EUROPEAN
COMMISSION

Brussels, 1.12.2021
SWD(2021) 391 final

COMMISSION STAFF WORKING DOCUMENT

Analytical supporting document

Accompanying the document

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

{COM(2021) 757 final}

CONTENTS

Term or acronym	*Meaning or definition*
CMS	Case Management System
CTR	Counter-Terrorism Register
DNA	Deoxyribonucleic acid
e-CODEX	e-Justice Communication via Online Data Exchange
ECRIS-TCN	Centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons
EDPS	European Data Protection Supervisor
eEDES	e-Evidence Digital Exchange System
Eurojust	European Union Agency for Criminal Justice Cooperation
EPPO	European Public Prosecutor's Office
EU	European Union
FRA	European Union Agency for Fundamental Rights
IP	Internet Protocols
IT	Information Technology
JHA	Justice and Home Affairs
LPs	Liaison Prosecutors
SIENA	Secure Information Exchange Network Application
TESTA	Trans European Services for Telematics between Administrations
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom

1. INTRODUCTION

The European Union Agency for Criminal Justice Cooperation (Eurojust) has been established to coordinate investigations and prosecutions of serious cross-border crime in Europe and beyond. Combating terrorism has been within the remit of Eurojust's mandate since its creation in 2002[1] and remains one of its key priorities[2]. As the European Union's hub for judicial cooperation in criminal matters, Eurojust continuously supports national investigating and prosecuting authorities. With the evolution of security threats and the changing complexity of terrorist attacks and terrorist activities targeting the Member States, it has become evident that an efficient judicial response to terrorism often needs to reach beyond a single jurisdiction and beyond European borders.

To combat terrorism effectively, it is crucial to exchange relevant information for the prevention, detection, investigation or prosecution of terrorist offences. Council Decision 2005/671/Justice and Home Affairs (JHA) of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences[3] provides that the Member States must take the necessary measures to ensure that relevant information concerning prosecutions and convictions for terrorist offences, which affect or may affect two or more Member States, is transmitted to Eurojust.[4]

Since 2005, the importance of sharing information among the Member States and with Eurojust has only become more evident. This is underlined in Directive (EU) 2017/541 on combating terrorism[5], which harmonised definitions of terrorist offences and introduced minimum rules to better combat terrorism. It also amended Council Decision 2005/671/JHA to ensure that relevant information is exchanged between the Member States in an effective and timely manner, where the information could be used in preventing, detecting, investigating or prosecuting terrorist offences.[6]

One of the key elements of Eurojust's work in this field should be the European Judicial Counter-Terrorism Register (CTR), the prototype of which was launched in September 2019[7]. The objective was to identify potential links between judicial counter-terrorism proceedings and possible coordination needs stemming from these.

For this prototype, the Member States provide information on ongoing and concluded judicial proceedings concerning terrorist offences in their jurisdiction. These data should

---

1 Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63 , 6.3.2002, p.1).

2 In 2019, Eurojust has assisted 222 counter-terrorism investigations, increasing from 191 cases in 2018, compare 2019 Eurojust Report on Counter-Terrorism, published in December 2020, 2019 Eurojust Report on Counter-Terrorism (europa.eu).

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

4 Article 2 para. 3 lit. b, para. 5 Council Decision 2005/671/JHA.

5 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).

6 Article 22 para. 2,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.

7 https://www.eurojust.europa.eu/launch-judicial-counter-terrorism-register-eurojust.

be stored and cross-checked in Eurojust's information processing system, the Eurojust Case Management System (CMS), in the same way as operative data related to ongoing cases of judicial cooperation supported by Eurojust. The CTR, however, is still under construction; from a technical perspective, there is no separate register for data on terrorist offences and the cross-checking happens manually. The main reason is that Eurojust' CMS, which is technically outdated, is not able to integrate and support the CTR.

Eurojust was provided with a new legal framework and transformed into an EU agency with the entry into force of Regulation (EU) 2018/1727 ('Eurojust Regulation') in December 2019.[8] As the Eurojust Regulation was adopted before the establishment of the CTR, the setting-up of the CTR and its functions were not provided for in the Eurojust Regulation. Therefore, and due to the other limitations explained in detail below, the current CTR is not capable of serving its purpose well yet and needs to be upgraded.

In the Commission's Communication on the digitalisation of justice in the EU[9], this proposal was announced as part of a broader initiative to enable the secure electronic communication and exchange of information and documents between courts, national authorities, and justice and home affairs agencies. As part of the digitalisation of justice package and together with the initiative on the digitalisation of cross-border judicial cooperation and the initiative on Joint Investigation Teams collaboration platform, it is one of the proposals in the 2021 Commission work plan under the heading 'A New Push for European Democracy.' In the EU strategy on tackling organised crime, the Commission also announced its support in modernising Eurojust's CMS to help Eurojust provide feedback to national authorities and detect judicial links between ongoing investigations.[10]

2. PROBLEM DEFINITION: WHAT ARE THE PROBLEMS THAT NEED TO BE ADDRESSED

Detecting potential links between cases and/or investigations has always been one of Eurojust's key tasks, which is now enshrined in Article 22(1) of the Eurojust Regulation. On terrorist offences, Eurojust has performed this task based on the information shared in line with Council Decision 2005/671/JHA. The establishment of the CTR facilitated this role, putting efforts into harmonising the procedure and data shared by the Member States. However, practice has shown that Eurojust is still not fully equipped to fulfil this role. Problems exist regarding the data national authorities share with Eurojust, Eurojust's data processing environment and the cooperation with third country Liaison Prosecutors (LPs).

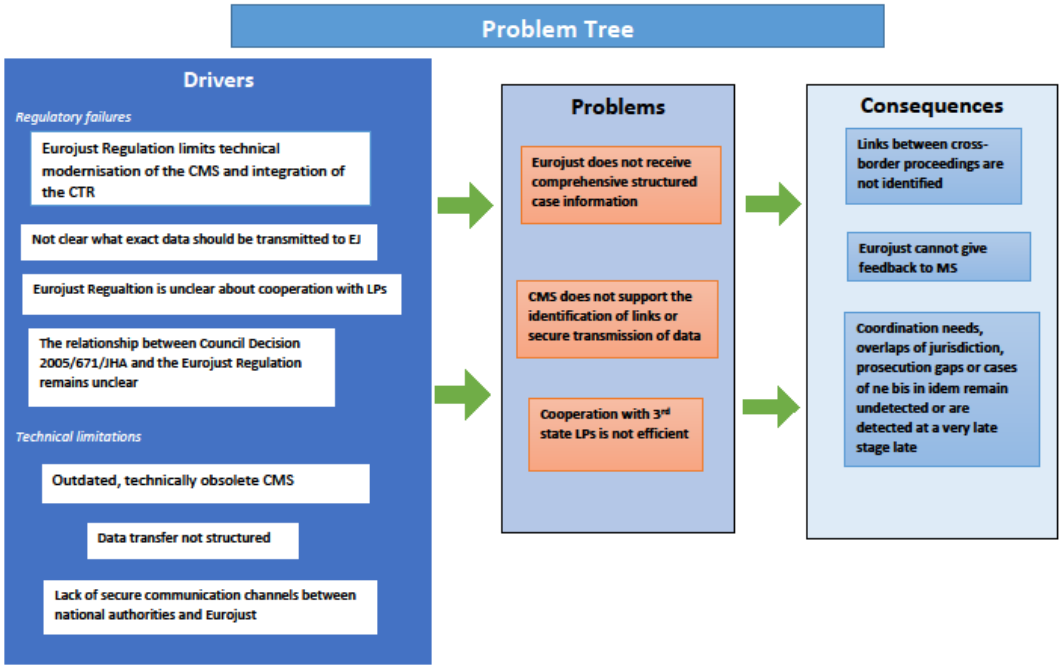
---

8 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).

9 Commission Communication on the Digitalisation of justice in the European Union - A toolbox of opportunities, COM(2020) 710 final, 2.12.2020.

10 Commission Communication on the EU strategy to tackle organised crime 2021-2021, COM(2021), 170final, 14.4.2021.

Figure 1: Problem Tree



a. Eurojust does not receive comprehensive structured case information from the Member States' national authorities

To identify links between ongoing or concluded investigations and court cases, Eurojust depends on information sent by the Member States. The obligation to provide Eurojust with information on counter-terrorism investigations and proceedings derives from Council Decision 2005/671/JHA. In addition to this third pillar instrument, Article 21 of the Eurojust Regulation sets out an obligation to send information on certain cross-border cases of serious crime. However, in many cases information is not shared at all. When data are shared, it is usually shared in an unstructured way. This means that data are sent e.g. via email in normal text. Such information cannot be entered into the CMS in an automated manner, rather it has to be entered manually.

The problem drivers

The root causes of these problems are both regulatory and technical.

Firstly, there is a lack of legal clarity in the application of Council Decision 2005/671/JHA. This third pillar instrument was not designed as a legal basis for the 2019 CTR but was intended to have a much broader scope. Although Article 2(5) of Council Decision 2005/671/JHA provides some guidance on what kind of information the

Member States must send to Eurojust,[11] it is still not specific enough to enable proper cross-checking, for which identical information would be necessary. Also, it does not specifically state when and how information should be sent by Member States to Eurojust, leaving it to the discretion of Member States' national authorities to decide what kind of information to send and at what point in the national procedures. In particular, the wording of that Decision lacks precision regarding at what stage of the national procedures information should be shared. While Article 2(3) only refers to 'all relevant information concerning prosecutions and convictions,' Article 2(5)(a) refers to the person, group or entity 'that is the object of a criminal investigation or prosecution.'

Secondly, the relationship between that Decision and the Eurojust Regulation is also unclear. Article 21(9) of the Eurojust Regulation states that the obligation to send information in line with its Article 21 should not affect other obligations regarding the sending of information to Eurojust, including Council Decision 2005/671/JHA. Therefore, it remains uncertain if other provisions of the Eurojust Regulation should apply to the implementation of that Decision. It is for example unclear, which data protection provisions are applicable or if Eurojust may determine the structure of the information received through the CTR in line Article 21(10) of the Eurojust Regulation[12].

Thirdly, the Eurojust Regulation does not detail what information must be sent under its Article 21. It also provides very limited requirements regarding the transmission of data to Eurojust. Only Article 21(10) refers to the structure, in which the Member States must send data, while Article 23(3) sets out the possibility to connect the CMS to secure telecommunication connections referred to in Council Decision 2008/976/JHA[13]. Therefore, only a limited number of Member States have secure communication channels with Eurojust. Also there currently is no technical solution in place for a more automated, structured information sharing between national authorities and Eurojust as the CMS is too obsolete for such exchanges. These problems have been analysed in detail in the Criminal Digital Justice study,[14] a study commissioned by the European Commission to identify the need and set out a vision to design digital measures for cross-border cooperation in criminal matters.

---

[11] Article 2 paragraph 5 of Council Decision 2005/671/JHA provides that:
5. The information to be transmitted in accordance with paragraph 3 to Eurojust shall be the following:
(a) data which identify the person, group or entity that is the object of a criminal investigation or prosecution;
(b) the offence concerned and its specific circumstances;
(c) information about final convictions for terrorist offences and the specific circumstances surrounding those offences;
(d) links with other relevant cases;
(e) requests for judicial assistance, including letters rogatory, addressed to or by another Member State and the response.

[12] Article 21 paragraph 10 of the Eurojust Regulation provides that:
10. Information referred to in this Article shall be provided in a structured way determined by Eurojust. The competent national authority shall not be obliged to provide such information where it has already been transmitted to Eurojust in accordance with other provisions of this Regulation.

[13] Article 9 of the Council Decision 2008/976/JHA of 16 December 2008 on the European Judical Network, (OJ L348/130, requires the establishment of a secure telecommunication connection, which may also be connected to the Eurojust CMS.

[14] Cross-border Digital Criminal Justice, Final Report, https://op.europa.eu/en/publication-detail/-/publication/e38795b5-f633-11ea-991b-01aa75ed71a1/language-en

Effects

Despite a clear legal obligation, national authorities often refrain from sending very sensitive data on terrorism cases to Eurojust due to the lack of secure communication channels. In some cases, sensitive data are sent to Eurojust via standard email or other unencrypted means, which are prone to interception. Therefore, national authorities either do not send sensitive data on ongoing investigations at all or send it through unsecure channels.

Where information is shared, Eurojust receives mixed information at different stages of the national procedures. The information sent does not necessarily match the data shared by other national authorities. It is not structured in the same categories. Therefore, the data needs to be entered manually by both the Member States and Eurojust. This creates an additional administrative burden for national authorities and the national desks at Eurojust and increases the risks of human error. In addition, it makes the detection of links between cases more difficult or even random.

In conclusion, due to the lack of comprehensive data, the CTR's and Eurojust's overall abilities to detect links are limited. Links remain often undetected or are only detected by chance and too late. Therefore, Eurojust is often not in a position to provide comprehensive and swift feedback to the Member States and not in a position to inform them about potential conflicts of jurisdiction, prosecution gaps or cases of double jeopardy.

b. Eurojust's outdated CMS does not support the identification of links or secure transmission of data

Eurojust's daily operations and casework rely on its CMS. Given its obsolete nature the current CMS does not support the innovative functions of the CTR, thus limiting Eurojust's proactive support and coordination role in this area. Additionally, it is not fit to support Eurojust's role in digitalised judicial cooperation, as the system is not connected electronically with other EU agencies or national authorities.

The CMS is very limited in its technical functions. With the current CMS, it is not possible to establish a separate database for the data related to the CTR. The CMS is not able to support more complex cross-checking functions but produces a high number of potential links that are of low quality, meaning that only a very few actually are a real hit. Processing a high number of low quality or fake hits is resource-intensive as it requires manual checking.

In addition, the CMS cannot be connected to secure channels other than TESTA[15], especially not to e-CODEX[16]. It cannot deal with structured data. There is no way to introduce any data automatically into the CMS, not to mention voluminous data. Finally, the current CMS is not able to deal with handling codes or with processing biometric data such as fingerprint data and facial images. The Digital Criminal Justice study

[15] TESTA (Trans-European Services for Telematics between Administrations) is a European network for data exchange between a wide variety of public administrations. The network uses internet protocols to ensure universal reach. It is operated by the Commission separately from the internet.

[16] e-CODEX (e-Justice Communication via Online Data Exchange) is an IT tool to ensure secure communication between judicial authorities in legal proceedings.

dedicated a full chapter to the redesign of the CMS to allow for its proper functioning and to ensure it addresses user needs.[17]

The problem drivers

The CMS was established in 2008 and is now technically outdated. It relies fully on manual data input and does not connect to other databases, e.g. those of national authorities or Europol.

The CMS was designed as an administrative support tool to open and follow-up specific operative case files between the Member States, i.e. within Eurojust. This technical set-up is reflected in the Eurojust Regulation. The Eurojust Regulation restricts the set-up of the CMS to temporary work file and an index[18].

The data on an individual case is saved in a 'temporary work file' with predefined settings. The file is called temporary, because by default, it is only stored as long as Eurojust is involved in the case. After the Eurojust case is closed, the data are deleted. The name temporary work file therefore reflects the phases of a Eurojust case and ensures compliance with data processing and retention periods.

This has practical consequences for the existing CTR prototype. When receiving information from their respective Member States in the context of the CTR, national authorities have to open one or several temporary work files for Eurojust to process the information. The files are not designed to deal with more static information such as concluded cases or terrorism convictions and its storage. They are also not well suited to cross-check data for a systematic detection of links between judicial proceedings at national level. To limit manual processing, Eurojust is obliged to import all data on investigations and prosecutions regarding terrorist offences received from a given Member States into one temporary work file, whereas this data may correspond to multiple separate proceedings at national level. This – on the other hand – is against the concept of a temporary work file, which is designed to be only associated to one specific case file.

The Eurojust Regulation does not allow to set up a database for the CTR within the CMS. In addition, processing of personal data outside the CMS is prohibited[19]. Therefore, the establishment of an additional database for the CTR outside the CMS is also not legally possible.

The same is true for data in certain cases of serious cross-border crime, which the Member States are obliged to share under Article 21(5) of the Eurojust Regulation. The Member States' competent national authorities are obliged to provide this information. However, Eurojust has no means to use such data efficiently.

---

[17] Cross-border Digital Criminal Justice, Final Report, https://op.europa.eu/en/publication-detail/-/publication/e38795b5-f633-11ea-991b-01aa75ed71a1/language-en, pp. 112ff.

[18] See Article 23(1) of the Eurojust Regulation.

[19] See Article 23(6) of the Eurojust Regulation.

Effects

The limited feedback from Eurojust makes the Member States reluctant to put all their efforts into sharing information. The lack of information, again, limits the data Eurojust can cross-check against, limiting its ability to identify links.

Due to the technical limitations, the current CMS identifies in the context of the CTR a high number of potential links with low quality, meaning that only a very small number actually have a real connection. Therefore, Eurojust cannot provide a full service to the Member States.

Due to the structure of the temporary work files, entering information and reviewing potential links require extensive manual intervention. For each potential link, it is necessary to examine whether or not a real link is established. As a result, staff working at the national desks have to follow up on each individual potential link and request further information from the other national desk involved in order to be able to assess if a real connection exists between the cases. This adds to the administrative burden of staff working in the national desks and gives rise to human error. Furthermore, those staff often cannot follow-up on all links in good time or even at all. This creates an increased risk that real links are missed and that the Member States are not informed about simultaneous investigations in another Member State, conflicts of jurisdiction, gaps of prosecution or cases of *ne bis in idem*[20].

c. Inefficient cooperation with third country Liaison Prosecutors

Practical and legal challenges arise when cooperating with third country Liaison Prosecutors (LPs). Eurojust has concluded cooperation agreements with 12 third countries[21] before the entry into force of the Eurojust Regulation. These agreements contain provisions on data exchange, data protection and practical cooperation. To facilitate the cooperation, they allow for seconded LPs to be posted to Eurojust. These LPs work side by side with their colleagues from the Member States and provide support in cross-border investigations involving their country in line with the applicable cooperation agreements. Currently, it is unclear how data, including personal data, can be exchanged efficiently and securely with third country LPs in compliance with the Eurojust Regulation.

---

[20] The principle of *ne bis in idem*, synonymously referred to as the prohibition of double jeopardy, provides that nobody should be judged twice for the same offence. It is enshrined in the domestic laws of the Member States as well as Article 50 of the Charter of Fundamental Rights of the European Union and Article 4 Protocol 7 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

[21] Cooperation agreements exist between Eurojust and Albania, Montenegro, North Macedonia, Serbia, Georgia, Iceland, Liechtenstein, Moldova, Norway, Switzerland, Ukraine and the USA. Eurojust has concluded another Cooperation Agreement with Denmark, which in not a member of Eurojust in line with Protocol 22 of the Lisbon Treaty. Part three, Title IV of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, also contains provisions on the future cooperation between national authorities of the UK and Eurojust.

The problem drivers

The Eurojust Regulation provisions on operational activities and Eurojust's obligations under the international cooperation agreements, concluded before the entry into force of the Eurojust Regulation, do not correspond.

The Eurojust Regulation contains general provisions on cooperation with third countries, including the posting of liaison magistrates. However, it does not contain any reference to LPs seconded to Eurojust by third countries. The general rights and obligations regarding these LPs are broadly defined in the cooperation agreements. Under these cooperation agreements, the LPs have certain participatory rights and are entitled to certain information. These rights have been put in practice through Eurojust College Decisions, in particular College Decision 2017-24 of 20 June 2017 on practical arrangements for Liaison Prosecutors seconded from Third States to Eurojust. This Decision, adopted in the context of the former legal framework, provided for LPs to access the CMS to ease the secure electronic exchange of information between LPs and Eurojust. It also allowed them to open temporary work files. However, after the entry into force of the Eurojust Regulation, such arrangements are only possible as long they do not contradict the Eurojust Regulation.

Article 24 of the Eurojust Regulation provides that only national members can open temporary work files in the CMS. It also contains an exhaustive list of people who might have access to temporary work files in the CMS on a case-by-case basis. In light of this, LPs seconded to Eurojust are not allowed to directly and independently open temporary work files in the CMS.

Effects

Legal uncertainty around the cooperation with third country LPs has already had a negative impact on the efficiency of this cooperation. To ensure the legality of data transfers to third countries, and in close cooperation with the European Data Protection Supervisor (EDPS), an interim solution to open cases has been put in place. LPs currently have to request the cooperation of one or more national members to open a case. The case is then opened by the national member and the LP together, meaning that they are also joint responsibility. For the national members concerned that means that they bear full responsibility for the data entered by the third country LPs. This process is ineffective and does not allow for the timely sharing of information. It makes the insertion of data of third countries ineffective and adds to the administrative burden of both, national members and LPs. There is also a risk that the current cooperation and exchange of data will be considered illegal as it might still be considered as circumvention of the provisions of the Eurojust Regulation on access to the CMS. This could potentially have effects on the admissibility of evidence in future cases and could therefore render the cooperation obsolete.

The importance of a legally sound and clear solution is even stronger with the UK now being a third country and in light of the Council mandate authorising the Commission to negotiate new cooperation agreements with additional 13 third countries[22].

[22] Council Decision of 16 March 2021 authorising the opening of negotiations for Agreements between the European Union and Algeria, Argentina, Armenia, Bosnia and Herzegovina, Brazil, Colombia, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey on cooperation between the European

3. LEGAL BASIS, SUBSIDIARITY AND EU ADDED VALUE

Legal basis

The legal basis for amending the Eurojust Regulation is Article 85 of the Treaty on the Functioning of the European Union (TFEU). Under Article 85 TFEU, Eurojust's structure, operation, field of action and tasks are to be determined by a regulation. This includes also the set-up of secure communication channels between the Member States and Eurojust. The amendments to Council Decision 2005/671/JHA are a consequence of these changes and therefore based on Article 85 TFEU.

Subsidiarity

According to the principle of subsidiarity laid down in Article 5(3) of the Treaty of the European Union (TEU), action at EU level should only be taken when the aims cannot be achieved sufficiently by the Member States alone and can therefore, by reason of the scale or effects of the proposed action, be better achieved at EU level. There is also a need to match the nature and intensity of a given measure to the identified problem.

As terrorism cases are often of a cross-border nature, action at national level alone cannot counter them effectively. That is why the Member States choose to work together to tackle the threats posed by terrorism. They seek to coordinate their judicial response and cooperate to address shared challenges. As the EU agency for criminal justice cooperation, Eurojust is a strong expression of this endeavour by the Member States to keep their citizen safe by working together.

There is a need for EU action because the measures envisaged have an intrinsic EU dimension, as they imply to improve the ability of Eurojust to act. It is Eurojust's mission to support and strengthen coordination and cooperation between national judicial authorities in relation to serious crime including terrorism affecting two or more Member States or requiring a prosecution on common bases. This objective can only be achieved at the EU level, in line with the subsidiarity principle. The Member States cannot create a more appropriate legal framework for the functioning of the CTR and amending Decision 2005/671 /JHA alone. It is therefore up to the EU to establish the legally binding instruments to achieve these results in line with the competences conferred upon it by the EU Treaties.

EU added value

The proposed changes will enable Eurojust to optimise its interaction with the Member States national authorities and provide them with the best service possible. More secure and efficient exchange of information in the field of terrorism and under the Eurojust Regulation will enable Eurojust to identify and follow up links between cases of terrorism more proactively and give timely feedback to the Member States. Eurojust will be in a better position to provide further support to the national authorities and to coordinate more efficiently cases on serious cross-border crime, in particular terrorism and organised crime.

Union Agency for Criminal Justice Cooperation (Eurojust) and the competent authorities for judicial cooperation in criminal matters of those third states.

4. WHAT SHOULD BE ACHIEVED/ OBJECTIVES

The general objective of this initiative is to enable Eurojust to fulfil its role better and in a more proactive manner when supporting and strengthening the coordination and the cooperation between the national investigating and prosecuting authorities in relation to serious crime, in particular terrorist offences.

The specific objectives are to:

- Enable Eurojust to identify links between parallel cross-border investigations and prosecutions regarding terrorist offences more efficiently and to provide proactively feedback on these links to the Member States.
- Render the data exchange between the Member States, Eurojust and third countries more efficient and secure.

5. HOW SHOULD THESE OBJECTIVES BE ACHIEVED?

To achieve these objectives, the Eurojust Regulation and Council Decision 2005/671/JHA should be amended to clarify and strengthen the Member States legal obligation to share data regarding terrorist offences with Eurojust. In addition, amendments to allow for a digitalisation of the Eurojust in view of the needs of the CTR should be brought about. Accordingly, comprehensive technical modernisation measures would also be connected to this initiative. In particular, secure communication channels and a more flexible data processing environment should also be put in place. Finally, the conditions under which third country LPs at Eurojust can get access and open cases in the CMS in line with the applicable data protection rules should also be clarified.

a. Improving the efficiency of data-exchange between national authorities and Eurojust

To improve information sharing with Eurojust, the cases in which the Member States are obliged to provide information on criminal investigations and judicial proceedings for terrorist offences would be more precisely set out. In addition, the stage of the criminal investigations and national proceedings and the kind of information to be sent would be identified more clearly and strengthened. And to make Eurojust fit for a digitalised European criminal justice, the technical possibilities to exchange semi-automated data in a structured way and through secure channels would be provided. This would improve the data exchange for the CTR, but as side effect, also improve the general data exchange between Eurojust and the Member States.

Data to be shared with Eurojust, especially identification data

The data that must be sent by the Member States to Eurojust is set out in Article 2(5) of Council Decision 2005/671/JHA and further defined in an internal Eurojust CTR template[23]. The data fields set out in the template relate primarily to the identity of the suspect(s): surname, name, birth date, birth city, country of birth, ID and gender. In addition, certain information on the crime itself and the proceedings are also to be sent:

[23] The template itself cannot be publicly shared. It requests Member States to provide certain details on the suspect of a terrorist offence, such as name, birth date and place, ID number, as well as certain details on the act of crime and the proceedings.

the relevant criminal provisions in original language, Eurojust crime, status of national proceedings, affiliation with a terrorist group, type of terrorism, responsible public prosecutor, case number, date of opening of formal proceedings, stage of judicial proceedings and a brief summary of case. This data set has been agreed in the College[24] of Eurojust and is based on experience with counter-terrorism proceedings. The consultation with the Member States and the survey of practitioners confirmed that the most important data to establish links between cross-border cases is reliable personal identification data. To enable Eurojust to follow-up, the stakeholders also considered the information and references to the national cases important. In order to render the obligation of the Member States more precise, the new legislation would be based on the information currently agreed on in the template.

Biometric data

All stakeholders underlined the importance of reliable identification data to identify links between cases. Therefore, biometric data would be added to the data set, which may be exchanged with Eurojust for identification. The survey results showed that in national proceedings biometric data, especially fingerprint data, are very important to identify links between investigations and judicial proceedings. In addition, facial images are an important means to identify suspects, relating to whom no reliable information exists. Facial images become a key identifier, the more facial recognition techniques develop.

During the consultations, several Member States questioned the need for such data. Other Member States, however, supported the idea. Some raised objections that in their Member State judicial authorities do not have access to such data.

However, taking into account the uncertainty of alphanumerical personal data in order to reliably identify terrorists, especially if they come from third countries or have been active in third countries, such data seems necessary to reliably identify suspects. To effectively fight against counter-terrorism, especially in connection to third countries, reliable identification of suspects is crucial. Therefore, a legal basis for the exchange of biometric data should be included in the CTR data.

Eurojust's access to biometric data isalso not new to the Eurojust Regulation, bearing in mind that national members already have access to national DNA registers (Article 9(d) Eurojust Regulation). In addition, Eurojust will be able to check biometric data through ECRIS-TCN[25]. However, the processing of biometric data would also only be possible in future, once a new CMS is put in place. The current CMS could not process such data, therefore it can also not be included in the CTR at the moment.

---

[24] The College of Eurojust, established in accordance with Article 10 Eurojust Regulation, is responsible for the organisation and operation of Eurojust. The College is formed of the National Members, one from each of the EU Member States, with the exception of Denmark, which by virtue of Protocol No 22 is not bound by the Eurojust Regulation. When the College exercises its management functions, it also comprises a representative of the European Commission. As management board it is, among others, responsible for adopting the budget, annual and multi-annual programming and the Annual Report, electing the President and Vice-Presidents and appointing the Administrative Director.

[25] Article 7 (3) 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.

As these data are not always available at the judicial stage of national proceedings, the transmission of such data can only be obligatory where judicial authorities have access to such information. In any case, a strict necessity test must be applied in each individual case due to the sensitive nature of the data and to ensure compliance with fundamental rights. Additional safeguards will be implemented in the design and setup of the new case management system (data protection by default and design).

Ongoing and concluded cases (including acquittals)

The Member States' obligation to provide data on ongoing as well as on closed cases would be set out in more detail and be strengthened. Currently, only data about ongoing investigations and convictions is to be provided. In the new proposal, this obligation should remain the same.

However, currently, under Article 27 and Annex 2 of the Eurojust Regulation, data on prosecutions must be deleted after Eurojust has been informed of an acquittal. However, at national level, data on previous prosecutions can be stored – for prosecution purposes only – and for a limited amount of time. To increase the CTRs effectiveness, data on prosecutions would also be stored for a limited time in order to improve the chances to identify a link. Data about earlier investigations could be extremely helpful to identify links with other counter-terrorist proceedings and to see, if certain suspects have already been party to terrorism investigations while insufficient evidence was collected to prosecute or convict them. During the prosecutions phase, such data would be extremely helpful. That said, retention periods in cases of acquittals would need to be significantly lower than in cases of convictions.

Cases with or without cross-border links

Under Council Decision 2005/671/JHA, data concerning terrorism cases 'which affect or may affect two or more Member States' must be sent to Eurojust. Currently, Eurojust considers this to include both, cases with or without an identified link because even if the link is not identified yet, once established, it would affect other Member States. In terrorism cases, these links are often only detected at a later stage and therefore it is particularly important that all cases are shared. To set such an obligation on all the Member States, competent national authorities would require an amendment to the legislation. Traditionally, many forms of terrorism are cross-border in nature and do not stop at either the borders of a Member State or the EU's borders.[26] In cases, which seem purely local at first, links appear after further investigation and cross-checking. This is even true for sole actors with increased self-radicalisation through the internet. Therefore, all terrorism cases regardless of whether links to another Member State or not are known should be sent to Eurojust. Many terrorist organisations are known to operate inside and outside of the EU. In addition, terrorist offenders are often involved in other forms of organised crime such as forging of documents, money laundering, smuggling, drug and human trafficking. Therefore, improved cross-checking of all terrorist cases with other Eurojust data could be helpful to establish links with other cases and to be aware of the extent of criminal activities of an organisation.

Stage of proceedings

[26] Eurojust has been requested to coordinate and facilitate judicial cooperation in an increasing number of multilateral cases of considerable complexity and diversity in the last years, 2019 Eurojust Report on Counter Terrorism, December 2020.

Currently, Eurojust is receiving data about terrorist cases at various stages in the national proceedings. This increases the difficulty to identify links and to identify parallel proceedings early on. Therefore, it would be important that data about those cases is shared with Eurojust at a similar stage of the national proceedings.

During the consultations, many stakeholders stressed the importance of this point. However, several Member States raised concerns over the potential overlap with Europol. This overlap will be mainly mitigated by a clearer definition of the stage, at which data is to be sent to Eurojust: The stakeholders agreed that Eurojust should be involved as soon as judicial authorities are involved. Some stakeholders requested to define judicial authorities to clarify that this already includes the prosecution stage. Therefore, it would be clarified that the national authorities that report to Eurojust include both, the prosecution offices and the courts. Such interpretation is backed by Eurojust's mandate in line with Article 2(1), Article 4(1)(a) of the Eurojust Regulation and Article 85 of the TFEU. However, this approach cannot fully prevent the judicial authorities from becoming involved at different stages in the different national systems due to the diversity of national criminal systems. A certain overlap with the data shared by national authorities with Europol seems unavoidable due to the diverse national systems, which reinforces the need for closer cooperation between the two EU agencies. To avoid gaps between the data shared with Europol and Eurojust, the hit-no-hit mechanism with Europol, which is already provided for by Article 49(1) of the Eurojust Regulation and Article 21(1) of the Europol Regulation, is to be set up. For this mechanism to work, a modernised CMS and the introduction of handling codes (see below) would be crucial.

Obligation to provide updates

The obligation to provide data would contain an obligation for the national authorities to provide updates on the developments of the ongoing cases. Such updates would be important to keep the register up to date and enable speedy detection of potential links. Updates would also ensure that the data processed by Eurojust is correct and that retention periods[27] are observed. Feedback from Eurojust, the Member States and practitioners in the targeted consultations underline the importance of such updates. To ensure the data is correct, updates could be required when changes regarding the person(s) under investigation and the stages of procedure occur (e.g. indictment, opening of court case, conviction, acquittal). Also, a general obligation for regular updates – for instance every three months - could ensure that the data are updated regularly.

Exceptions/ derogations

During the consultations, the option to exclude any possibility for national authorities to derogate from the obligation to provide data on terrorism cases was quickly discarded. The Member States and national authorities stressed in their feedback the importance to temporarily hold back information on especially sensitive investigations. Therefore, the derogation as currently set out in Article 2(7) Council Decision 2005/671/JHA[28] as

[27] At least under the current Eurojust Regulation, data has to be deleted on whenEurojust is informed that the person has been acquitted and the judicial decision became final, see Article 29 (1) (b).

[28] Article 2 (7) Council Decision 2005/671/JHA as amended by Directive (EU) 2017/541 exempts Member States from the obligation to make accessible, as soon as possible, t the competent authorities of another Member State, relevant information in connection with terrorist offences, where such

amended by Directive (EU) 2017/541 for information shared between the Member States in line with Article 2(6), would be extended to Eurojust in the proposal.

Mandatory secure communication channel(s)

The legislation would provide for the establishment and use of a secure connection between all Member States and Eurojust. In 2020, Eurojust reported 10 personal data breaches to the EDPS in line with the procedures defined in Regulation 2018/1725[29] and the Eurojust Regulation[30]. One of the most complex of these breaches concerned the receipt by two Member States and an administrative assistant of an email sent from a fraudulent Eurojust email address which contained malware. This attack launched by a criminal network aimed at installing malware on Eurojust computers and shows the threat cyber-crime poses for judicial authorities. All stakeholders stressed the importance of secure communication channel(s) to exchange sensitive data, especially in counter-terrorism cases, which confirmed the previous findings of the Digital Criminal Justice study. Lack of secure communication channel(s) is one of the main reasons why national authorities are hesitant to provide data regarding terrorist offences.

Some Member States already have a central secure connection with Eurojust through TESTA in place. However, there are no secure connections or secure communication channel(s) between competent national authorities on local level and Eurojust. As described above, such secure communication channel(s) would be crucial to improve data exchange between national authorities and Eurojust. As e-CODEX is currently proposed as the IT system for judicial cross-border cooperation, this legislation would build on it and propose e-CODEX as the gold standard. As the use of different national IT-systems would create additional challenges to ensuring interoperability, the legislation would also provide for the mandatory use of e-CODEX for all electronic communication. While some justified exceptions would be necessary, only mandatory use would ensure that Eurojust and the data transferred to and stored at Eurojust is properly protected.

Method of data exchange for the CTR and serious crimes under Article 21

The new piece of legislation would require the Member States to provide for means to upload semi-automated update of structured data from national databases. This means, that data should be provided in a prescribed structure or format and be digitalised, as suggested by the Digital Criminal Justice study. That said, it would be the national authorities that would identify the data and authorise the data transfer.

Access of national members to national databases is already provided for in Article 8 of the Eurojust Regulation. The obligation to provide for facilities to upload data semi-automatically would be included as well for information in the CTR and Article 21 of the Eurojust Regulation. The structured data exchange would enable staff working in the

---

sharing of information would 'jeopardizing current investigations or the safety of an individual, or contrary to essential interests of the security of the Member State concerned.'

29 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 (Text with EEA relevance.) OJ L 295, 21.11.2018, p. 39–98.

30 Compare Article 38 (4) of the Eurojust Regulation.

national administrations to limit manual processing and to input data into the CSM without additional administrative burden. [31]

b. Adapting the data-processing environment to digital justice

The data processing environment of the Eurojust Regulation would be made more flexible. Processing of operational personal data would not be possible solely in TWFs, but would also allow to set up a more permanent database for the CTR. That said, the purpose of and the conditions, under which cross-checking of information processed at Eurojust could take place, would be clearly identified. This would allow to better integrate the CTR within Eurojust's legal framework and its data processing environment. The data processing environment of the Eurojust Regulation would allow data processing connected to a more permanent database such as the CTR, so that it is no longer limited to processing operational personal data solely in TWFs.

Based on such rules, a new, technically up-to date CMS would be put in place with the CTR as integrated function. Secure, more-automated transmission of data by national authorities would reduce the administrative burden on them and on Eurojust. A new CMS would improve Eurojust's ability to find links between cases reported by the Member States, to follow up on detected links and to get more proactively involved in supporting their investigations and prosecutions, thus also helping them to prevent jurisdiction conflicts and *ne bis in idem* cases. The necessity and advantages of a new CMS have been analysed in detail in the Digital Criminal Justice study.

Overall design

Under the Eurojust Regulation, by default, only national desks have access to the data they store in a TWF to ensure data ownership of the national authorities. Access of other national desks or Eurojust staff must be explicitly granted. This ownership principle would be maintained. However, the overall design of the data processing environment would be detached from the technical design of the CMS. Therefore, technical details would be deleted from the Eurojust Regulation. This would enable the development of a modernised CMS, which could be adapted with time.

The processing of data would depend on the type of data. In addition to the data relating to cases supported by Eurojust based on other instruments, data relating to the CTR and the information, which the Member States have to share with Eurojust under Article 21 of the Eurojust Regulation on serious crimes, would be processed at Eurojust. Without a possibility to store the data, which is already to be submitted under the current Article 21 of the Eurojust Regulation, in a structured way, Eurojust cannot fulfil its task to identify links and give feedback to national authorities. This data would be cross-checked internally and against each other, as it is already done under the Eurojust Regulation at the moment. Once a link would be established, a new case would be opened or the information about the link would be fed into an existing case file.

Handling codes

[31] Based on the findings of the Cross-border Digital Criminal Justice, Final Report, https://op.europa.eu/en/publication-detail/-/publication/e38795b5-f633-11ea-991b-01aa75ed71a1/language-en. p. 99.

To facilitate the follow-up on links identified during the cross-checking, handling codes would be added to the information inserted to the CMS. These handling codes will help national authorities to decide in advance with whom the data may be exchanged. They can, for example, provide prior authorisation to share the data with certain parties, e.g. with the Member States or with Europol. After a link is identified, the data would, like today, not be automatically shared, but only if the handling code allows for it. If not, one could still request from the data owner permission to share or access information. The principle that data stored in the CMS may only be shared with the data owner's authorisation would therefore fully remain in place.

Retention periods

For the different types of data, different retention periods would be specified. For operative data, the current retention periods should remain unchanged. As criminal proceedings in different Member States are often at different stages of procedure, it is important to also have the ability to cross-check also against concluded cases and the possibility to identify new links through that. For the same reason, it would also be important to prolong the retention periods of the CTR data, in order improve the effectiveness of the cross-checking function of the CTR.

It would be possible to store the data while the investigations are ongoing, the retention periods should start with the end of the national proceedings. Retention periods in case of a conviction would be as long as in the respective national system; in case of an acquittal or in case the proceeding is terminated in another way, the data would be stored for three years after the final decision.

c. Third country Liaison Prosecutors

The conditions for cooperating with third country LPs seconded to Eurojust in line with a cooperation agreement would be clarified and aligned with the requirements of the Eurojust Regulation. This would increase the efficiency of exchanging information with third countries, ensure legality of data transfers and clarify responsibilities.

Opening and closing of cases

LPs seconded to Eurojust from third countries would have access to the CMS in order to enter, send and receive operative data on cases in which they cooperate with the Member States. Giving LPs limited access to the CMS is the best way to ensure that operative case information, including personal data, is exchanged securely and in line with data protection rules. LPs would be able to open and close cases independently, in the same way as they can request legal assistance without the agreement of the other party. The consultations with the Member States, Eurojust and national authorities showed that access of LPs is crucial for the cooperation with third countries. If third country LPs are unable to exchange data through the CMS under certain conditions, this also directly affects the easy and secure exchange of data of the Member States with the third countries. Therefore, there was strong support to grant the LPs access levels to the CMS for operational purposes, appropriate to the tasks performed and with appropriate safeguards to ensure that such access is in line with the rules in the Eurojust Regulation, including data protection rules.

On the links established with other desks, it would be distinguished between links to ongoing operative cases and links to CTR / Article 21 data. Hits with links to ongoing operative cases would be shown (in as far the data owner allowed for it), hits to links to

information in the CTR or in Article 21 register would be treated as blind hits. That means that in case of ongoing operative cases, LPs as well as national desks would be informed about a potential hit with another desk, enabling them to request more information from the relevant national desk. On the CTR and Article 21 data, only the national desk would be informed about the potential hit, leaving it to them, to decide if they want to approach the LP. CTR and Article 21 information is especially sensitive and the third countries do not contribute to these registers. A solution, in which only the data owner of the information in the register is informed about the hit and has the possibility to follow up, is therefore more adequate. As additional safeguard, the use of handling codes would enable national authorities to exclude third countries from accessing their data.

Responsibility for data

The responsibility for data would be shared between Eurojust and third countries sending the LPs. Until the data are entered into the CMS, the third countries would be solely responsible. After entering the data in the CMS, Eurojust would be responsible. However, the third country would have to accept the rules governing the CMS, including those on security and safeguards. In addition, a technical solution would be put in place in the CMS to restrict and control the possibilities for data processing abilities of all users.

6. STAKEHOLDER CONSULTATION AND EXPERTISE USED

The initiative is based on the findings of the Digital Criminal Justice study[32]. The study reviewed the needs and options for the creation of a 'Cross-Border Digital Criminal Justice,' a fast, reliable and secure IT infrastructure to enable national prosecution authorities in the Member States to interact with their national counterparts, Justice and Home Affairs (JHA) agencies and EU bodies in the JHA area.

The study shows that stakeholders in cross-border judicial cooperation in criminal matters need to securely communicate and exchange information through digital means. In addition, stakeholders need to easily manage data and ensure its quality. Authorities investigating a given (cross-border) case need to be able to identify links with other cases. An important help for this could be a modernised, redesigned Eurojust CMS.[33] The study concludes that the CTR should be one of the main components of the redesigned Eurojust CMS. It should be connected to a secure channel of communication.[34] The study also contains an analysis of possible IT solutions for a modernised CMS and some cost estimate.[35]

An extensive targeted consultation strategy was undertaken to ensure a wide participation of relevant stakeholders for the preparation of the proposal. Consultations included

[32] Cross-border Digital Criminal Justice, Final Report, https://op.europa.eu/en/publication-detail/-/publication/e38795b5-f633-11ea-991b-01aa75ed71a1/language-en.

[33] Cross-border Digital Criminal Justice, Final Report, https://op.europa.eu/en/publication-detail/-/publication/e38795b5-f633-11ea-991b-01aa75ed71a1/language-en, pp. 3f.

[34] Cross-border Digital Criminal Justice, Final Report, https://op.europa.eu/en/publication-detail/-/publication/e38795b5-f633-11ea-991b-01aa75ed71a1/language-en, pp. 119f.

[35] Cross-border Digital Criminal Justice, Final Report, https://op.europa.eu/en/publication-detail/-/publication/e38795b5-f633-11ea-991b-01aa75ed71a1/language-en, pp.234ff.

bilateral contacts, stakeholder and expert meeting, written contribution and a survey of practitioners.

The Commission has gathered a broad and balanced range of views on this issue by giving the opportunity to all relevant parties to express their opinions; in particular, the Member States, national authorities such as the national correspondents for terrorism matters, prosecutors and judges, Eurojust, its national desks and administration, the European Counter-Terrorism Coordinator, Europol, academics, fundamental rights and data protection stakeholders.

In addition, the issue was discussed, on 17 June 2021, in the Commission's Expert Group on EU Criminal policy, consisting of academics and practitioners in EU criminal law, and, on 24 June 2021, in the Commission's Digital Criminal Justice Expert Group, consisting of experts nominated by the Member States.

All stakeholders broadly welcomed the initiative and agreed with the problem areas identified.

The stakeholders were quite clear about the information to be shared with Eurojust: it should be the data necessary to identify subjects of investigations. Overall, the respondents were satisfied with the extent of data collected with the current Eurojust template. That said, the Member States requested to keep the information shared to a minimum and to define the data to be shared as precise as possible. There were differing opinions about the use of biometric data to identify suspects more reliably, especially terrorists with relation to third countries. Several Member States voiced doubts over the need to collect biometric data. They also raised doubts over the practical aspects of this issue, as some judicial authorities seem not to have access to biometric data and the current outdated CMS cannot process biometric data. There was general support for providing information on ongoing and concluded cases. Stakeholders agreed that Eurojust should be informed about counter-terrorism proceedings as soon as judicial authorities are involved. However, several stakeholder requested a clear distinction between the information shared with Eurojust and Europol to avoid duplication. Focus of the CTR should be justice needs. Almost all stakeholders stressed that timely feedback from Eurojust on data shared would be important as it would encourage the Member States' authorities to keep sharing data with Eurojust.

There was strong support to introduce secure communication channels between the Member States and Eurojust. Eurojust would prefer secure communication channels for all operational personal data sent to Eurojust. Some Member States were in favour of the mandatory use of secure channels. There was also support to prescribe the mandatory use of e-CODEX in the legislation to ensure the use of one single system in the EU. However, other stakeholders, including some experts of the Expert Group on EU Criminal policy, called for caution. Mandatory use of secure communication channels could exclude national authorities if they have no secure connections in place and make the investigation and prosecution of cross-border cases even more challenging. The interviews showed that, according to the interviewees, the main reason not to send CTR data is the additional administrative burden. Therefore, most stakeholders would prefer structured and (semi-) automated data transfers, but have doubts about their feasibility.

Many stakeholders underlined that the current CMS would not be able to fulfil the tasks envisaged for the CTR. Therefore, most stakeholders supported the idea to delete from the Eurojust Regulation technical details about the CMS. Eurojust considers this as a high priority issue in order to ensure Eurojust's ability to fulfil its tasks.

Most Member States and national authorities stressed that it would be important to maintain the principle of data ownership. Eurojust suggested introducing handling codes, already used effectively at Europol in order to ensure data ownership, for Eurojust as well.

There is general agreement that LPs should have full operational access to the CMS. The Member States and Eurojust practitioners pointed out that third countries, which have concluded a cooperation agreement and are therefore able to post a LP to Eurojust, should be treated on an equal footing as regards operative cases. LPs should be able to open and close cases independently. As for the list with links between cases, most stakeholders agree to continue to grant LPs similar access rights as those given to national members (without access to the CTR). Few stakeholders suggested that they would prefer a blind hit system.

7. ASSESSMENT OF THE PROPOSED INITIATIVE

a. Effectiveness: the extent to which the measure fulfils the objectives of the proposal

Specific objectives:

- To render data exchange between the Member States, Eurojust and third countries more efficient and secure.

The establishment of secure communication channels and structured upload are expected to significantly improve the security and efficiency of data exchange between the Member States and Eurojust. It is also expected to improve the level of data protection significantly, as the information shared will be less prone to interception. The improved digital exchange of data is expected to make the exchange quicker and to reduce the administrative burden. The Member States would know exactly which data to send for the CTR as it will be clearly set out in the Eurojust Regulation. While it is expected, that the information on terrorism cases will be increased, it will also be more clear, which data is necessary to be sent to Eurojust. This should reduce the exchange of unnecessary data and therefore contribute to the principle of data minimalisation. More clarity on the role of third country LPs, which would follow from setting out clear rules on the access and exchange of data between the Member States and third country LPs at Eurojust inside the new CMS, is expected to render data exchange between the Member States, Eurojust and third countries more efficient and secure.

- To enable Eurojust to identify links between cases more efficiently and to proactively provide feedback to the Member States more regularly.

The comprehensive establishment of secure communication channels, more structured and automated upload as well as clarification of information to be sent to Eurojust is expected to enable Eurojust to identify links between cases more efficiently. The clarified reporting obligation would ensure Eurojust receives the necessary and comparable information in order to identify links. The improved data exchange would ensure that the national authorities do not omit sending information due to the administrative burden. The new data processing environment and new CMS would also allow Eurojust to directly establish quality links, which would require only very limited manual intervention. At the same time, the new CMS could be built on the basis of data protection by default and design, which would contribute to an overall better level of data

protection. The improved identification of links and more efficient communication would enable Eurojust to give more and better feedback to the Member States and therefore support them better in their investigations.

General objective:

- To enable Eurojust to fulfil its stronger, more proactive role in supporting the Member States in their investigations, especially in terrorism cases.

The ability to identify links more efficiently, as well as and improved communication with the Member States are expected to enable Eurojust to fulfil the more proactive role, which the Eurojust Regulation envisaged for it. Eurojust will be able to provide better services to the Member States' national authorities, identify cases of conflict of jurisdiction, gaps in prosecutions and cases of double jeopardy and inform and support the Member States accordingly.

b. Technical and operational feasibility

Overall, the introduction of secure communication channels, structured data exchange and establishment of a modernised CMS is feasible from a technical and operational point of view. The Digital Criminal Justice study analysed the feasibility, also regarding the use of e-CODEX. It also analysed different option for the revamp of the Eurojust CMS. However, in order to ensure that Member States and Eurojust have sufficient time to comply with the technical requirements, a transitional period is needed.

c. Costs (set-up and recurring)

The Digital Criminal Justice study identified the technical costs for implementing the various solutions including consultancy resources to support the implementation programme at Eurojust.

In the Digital Criminal Justice study, the total cost of modernising the CMS was estimated at around EUR 39 million for setting it up and maintaining it over five years. As the current EU budget (multiannual financial framework, MFF) only covers the period until 2027, the maintenance costs for the years 2028 and 2029 were deducted from this amount. The remaining costs are estimated at EUR 31 million.

Based on the findings of the Digital Criminal Justice study and due to the urgency of the renewal of a new CMS, Eurojust took already first preliminary steps for the renewal. It mandated a market analysis study, inquiring in depth the most appropriate solution. At the end of 2021, Eurojust was attributed 9,5 Mio EUR unspent funds from the European Public Prosecutor's Office (EPPO), which will be used to prepare the development of the new CMS further. These funds are to be spent on consultancy services to support the analysis and design phase, infrastructure and off-the-shelf software purchase and installation services and consultancy services to provide programme and project management, to support the administrative changes and governance of the renewal of Eurojust CMS. These EUR 9,5 million are therefore also to be deducted from the cost estimation for the new CMS, which is why the outstanding costs for the CMS are estimated at EUR 21,5 million.

	Year 2024	Year 2025	Year 2026	Year 2027	Total
Commitments	1,033	8,128	7,027	5,390	**21,577**
Payments	0,578	4,780	6,458	9,771	**21,577**

The costs for the Member States to establish and use secure communication channels through e-CODEX are significantly lower, as e-CODEX over the internet will be implemented in all the Member States by the end of 2021. Therefore, in the context of this proposal, only Eurojust will be required to implement it.

In addition to these costs, Eurojust will have increased human resources requirements. A total of 25 permanent new staff will be necessary to enable Eurojust to fulfil its mandate under the Eurojust Regulation. Over a period of four years, this amounts to a total of about EUR 11 million.

Year **2024**	Year **2025**	Year **2026**	Year **2027**	Total
1,125	2,683	3,376	3,981	**11,165**

To equip Eurojust with a state-of-the-art technical infrastructure is a corner piece of this legislation. Additional staff will be necessary to implement these technical changes. While the implementation of the new CMS will be largely done through consultancy contracts, Eurojust will also need additional nine staff. These staff would for example ensure that the product will fit into the overall structure and that it will comply with the security and data protection requirements of Eurojust as an JHA agency. In the implementation phase, these staff will be involved in the development of the new CMS, in the later phase, these staff will be allocated to maintenance and control functions.

As result of the improved CTR and the improved cooperation with third countries, a substantive increase in data volume is expected to be processed at Eurojust. Therefore, additional eleven staff for operational support will be necessary. They will be necessary to analyse and manage data, follow cases and support the exchange with Member States. Three staff members are necessary to perform similar tasks with regard to the cooperation with third states. More detail can be found in the legislative financial statement.

d. Administrative costs

The impact on administrative costs is limited. It is estimated that one official staff is necessary to follow up and supervise the implementation of the legislation, especially the set-up of the technical infrastructure, to follow the relevant discussions in the Executive Board of the Agency on this issue as well as to monitor implementation of the budget in relation to the establishment of the CTR and to assist the agency to align their further digitalisation strategy with other developments in this area. One SNE will support the official in the above tasks.

e. Impact on the Area of Freedom, Security and Justice

The proposal is expected to:

- strengthen Eurojust's ability to fulfil its role under the Eurojust Regulation;
- optimise Eurojust's cooperation with the Member States and other JHA agencies and EU bodies; and
- improve Eurojust's ability to provide services to the Member States.

Eurojust will be in a better position to support the Member States in their investigations, to coordinate parallel investigations and prosecutions and detect cases of double jeopardy or prosecution gaps. In addition, Eurojust will be able to provide better services to the many requests to coordinate and facilitate judicial cooperation in multilateral terrorism cases of considerable complexity and diversity. Eurojust will therefore help to make Europe a safer place.

The new CMS is also expected to improve the cooperation and exchange of data with other JHA agencies and EU bodies and the functioning of the hit/no-hit mechanism. Eurojust will therefore better fulfil its complementary role in Freedom, Security and Justice in relation to the other JHA agencies and EU bodies.

The clarified provisions on the exchange of data with third countries are expected to improve Eurojust's services to the Member States' national authorities also when they need to cooperate with third countries' authorities. Eurojust's role as the central gateway for judicial cooperation in criminal matters between the EU and third countries will be strengthened. This will also improve the Member States' access to third countries for the investigation and prosecution of serious crimes.

f. Impact on fundamental rights, especially data protection

The proposal is expected to have a positive impact regarding several general interests of the EU. Strengthening Eurojust's abilities to provide services to the Member States' judicial authorities is expected to have a positive impact on the fight against serious crime, especially terrorism.

The identification of conflicts of jurisdiction has a positive impact on justice being effectively served and therefore also the right to an effective remedy and to a fair trial[36]. Preventing prosecution gaps ensures victims' rights to justice, while preventing prosecution in cases of *ne bis in idem* directly protects the rights of the accused under Article 50 of the EU Charter of Fundamental Rights.

The mandatory use of a secure communication channel between the Member States and Eurojust is expected to ensure better protection of sensitive investigation data, but also sensitive personal data, including these of witnesses and victims. The mandatory use of secure communication channels and the new CMS is expected to significantly lower the risk of cyber-attacks through malware and related data leaks. This should have a positive impact on the overall data security and data protection at Eurojust.

The revised data processing environment is expected to have positive, but also negative impacts on data protection, as outlined below.

---

[36] Article 47 of the EU Charter of Fundamental Rights (OJ C 326, 26.10.2012, p. 391).

Integrating the CTR in the Eurojust Regulation will clarify the legal rules applicable on the personal and non-personal data stored in the CTR. It ensures that the impact is provided by law in a clear and predictable manner, providing a clear legal basis for such processing. The storage of the data in a register separate from the TWF should not have an impact on data protection. The data will continue to be stored in the CMS, only in a different format, with a different structure and different information to be shared. The CMSs improved cross-checking function will affect data protection as it will lead to increased data processing. In addition, the more data will be shared with Eurojust, the more data will be processed at Eurojust. In connection with the CMSs improved ability to cross-check data, this will have a significant impact on the amount of data processed at Eurojust. However, it is necessary as this is the only way to achieve the objective of the proposal, which is to improve the ability of Eurojust to identify links, connect simultaneous cross-border investigations and provide the best service possible in the follow-up to the Member States investigations. Eurojust's task, however, is crucial to coordinate cross-border investigations and prosecutions and fight cross-border crime effectively. It is also proportionate, taking into account the difficulties of the Member States to follow-up and identify connections between cross-border criminal activities and cross-border investigations and prosecutions and the threat terrorism poses to our society. As a safeguard measure, the data will be sent through secure channels and stored in the new, safer CMS. In addition, cross-checking in the CMS is based on an indirect hit/no hit system: an automated comparison will produce an anonymous 'hit' if the data held by the requesting national desk matches data held by Eurojust. The related personal or case data are only provided in response to a separate follow-up request, if the national authority did not in advance authorise to share the data in the handling codes. Therefore, the principle of data ownership is protected and the sharing of operational personal information kept to a minimum.

The extension of retention period for CTR and Article 21 data would have an impact on the rights of the affected data subjects to data protection as well as on the right to private life [37], especially as data relating to criminal investigations and criminal convictions are sensitive in nature. The extension of retention periods aims at ensuring that links with previous proceedings are not missed, because data has been erased. Without affecting the presumption of innocence, criminal cases are also closed due to insufficient evidence. This is even more true in cross-border cases, in which it is even more difficult to gather admissible evidence. To identify links, it can be therefore useful to know that a specific suspect was already suspicious in connection to a similar crime in another jurisdiction, even if they were not convicted. As the data, which is to be stored, only relates to terrorism, which causes serious harm to the rights of citizen and the society as a whole, the storage of the data are proportionate to ensure effective fight against these crimes. As a further safeguard measure, however, it must be ensured that the data are not used for any purpose other than to prosecute in a given case.

The storage of biometric data, i.e. fingerprints and photographs, with the central system and its cross-checking through a hit/no-hit search with other data stored in the CMS would have a negative impact on the right to the protection of personal data, as well as on the right to private life.[38] As biometric data are of even more sensitive nature, it would require special justification and safeguards. However, due to the uncertainty of alphanumerical data of individuals who are suspected of terrorism (especially from third

[37] Article 8 and Article 7 of the European Charter of Fundamental Rights, respectively.

[38] Article 8 and 7 of the European Charter of Fundamental Rights, respectively.

countries), it is necessary to use such data, where available, for the reliable identification of suspects and for the effective prosecution in counter-terrorism cases. The identification of links is important to effectively prosecute crimes and contributes considerably to the security in a common area of justice and security. An important safeguard is the introduction of a secure communication channel and the new CMS to ensure that this sensitive data are processed in a secure environment. In addition, it will also be necessary to ensure that this data are used only for prosecution in a given case. Finally, in each specific case a strict necessity test should be applied by the national authorities before the transmission.

The access of third country LPs to the CMS and ability to open cases has no additional impact on fundamental rights or data protection. The aim of the legislative amendment is to give structure and clear rules, and therefore safeguards, to practices that are already taking place. The access of the third country LPs to the CMS only facilitates the secure and controlled exchange of data, which is in substance regulated by international mutual legal assistance agreements.

g. Proportionality

According to the principle of proportionality laid down in Article 5(4) of the TEU, there is a need to match the nature and intensity of a given measure to the identified problem. All problems addressed in this initiative call for EU-level support for the Member States to tackle these problems effectively.

Without the necessary technical and legal framework, Eurojust is not able to identify links between simultaneous investigations and prosecutions and cannot fulfil its crucial role, supporting and strengthening the cooperation between the Member States' national authorities in the investigation and prosecution of serious forms of crime, especially terrorism. Due to the increasingly cross-border set-up of organised crime and terrorist organisational, facilitated by digital communication tools, also a more coordinated approach is necessary in the judicial response. The judicial response does also often involve authorities outside the EU. To enable Eurojust to perform its crucial task fully is necessary to ensure the coordinated judicial follow-up.

Therefore, in line with the principle of proportionality, this proposal does not go beyond what is necessary in order to achieve this objective.

8. HOW WILL THE ACTUAL IMPACTS BE MONITORED

The Commission will commission an external independent evaluation on the implementation of the Regulation, including Eurojust's activities concerning the digitalisation of data exchange, by 13 December 2024. This evaluation will be carried out every five years to assess the implementation and impact of the Regulation and the effectiveness and efficiency of Eurojust in line with Article 69(1) of the Eurojust Regulation.