collaboration platform

1. The purpose of the JITs collaboration platform shall be to facilitate:

(a) the coordination and management of a JIT, through a set of functionalities supporting the administrative and financial processes within the JIT;

(b) the rapid and secure exchange and temporary storage of operational data, including large files, through an upload and download functionality;

(c) secure communications through a functionality covering instant messaging, chats, audio and video-conferencing;

(d) the traceability of exchanges of evidence through a business logging and tracking mechanism allowing to keep track of all evidence exchanged, including its access and processing, through the JITs collaboration platform;

(e) the evaluation of a JIT through a dedicated collaborative evaluation process.

CHAPTER II

Development and operational management

Article 6

Adoption of implementing acts by the Commission

The Commission shall adopt the implementing acts necessary for the technical development of the JITs collaboration platform as soon as possible, and in particular acts concerning:

(a) the list of functionalities required for the coordination and management of a JIT, including machine translation of non-operational data";

(b) the list of functionalities required for secure communications;

(c) business specifications of the connection referred to in Article 4, point (c);

(d) security in accordance with Article 15;

(e) technical logs in accordance with Article 21;

(f) statistics and data in accordance with Article 22;

(g) performance and availability requirements of the JITs collaboration platform.

The implementing acts referred to in the first subparagraph of this Article shall be adopted in accordance with the examination procedure referred to in Article 25 (2).

Article 7

Responsibilities of eu-LISA

1. The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice ('eu-LISA') shall establish the design of the physical architecture of the JITs collaboration platform including its technical specifications and evolution on the basis of the decisions taken in accordance with Article 6. That design shall be approved by its Management Board, subject to a favourable opinion of the Commission.

2. eu-LISA shall be responsible for the development of the JITs collaboration platform in accordance with the principle of data protection by design and by default. The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project coordination.

3. eu-LISA shall make the communication software available to the JITs collaboration platform users.

4. eu-LISA shall develop and implement the JITs collaboration platform as soon as possible after the entry into force of this Regulation and following the adoption by the Commission of the implementing acts pursuant to Article 6.

5. eu-LISA shall ensure that the JITs collaboration platform is operated in accordance with this Regulation, with the implementing act referred to in Article 6, as well as in accordance with Regulation (EU) 2018/1725.

6. eu-LISA shall be responsible for the operational management of the JITs collaboration platform. The operational management of the JITs collaboration platform shall consist of all the tasks necessary to keep the JITs collaboration platform operational in accordance with this Regulation, and in particular the maintenance work and technical developments necessary to ensure that the JITs collaboration platform functions at a satisfactory level in accordance with the technical specifications.

7. eu-LISA shall ensure the provision of training on the technical use of the JITs collaboration platform to the JITs Network Secretariat, including by providing training materials.

7a. eu-LISA shall set up a support service for mitigating technical incidents reported to it in a timely manner.

7b. eu-LISA shall continuously carry out improvements and add new functionalities to the JITs collaboration platform, based on the input it receives from the Advisory Group referred to in Article 11 and the annual report of the JITs Network Secretariat referred to in Article 9a, point (e).

8. eu-LISA shall not have access to the content of the JIT collaboration spaces.

9. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68[10], eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its entire staff required to work with data registered in the centralised information system. That obligation shall also apply after such staff leave office or employment or after the termination of their activities.

10 Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission,(OJ L 56, 4.3.1968, p. 1).

Article 8

Responsibilities of the Member States

Each Member State shall make the technical arrangements necessary for access of its competent authorities to the JITs collaboration platform in accordance with this Regulation.
Member States shall ensure that the JITs collaboration platform users have access to the training provided by the JITs Network Secretariat pursuant to Article 9a, point (c) or an equivalent training provided at the national level. Member States shall also ensure that the JIT collaboration platform users are fully aware of data protection requirements under Union law.

Article 9

Responsibilities of competent Union bodies, offices and agencies

1. Eurojust, Europol, the European Public Prosecutor's Office, OLAF and other competent Union bodies, offices and agencies shall make the necessary technical arrangements to enable them to access the JITs collaboration platform.

2. Eurojust shall be responsible for the necessary technical adaptation of its systems, required to establish the connection referred to in Article 4, point (c).

Article 9a

Responsibilities of the JITs Network Secretariat

The JITs Network Secretariat shall support the functioning of the JITs collaboration platform by:

(a) providing, at the request of the JIT space administrator or administrators, administrative, legal, and technical support in the context of the setup and access rights management of individual JIT collaboration spaces, pursuant to Article 12(3a);

(b) providing day-to-day guidance, functional support, and assistance to practitioners on the use of the JITs collaboration platform and its functionalities;

(c) designing and providing training-modules for the JITs collaboration platform users aiming to facilitate the use of the JITs collaboration platform;

(d) enhancing a culture of cooperation within the Union in relation to international cooperation in criminal matters by raising awareness and promoting the use of the JITs collaboration platform among practitioners;

(e) keeping, after the start of operations of the JITs collaboration platform, eu-LISA informed of additional functional requirements by drafting an annual report on potential improvements and new functionalities of the JITs collaboration platform based on the feedback on the practical use of the JIT collaboration platform it collects from the JIT collaboration platform users.

Article 10

Programme Management Board

1. Prior to the design and development phase of the JITs collaboration platform, the Management Board of eu-LISA shall establish a Programme Management Board for the duration of the design and development phase.

2. The Programme Management Board shall be composed of ten members as follows:

(a) eight members appointed by the Management Board;

(b) the Chair of the Advisory Group referred to in Article 11;

(c) one member appointed by the Commission.

3. The Management Board of eu-LISA shall ensure that the members it appoints to the Programme Management Board have the necessary experience and expertise in the development and management of IT systems supporting judicial authorities.

4. eu-LISA shall participate in the work of the Programme Management Board. To that end, representatives of eu-LISA shall attend the meetings of the Programme Management Board in order to report on work regarding the design and development of the JITs collaboration platform and on any other related work and activities.

5. The Programme Management Board shall meet at least once every three months, and more often as necessary. It shall ensure the adequate management of the design and development phase of the JITs collaboration platform. The Programme Management Board shall submit written reports regularly to the Management Board of eu-LISA, and where possible every month, on the progress of the project. The Programme Management Board shall have no decision-making power nor any mandate to represent the members of the eu-LISA Management Board.

6. The Programme Management Board, in consultation with eu-LISA's Management Board, shall establish its rules of procedure which shall include in particular rules on chairmanship, meeting venues, preparation of meetings, admission of experts to the meetings, communication plans ensuring that non-participating Members of the eu-LISA Management Board are kept fully informed.

7. The chairmanship of the Programme Management Board shall be held by a Member State.

8. The Programme Management Board's secretariat shall be provided by eu-LISA.

Article 11

Advisory Group

1. eu-LISA shall establish an Advisory Group in order to obtain expertise related to the JITs collaboration platform, in particular in the context of the preparation of its annual work programme and its annual activity report, and identify potential improvements and new functionalities to be implemented in the JITs collaboration platform.

2. During the design and development phase of the JITs collaboration platform, the Advisory Group shall be composed of the representatives of the Member States, the Commission and the JITs Network Secretariat. It shall be chaired by eu-LISA. It shall:

   (a) meet regularly, where possible at least once a month, until the start of operations of the JITs collaboration platform;

   (b) report after each meeting to the Programme Management Board;

(c) provide the technical expertise to support the tasks of the Programme Management Board.

CHAPTER III

Setting up of the JIT collaboration spaces and access to the JITs collaboration platform

Article 12a

Setting up of the JIT collaboration spaces

Where a JIT agreement provides for the use of the JITs collaboration platform in accordance with this Regulation, a JIT collaboration space shall be created within the JITs collaboration platform for each JIT.

1. The agreement shall determine the rules for access to competent authorities to the relevant JIT collaboration space and may provide for competent Union bodies, offices and agencies, and, where appropriate, third countries which have signed the agreement, to be granted access to the relevant JIT collaboration space. The JIT agreement shall provide for the rules for such access, in accordance with this Regulation

2. The JIT collaboration space shall be opened by the JIT space administrator or administrators, with the technical support of eu-LISA.

3. If the JIT members decided not to use the JITs collaboration platform when they signed the JIT agreement but agree to start using the JITs collaboration platform over the course of a JIT, the JIT agreement, when it did not already provide for this possibility, shall be amended and paragraphs 1 to 3 of this Article shall apply. In case the JIT members agree to stop using the JITs collaboration platform over the course of the JIT, the JIT agreement shall be amended if this possibility was not already included in the agreement.

Article 12b

Designation and role of the JIT space administrator

1. If the use of the JITs collaboration platform is provided for in the JIT agreement, one or several JIT space administrators shall be designated in the JIT agreement, among the Member States' JIT members or European Public Prosecutor's Office's JIT member.

2. The JIT space administrator or administrators shall manage the access rights of the JITs collaboration platform users to the JIT collaboration space, in accordance with the JIT agreement.

3. The JIT agreement may provide for the JITs Network Secretariat to have access to a JIT collaboration space for the purpose of technical and administrative support, including for the management of access rights. In such situations, as agreed by the JIT members, the JIT space administrator shall grant the JITs Network Secretariat access to the JIT collaboration space.

Article 12c

Access to the JIT collaboration spaces by Member States' competent authorities and the European Public Prosecutor's Office

In accordance with the relevant JIT agreement, the JIT space administrator or administrators shall grant access to a JIT collaboration space to the competent authorities designated in that JIT agreement.

Article 13

Access to the JIT collaboration spaces by competent Union bodies, offices and agencies

In accordance with the relevant JIT agreement, the JIT space administrator or administrators shall grant access, to the extent necessary, to a JIT collaboration space to:

a) Eurojust, for the purpose of fulfilling its tasks set out in Regulation (EU) 2018/1727 of the European Parliament and of the Council[11].

b) Europol for the purpose of fulfilling its tasks set out in Regulation (EU) 2016/794 of the European Parliament and of the Council[12].;

c) OLAF for the purpose of fulfilling its tasks set out in Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[13]. and

d) other competent Union bodies, offices and agencies for the purpose of fulfilling tasks set out in their basic acts.

Article 14

Access to the JIT collaboration spaces by the competent authorities of third countries

1. In accordance with the relevant JIT agreement, and for the purposes listed in Article 5, the JIT space administrator or administrators shall grant access to a JIT collaboration space to the competent authorities of third countries which have signed that JIT agreement.

---

11 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) (OJ L 295, 21.11.2018, p. 138).

12 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).

13 Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).

2. Whenever Member States' JIT members and, when it participates, the European Public Prosecutor's Office JIT member upload operational data to a JIT collaboration space for the download by a third country, the relevant Member States' JIT member or the European Public Prosecutor's Office JIT member shall verify that the data they have respectively uploaded is limited to what is required for the purposes of the relevant JIT agreement and subject to the conditions laid therein.

3. Whenever a third country uploads operational data to a JIT collaboration space, the JIT space administrator or administrators shall verify that such data is limited to what is required for the purposes of the JIT agreement and subject to the conditions laid therein, before it can be downloaded by other users of the JITs collaboration platform.

4. Member States' competent authorities shall ensure that their transfers of personal data to third countries that have been granted access to a JIT collaboration space only take place where the conditions laid down in Chapter V of Directive 2016/680 are met.

4a. Union bodies, offices and agencies shall ensure that their transfers of personal data to third countries that have been granted access to a JIT collaboration space take place only where the conditions laid down in Chapter IX of Regulation (EU) 2018/1725 are met, without prejudice to data protection rules applicable to such Union bodies, offices or agencies in the relevant legal acts establishing them which might impose specific conditions for data transfers

5. The European Public Prosecutor's Office, when acting in accordance with its competences as provided for by Articles 22, 23 and 25 of Council Regulation (EU) 2017/1939, shall ensure that its transfers of personal data to third countries that have been granted access to a JIT collaboration space take place only when the conditions laid down in Articles 80-84 of Regulation (EU) 2017/1939 are met.

Article 14a

Access to the JIT collaboration spaces by representatives of international judicial authorities participating in a JIT

1. For the purposes listed in Article 5, the JIT space administrator or administrators shall, where provided for in the JIT agreement, grant access to a JIT collaboration space to the representatives of international judicial authorities who participate in the JIT.

2. The JIT space administrator or administrators shall verify and ensure that the exchanges of operational data with representatives of international judicial authorities that have been granted access to a JIT collaboration space are limited to what is required for the purposes of the JIT agreement and subject to the conditions laid therein.

3. Member States shall ensure that their transfers of personal data to representatives of international judicial authorities that have been granted access to a JIT collaboration space only take place where the conditions laid down in Chapter V of Directive 2016/680 are met.

4. Union bodies, offices and agencies shall ensure that their transfers of personal data to representatives of international judicial authorities that have been granted access to a JIT collaboration space take place only where the conditions laid down in Chapter IX of Regulation (EU) 2018/1725 are met, without prejudice to data protection rules applicable to such Union bodies, offices or agencies in the relevant legal acts establishing them which might impose specific conditions for data transfers.

CHAPTER IV

Security and liability

Article 15

Security

1. eu-LISA shall take the necessary technical and organisational measures to ensure a high level of cyber security of the JITs collaboration platform and the information security of data within the JITs collaboration platform, in particular in order to ensure the confidentiality and integrity of operational and non-operational data stored in the centralised information system.

2. eu-LISA shall prevent unauthorised access to the JITs collaboration platform and shall ensure that persons authorised to access the JITs collaboration platform have access only to the data covered by their access authorisation.

3. For the purposes of paragraphs 1 and 2, eu-LISA shall adopt a security plan, a business continuity and disaster recovery plan, to ensure that the centralised information system may, in case of interruption, be restored eu-LISA shall provide for a working arrangement with the Computer Emergency Response Team for the Union's institutions, bodies and agencies (CERT-EU) and shall adopt the security plan, taking into account the possible recommendations of the security experts present in the Advisory Group referred to in Article 11.

4. eu-LISA shall monitor the effectiveness of the security measures referred to in this Article and shall take the necessary organisational measures related to self-monitoring and supervision to ensure compliance with this Regulation.

Article 16

Liability

1. Where a Member State, Eurojust, Europol, the European Public Prosecutor's Office, OLAF or any other competent Union body, office or agency, as a consequence of a failure on their part to comply with their obligations under this Regulation, cause damage to the JITs collaboration platform, that Member State, Eurojust, Europol, the European Public Prosecutor's Office, OLAF or other competent Union body, office or agency respectively, shall be held liable for such damage, unless and insofar as eu-LISA fails to take reasonable measures to prevent the damage from occurring or to minimise its impact.

2. Claims for compensation against a Member State for the damage referred to in paragraph 1 shall be governed by the law of the defendant Member State. Claims for compensation against Eurojust, Europol, the European Public Prosecutor's Office, OLAF or any other competent Union body, office or agency for the damage referred to in paragraph 1 shall be governed by their respective founding acts.

CHAPTER V

Data protection

Article 17

Retention period for storage of operational data

1. Operational data pertaining to each JIT collaboration space shall be stored in the centralised information system for as long as needed for all concerned JITs collaboration platform users to complete the process of its downloading. The retention period shall not exceed four weeks.

2. As soon as the process of downloading is completed by all intended JITs collaboration platform users or, at the latest, upon expiry of the retention period referred to in paragraph 1, the data shall be automatically and permanently erased from the centralised system.

Article 18

Retention period for storage of non-operational data

1. Where an evaluation of the JIT is envisaged, non-operational data pertaining to each JIT collaboration space shall be stored in the centralised information system until the JIT evaluation has been completed. The retention period shall not exceed five years.

2. If it is decided not to conduct evaluation at the closure of the JIT or, at the latest, upon expiry of the retention period referred to in paragraph 1, the data shall be automatically erased from the centralised system.

Article 19

Data controller and data processor

1. Each competent national authority of a Member State, and where appropriate, Eurojust, Europol, the European Public Prosecutor's Office, OLAF or any other competent Union body, office or agency shall be considered to be data controllers in accordance with applicable Union data protection rules, for the processing of operational personal data under this Regulation.

2. With regard to data uploaded to the JITs collaboration platform by the competent authorities of third countries or representatives of the international judicial authorities, one of the JIT space administrators shall be designated in the relevant JIT agreement as data controller as regards the personal data exchanged through, and stored in the JITs collaboration platform.

   No data from third countries or representatives of international judicial authorities shall be uploaded prior to the designation of the data controller.

3. eu-LISA shall be considered to be data processor in accordance with Regulation (EU) 2018/1725 as regards the personal data exchanged through, and stored in the JITs collaboration platform.

4. The JITs collaboration platform users shall be joint controllers for the processing of non-operational personal data in the JITs collaboration platform.

Article 20

Purpose of the processing of personal data

1. The data entered into the JITs collaboration platform shall only be processed for the purposes of:

   (a) the exchange of operational data between the JITs collaboration platform users for the purpose of which the particular JIT has been set up;

   (b) the exchange of non-operational data between the JITs collaboration platform users, for the purposes of managing the JIT.

2. Access to the JITs collaboration platform shall be limited to duly authorised staff of the competent Member States' and third country authorities, Eurojust, Europol, the European Public Prosecutor's Office, OLAF and other competent Union bodies, offices or agencies, or representatives of international judicial authorities to the extent needed for the performance of their tasks in accordance with the purposes referred to in paragraph 1, and to what is strictly necessary and proportionate to the objectives pursued.

Article 21

Technical logs

1. eu-LISA shall ensure that a log is kept of all access to the centralised information system and all data processing operations in the centralised information system, in accordance with paragraph 2.

2. The logs shall show:

   (a) the date, time zone and exact time of accessing the centralised information system;

   (b) the identifying mark of each individual JITs collaboration platform user who accessed the centralised information system;

(c) the date, time zone and access time of each operation carried out by each individual JITs collaboration platform user;

(d) the operation carried out by each individual JITs collaboration platform user

The logs shall be protected by appropriate technical measures against modification and unauthorised access. The logs shall be kept for three years or for such longer period as required for the termination of ongoing monitoring procedures.

3. On request, eu-LISA shall make the logs available to the competent authorities of the Member States who participated in a particular JIT without undue delay.

4. Within the limits of their competences and for the purpose of fulfilling their duties, the national supervisory authorities responsible for monitoring the lawfulness of data processing shall have access to logs upon request.

5. Within the limits of its competences and for the purpose of fulfilling its supervisory duties in accordance with Regulation (EU) 2018/1725, the European Data Protection Supervisor shall have access to logs upon request.

CHAPTER VI

Final provisions

Article 22

Monitoring and evaluation

1. eu-LISA shall establish procedures to monitor the development of the JITs collaboration platform as regards the objectives relating to planning and costs and to monitor the functioning of the JITs collaboration platform as regards the objectives relating to the technical output, cost-effectiveness, usability, security and quality of service.

2. The procedures referred to in paragraph 1 shall provide for the possibility to produce regular technical statistics for monitoring purposes and shall contribute to the overall evaluation of the JITs collaboration platform.

3. If there is a risk of substantial delays in the development process, eu-LISA shall inform the European Parliament and the Council as soon as possible of the reasons for the delays, their impact in terms of timeframes and finances, and the steps it intends to take to remedy the situation.

4. Once the development of the JITs collaboration platform is finalised, eu-LISA shall submit a report to the European Parliament and to the Council explaining how the objectives, in particular relating to planning and costs, were achieved and justifying any divergences

5. In the event of a technical upgrade of the JITs collaboration platform, which could result in substantial costs, eu-LISA shall inform the European Parliament and the Council before making the upgrade.

6. Two years after the start of operations of the JITs collaboration platform and every year thereafter, eu-LISA shall submit to the Commission a report on the technical functioning of the JITs cooperation platform, including its non-sensitive security aspects. The report shall be made publicly available.

7. Two years after the start of operations of the JITs collaboration platform, following the report of eu-LISA referred to in paragraph 6, and every four years thereafter, the Commission shall conduct an overall evaluation of the JITs collaboration platform. The Commission shall transmit the overall evaluation report to the European Parliament and the Council.

7a. Within eighteen months after the date of the start of operations, the Commission, following consultation with Europol and the Advisory Group referred to in Article 11, shall submit a report to the European Parliament and to the Council assessing the necessity, feasibility, suitability and cost-effectiveness of a potential connection between the JITs collaboration platform with and SIENA. The report shall also include conditions, technical specifications and procedures for ensuring a secure and efficient connection. Where appropriate, the report shall be accompanied by the necessary legislative proposals, which may include an empowerment to the Commission for adopting the technical specifications of such a connection.

8. The Member States' competent authorities, Eurojust, Europol, the European Public Prosecutor's Office, OLAF and other competent Union bodies, offices and agencies shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 7. They shall also provide the JITs Network Secretariat with the information necessary to draft the annual report referred to in Article 9a, point (e). That information shall not jeopardise working methods or include information that reveals sources, names of staff members or investigations.

9. eu-LISA shall provide the Commission with the information necessary to produce the overall evaluation referred to in paragraph 7.

Article 23

Costs

The costs incurred in connection with the establishment and operation of the JITs collaboration platform shall be borne by the general budget of the Union.

Article 24

Start of operations

1. The Commission shall determine the date of the start of operations of the JITs collaboration platform, once it is satisfied that the following conditions are met:

   (a) the relevant implementing acts referred to in Article 6 have been adopted;

   (b) eu-LISA has carried out successfully a comprehensive test of the JITs collaboration platform, with the involvement of Member States, using anonymous test data.

   In any case, that date of start of the operations shall not be later than two years and a half after the entry into force of this Regulation.

2. Where the Commission has determined the date of start of operations in accordance with paragraph 1, it shall communicate that date to the Member States, Eurojust, Europol, the European Public Prosecutor's Office and OLAF. It shall also inform the European Parliament.

3. The decision of the Commission determining the date of the start of operations of the JITs collaboration platform, as referred to in paragraph 1, shall be published in the Official Journal of the European Union.

4. The JITs collaboration platform users shall start using the JITs collaboration platform from the date determined by the Commission in accordance with paragraph 1.

Article 25

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.

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

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

Article 26

Amendments to Regulation (EU) 2018/1726

Regulation (EU) 2018/1726 is amended as follows:

(1) in Article 1, the following paragraph 4a is inserted:

4a. The Agency shall be responsible for the development and operational management, including technical evolutions, of the Joint Investigation Teams ('JITs') collaboration platform;

(2) the following Article 8b is inserted:

Article 8b

Tasks related to the JITs collaboration platform

In relation to the JITs collaboration platform, the Agency shall perform:

(a) the tasks conferred on it by Regulation (EU) No XXX/20XX of the European Parliament and of the Council*;

(b) tasks relating to training on the technical use of the JITs collaboration platform provided to the JITs Network Secretariat, including provision of training materials.

(3) in Article 14, paragraph 1 is replaced by the following:

1. The Agency shall monitor developments in research relevant for the operational management of SIS II, VIS, Eurodac, the EES, ETIAS, DubliNet, ECRIS-TCN, e-CODEX, the JITs collaboration platform and other large-scale IT systems as referred to in Article 1(5).;

(4) in Article 19(1), point (ff) is replaced by the following:

(ff) adopt reports on the technical functioning of the following:

(i) SIS pursuant to Article 60(7) of Regulation (EU) 2018/1861 of the European Parliament and of the Council** and Article 74(8) of Regulation (EU) 2018/1862 of the European Parliament and of the Council***;

(ii) VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA;

(iii) EES pursuant to Article 72(4) of Regulation (EU) 2017/2226;

---

* Regulation (EU) No XXX/20XX of the European Parliament and of the Council establishing a centralised collaboration platform to support the functioning of Joint Investigation Teams and amending Regulation (EU) 2018/1726 (OJ L …).;

** Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

*** Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

(iv) ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240;

(v) ECRIS-TCN and of the ECRIS reference implementation pursuant to Article 36(8) of Regulation (EU) 2019/816 of the European Parliament and of the Council[****];

(vi) the interoperability components pursuant to Article 78(3) of Regulation (EU) 2019/817 and Article 74(3) of Regulation (EU) 2019/818;

(vii) the e-CODEX system pursuant to Article 14(1) of Regulation (EU) XXX[*****];

(viii) the JITs collaboration platform pursuant to Article xx of Regulation (EU) XXX[******] [this Regulation];

(5) in Article 27(1), the following point (dc) is inserted:

(dc) the JITs collaboration platform Advisory Group;.

Article 27

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 all Member States in accordance with the Treaties.

Done at Brussels,

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

[****] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

[*****] Regulation (EU) XXX of … (OJ L …).

[******] Regulation (EU) XXX of … (OJ L …).;

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) 2018/1727 of the European Parliament and the Council and Council Decision 2005/671/JHA, as regards the digital information exchange in terrorism cases

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

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

Whereas:

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

---

1 [...].

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

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

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

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

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

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

---

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

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

(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.

3

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

(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.

---

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).

(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.

5

(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.

6

(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.[5]

(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[6]. 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.

---

5 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).

6 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[7] allows for the secondment of a liaison prosecutor. In March 2021, the Council gave the Commission a mandate[8] to negotiate further cooperation agreements on the cooperation between Eurojust and thirteen further third states.

---

7 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).

8 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[9], 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:

---

[9] 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;

17

(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	*For the Council*
The President	*The President*