Council of the European Union

**Brussels, 26 August 2026**
**(OR. en)**

**12326/26**

**ENFOPOL 282**
**JAI 1050**

**COVER NOTE**

| | |
|---|---|
| From: | Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director |
| date of receipt: | 29 July 2026 |
| To: | Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union |
| No. Cion doc.: | COM(2026) 408 final |
| Subject: | REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Directive (EU) 2019/1153 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, including the assessment of the need for, and proportionality of, extending the definition of financial information |

Delegations will find attached document COM(2026) 408 final.

Encl.: COM(2026) 408 final

EUROPEAN
COMMISSION

Brussels, 29.7.2026
COM(2026) 408 final

**REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL**

**on the implementation of Directive (EU) 2019/1153 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, including the assessment of the need for, and proportionality of, extending the definition of financial information**

# 1. INTRODUCTION

Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (hereinafter "the Directive"), entered into force on 31 July 2019. The 26 EU Member States bound by the Directive (i.e. all except Denmark) had to bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 1 August 2021.

The overall objective of the Directive is to facilitate access to financial information by law enforcement authorities[1], thereby contributing to the broader policies in the realm of the internal market and security to prevent and combat money laundering and criminal activities. The Directive sets out rules to provide law enforcement authorities with access to the centralised bank account registries established in 2015 by the Directive (EU) 2015/849 of the European Parliament and of the Council [2] (hereinafter the "currently applicable AML Directive"). It also establishes requirements to facilitate the exchange of information between law enforcement authorities and Financial Intelligence Units, both at national and cross-border level, as well as cooperation of these actors with Europol. Such access and exchanges of information are subject to a set of specific data protection safeguards.

This report reviews the implementation of the Directive[3], assessing the transposition of the Directive by Member States into national law. **While the majority of Member States have correctly transposed the Directive, some issues remain**. At the same time, and taking into account the principle of stress testing the EU acquis and the Commission's policy of simplification and burden reduction, the report assesses the links of the Directive with other legislative instruments at EU level.

This report also includes an assessment on the need for, and proportionality of, extending the definition of financial information contained in the Directive. That is required by Article 21(3) of the Directive, which also requires the Commission to present a legislative proposal, if appropriate. The assessment, based on questionnaires to practitioners and discussions with Financial Intelligence Units and law enforcement authorities, shows that there are some challenges in the capacity of law enforcement to obtain and process financial information, but also some recent improvements and best practices that can help address existing hurdles, without excluding the possibility that future measures – including the extension of the definition of financial information – may be adopted to improve the ability of law enforcement to *follow the money*, an approach which entails investigating financial transactions to extract information or evidence about a crime, suspect or criminal network, and to identify illicit assets that can be frozen and confiscated.

1 The Directive covers authorities competent for the prevention, detection, investigation or prosecution of criminal offences as designated by Member States; tax authorities and anti-corruption agencies might also be covered to the extent that they are competent for such tasks pursuant to national law.

2 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73, ELI: http://data.europa.eu/eli/dir/2015/849/oj).

3 Article 21(1) of the Directive.

It is worth noting that the implementation of the Directive has taken place in a context of further improvements to the EU framework against money laundering and criminal finances, an area highlighted in the European Internal Security Strategy ('ProtectEU')[4]. In 2024, the co-legislators adopted the **Sixth Anti-Money Laundering package**, which includes Directive (EU) 2024/1640 of the European Parliament and of the Council (hereinafter the "new AML Directive")[5], Regulation (EU) 2024/1624 of the European Parliament and of the Council[6] and the creation of a new EU Anti-Money Laundering Authority[7], **and Directive (EU) 2024/1260 of the European Parliament and of the Council**[8], which will allow, among others, for the confiscation of unexplained wealth. The Directive was amended in the same year[9] to provide authorities access to bank account information across borders. That amendment is not in scope of this implementation report[10].

Once fully deployed on the ground, the revamped legal framework will facilitate the provision of better financial intelligence by Financial Intelligence Units and will improve the capacity of law enforcement, and notably asset recovery offices, to trace illicit assets.

## 2. ANALYSIS OF TRANSPOSITION BY MEMBER STATES OF THE DIRECTIVE

This section reviews the transposition of the Directive by Member States into national law, assessing the completeness and conformity of national laws and regulations with the requirements of the Directive.

### 2.1 Designation of competent authorities

According to **Article 3(1)** of the Directive, each Member State is to **designate**, among its **authorities** competent for the prevention, detection, investigation or prosecution of criminal offences, the competent authorities **that are empowered to access and search its national centralised bank account registry**. Those competent authorities are to include at least the Asset Recovery Offices. Pursuant to **Article 3(2)** of the Directive, each Member State is to designate among its authorities competent for the prevention, detection, investigation or prosecution of criminal offences those competent authorities that can **request and receive**

4 EUR-Lex - 52025DC0148 - EN - EUR-Lex

5 Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (OJ L, 2024/1640, 19.6.2024, ELI: http://data.europa.eu/eli/dir/2024/1640/oj).

6 Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L, 2024/1624, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1624/oj).

7 Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (OJ L, 2024/1620, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1620/oj).

8 Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation (OJ L, 2024/1260, 2.5.2024, ELI: http://data.europa.eu/eli/dir/2024/1260/oj).

9 Directive (EU) 2024/1654 of the European Parliament and of the Council of 31 May 2024 amending Directive (EU) 2019/1153 as regards access by competent authorities to centralised bank account registries through the interconnection system and technical measures to facilitate the use of transaction records (OJ L, 2024/1654, 19.6.2024, ELI: http://data.europa.eu/eli/dir/2024/1654/oj).

10 Pursuant to Article 2 of Directive 2024/1654, "Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 10 July 2027".

financial information or financial analysis from the Financial Intelligence Unit. **Article 3** of the Directive has been **correctly transposed** by all 26 Member States concerned. The list of designated competent authorities per Member State can be found on the page [Money laundering - Migration and Home Affairs - European Commission][11] and in the annex of this report.

### 2.2 Access by competent authorities to bank account information

According to **Article 4(1)** of the Directive, Member States are to ensure that the competent authorities designated pursuant to Article 3(1) of the Directive have the **power to access and search, directly and immediately, bank account information** when necessary for the performance of their tasks for the purposes of preventing, detecting, investigating or prosecuting a serious criminal offence or supporting a criminal investigation concerning a serious criminal offence. **Article 5** of the Directive contains the **conditions** for competent authorities to access and search bank account information: searches in the centralised bank account registry shall be performed only on a case-by-case basis by specifically designated staff with high confidentiality standards, and the security of the data is to be ensured through technical and organisational measures.

**Article 6** of the Directive requires that the authorities operating the bank account registries keep **logs of accesses and searches** by competent authorities, and specifies the minimum content of such logs: the file reference, the date and time of the query or search, the type of data used to launch the query or search, the identifier of the results, the name of the designated competent authority that consulted the registry and the identifier of the official who performed the query or search. Moreover, the logs are to be regularly checked by data protection officers, are to be made available upon request to the national competent supervisory authority and are to be erased five years after their creation.

Overall, the **transposition** of those Articles of the Directive by Member States **ensures** that competent authorities have **swift access to bank account information** while guaranteeing the security of the data.

Several Member States have not correctly transposed some requirements laid down in Article 5. That concerns in particular the requirement for staff to maintain high professional standards of confidentiality and data protection, the requirement for such staff to be of high integrity and appropriately skilled, and the requirement of technical and organisational measures that ensure the security of the data to be held to high technological standards. It should be noted, however, that several Member States apply those requirements in practice without having a specific legal provision in their national law.

All Member States concerned keep logs to monitor access to and searches of bank account information by the designated competent authorities. However, some compliance issues remain. In two instances, the bodies keeping the logs are the authorities accessing the information rather than the operator of the national centralised bank account registry. In some instances, the transposing provisions do not ensure that logs contain all the required content, or establish retention periods for the logs which do not coincide with the five years required by the Directive.

It should be noted that the requirements laid down in Article 6 of the Directive are more specific than the general requirements for law enforcement authorities to process personal data as laid

[11] Direct link: https://home-affairs.ec.europa.eu/competent-authorities-designated-pursuant-article-3-directive-eu-20191153_en

down in Directive (EU) 2016/680 of the European Parliament and of the Council[12], establishing safeguards that match the access to information provided for in the Directive. The transposition gaps identified often relate to aspects where the Directive introduced requirements that are more specific than those provided by Directive (EU) 2016/680. For example, while Article 25(1) of that Directive requires logs that "*make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data*" to be made available to the supervisory authority on request, Article 6 of the Directive goes a step further, by requiring the logging of the unique identifier, or of the results, or of the national file reference, by obliging the data protection officers for the centralised bank account registries to regularly check the logs, and by establishing specific retention periods after which the logs are to be erased.

### 2.3 Exchange of information between competent authorities and Financial Intelligence Units nationally, and between competent authorities or Financial Intelligence Units internationally

Chapter III of the Directive (Articles 7 to 10) contains provisions to facilitate cooperation at national level between Financial Intelligence Units and law enforcement authorities, whereby Financial Intelligence Units provide financial information and analyses to law enforcement authorities, and law enforcement authorities provide law enforcement information to Financial Intelligence Units. Those Articles provide for the possibility for such information to be transferred to other Member States, and set rules on the exchange of information between Financial Intelligence Units of different Member States and on the exchange of information obtained by law enforcement authorities from their Financial Intelligence Units with law enforcement authorities of other Member States.

#### 2.3.1 Exchanges of information between competent authorities and Financial Intelligence Units at national level

**Article 7 of the Directive requires Financial Intelligence Units** to cooperate with their national competent authorities designated pursuant to Article 3(2) of the Directive, upon request and on a case-by-case basis, by providing **financial information** already in its possession or by providing the **financial analyses** it produces. Article 7(2) and (4) of the Directive set out additional **conditions** governing such information exchanges: the decision to disseminate the information is to remain with the Financial Intelligence Unit which may refuse a request for various reasons, including the possible negative impact on ongoing investigations or analyses, the disproportionality of the request with regard to the legitimate interests of a natural or legal person, or the irrelevance of the request. According to Article 7(3) of the Directive, Financial Intelligence Units have to explain any refusal to reply to a request for information and any use by the competent authority of such information for purposes beyond those originally approved can only be made subject to the prior consent of the Financial Intelligence Unit concerned.

There are minor gaps in a few Member States: one Member State uses general provisions on cooperation among authorities to transpose this article, another Member States refers to terrorism financing, money laundering and predicate offences instead of referring to the scope

[12] 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, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

of the Directive, i.e. serious crimes, another Member State does not enable the Financial Intelligence Unit to reply to requests by all designated authorities, but only by judicial ones. The same is the case for the additional conditions regulating the exchange of information, where some Member States still have gaps in transposition.

According to **Article 8** of the Directive, Member States have to ensure that their designated **competent authorities reply** in a timely manner to requests for **law enforcement information** made by the national **Financial Intelligence Unit** on a case-by-case basis, where that information is necessary for the prevention, detection and combating of money laundering, associate predicate offences and terrorist financing.

**All 26 Member States** concerned have enabled their **Financial Intelligence Units to reply to requests for financial information or analyses made by designated competent authorities** and have required those authorities to reply to Financial Intelligence Unit requests for law enforcement information.

Two elements should be highlighted when assessing the application of Articles 7 and 8 of the Directive in the broader framework. First, since 2024 the new AML Directive governs in particular detail the responses to requests for information from competent authorities and the access to law enforcement information, establishing principles such as the Financial Intelligence Units autonomy to disseminate information and encouraging the direct access of Financial Intelligence Units to law enforcement information[13]. Not only does the new AML Directive go beyond the Directive in some respects, but also a few minor discrepancies and overlaps with the corresponding provisions in the new AML Directive and the Directive may bring a certain degree of uncertainty in the implementation of the two instruments by national authorities[14]. Second, as further expanded in the analysis in Section III of this report, many Member States have established effective mechanisms for cooperation between Financial Intelligence Units and law enforcement authorities, from the posting of liaison officers in each other's premises to the creation of inter-agency task forces, that go beyond the model of request-response regulated in the Directive.

### 2.3.2 Exchange of information between Financial Intelligence Units of different Member States

Under **Article 9** of the Directive, Member States are to ensure that, in exceptional and urgent cases, their **Financial Intelligence Units** are **entitled to exchange** financial information or financial analyses that may be relevant for the processing or analysis of information related to terrorism or organised crime associated with terrorism.

---

13 See in particular Article 21(1), point (c), of the new AML Directive, which provides Financial Intelligence Units with direct or indirect access to law enforcement information (clarifying in Article 21(3) of that Directive that "whenever possible, the FIU is granted direct access" to such information), and Article 22 of that Directive, which enables Financial Intelligence Units to respond in a timely manner to reasoned requests for information justified by concerns relating to money laundering, its predicate offences or terrorist financing from a set of authorities.

14 For example, the fact that the new AML Directive contemplates the possibility of direct access by the Financial Intelligence Unit to law enforcement information (while Article 8 of the Directive only regulates access upon request), that it enables the Financial Intelligence Unit to reply to public authorities that have the function of investigating or prosecuting money laundering, its predicate offences or terrorist financing, or that have the function of tracing, seizing or freezing and confiscating criminal assets (while Article 7 of the Directive only enables the Financial Intelligence Unit to reply to designated authorities) and that it requires the authority to provide feedback to the Financial Intelligence Unit, an obligation which is not contemplated in the Directive.

All 26 Member States concerned have correctly transposed that requirement. In that context, it should be noted that, since May 2024, Article 31(7) of the new AML Directive goes beyond the requirement laid down in Article 9 of the Directive by requiring Financial Intelligence Units to reply to each other's request in one working day for exceptional and urgent cases. That new obligation provides greater clarity on the obligations for Financial Intelligence Units in the situations governed by Article 9 of the Directive, for example by specifying a 1-day deadline to provide information and is also broader in scope as it is not limited to terrorism or organised crime associated with terrorism.

**2.3.3 Exchange of information between competent authorities of different Member States**

**Article 10(1)** of the Directive requires Member States to enable their designated **competent authorities to exchange with designated competent authorities of other Member States,** upon request and on a case-by-case basis, **financial information or financial analyses** obtained from their Financial Intelligence Units. According to that provision, such information is to be used for the purpose for which it was sought or provided. Such information can only be used for different purposes or by other authorities provided that the prior consent of the providing Financial Intelligence Unit has been obtained.

**Member States** have ensured that their **designated competent authorities are able to exchange the information provided by their Financial Intelligence Unit with their counterparts** in other Member States, with a few transposition gaps remaining in a few Member States. For example, the legislation of one Member State enables its designated competent authority to exchange personal data across Member States, covering in a broad manner – without explicitly mentioning – financial information or financial analysis. In two Member States, Article 10 of the Directive was transposed without explicit references to purpose limitation or prior consent. However, the limitation to the original purpose and the prior consent by the providing Financial Intelligence Unit is now enshrined in Article 34 of the new AML Directive. That Article allows Financial Intelligence Units to impose certain restrictions or limitations to the use of information they provide to Financial Intelligence Units of other Member States and establishes that a prior consent is to be granted by that Financial Intelligence Unit to the Financial Intelligence Unit of another Member State in case of further dissemination of the information concerned. That prior consent is to be granted promptly and is to be refused in limited circumstances.

It is also worth noting that Article 34 of the new AML Directive is a *lex specialis* vis-à-vis Directive (EU) 2023/977 of the European Parliament and of the Council[15], which already sets out detailed organisational and procedural rules to ensure an adequate and efficient exchange of information between the law enforcement authorities of Member States, including on single points of contact and setting clear time limits for exchanging information. The status of the Directive as *lex specialis* in relation to Directive (EU) 2023/977 entails that the exchange of financial information and analyses among law enforcement authorities is subject to a different set of rules compared to the type of information referred to in Article 2, point (4) of Directive (EU) 2023/977: in Articles 7 to 10 of the Directive there are no time limits to ensure that Financial Intelligence Units and competent authorities exchange financial information or analyses swiftly across borders, nor rules to ensure that the single points of contact are aware of those exchanges. That divergence conflicts with reality since authorities, when cooperating

---

[15] Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA (OJ L 134, 22.5.2023, p. 1, ELI: http://data.europa.eu/eli/dir/2023/977/oj).

on a specific investigation, often share information on the facts and circumstances of the case at hand, of which financial information is simply a part of that set of leads and evidence. That distinct set of rules for sharing financial information as compared to other types of information might pose practical challenges and does not reflect operational practices of law enforcement.

### 2.4 Exchange of information with Europol

Chapter IV of the Directive regulates the **exchange of information by law enforcement and Financial Intelligence Units with Europol**. Articles 11 and 12 of the Directive requires Member States to ensure that their competent authorities and Financial Intelligence Units are entitled to provide Europol with bank account information (for competent authorities) and financial information or analyses (for Financial Intelligence Units), upon duly justified requests and on a case-by-case basis. Article 12(3) of the Directive requires Financial Intelligence Units to explain any failure to comply with such a request. **Article 13(1)** of the Directive requires that the exchanges of information with Europol take place electronically through **SIENA** or, where applicable, **FIU.Net**. **Article 14** of the Directive deals with data protection **requirements** for Europol, such as limiting the processing of the information received under Chapter IV of the Directive to specifically designated staff and informing the Europol's data protection officer of each exchange.

Overall, those provisions have been correctly transposed by the Member States concerned, with some transposition issues remaining, such as the absence of explicit references to SIENA/FIU.Net or to the Financial Intelligence Units' explanations for not complying with a request from Europol. However, even in those Member States lacking an explicit provision, SIENA and FIU.Net are the default channel for communication between Europol and, respectively, law enforcement authorities and Financial Intelligence Units. As showcased in the analysis in Section 3 of this report, those provisions have improved Europol's access to bank account and financial information.

### 2.5 Additional provisions relating the processing of personal data and monitoring

Chapter V of the Directive contains additional provisions on the processing of personal data, and governs the exchanges of information between Financial Intelligence Units and law enforcement authorities, both nationally and cross-border, and between Financial Intelligence Units and Europol, as indicated in Article 15 which sets out the scope of the provisions of that Chapter V.

**Article 16** of the Directive **requires that the processing of sensitive personal data**, such as information revealing a person's racial or ethnic origin or political opinions, is subject to appropriate safeguards and that such processing is **performed in accordance with applicable data protection rules**. In addition, those data are to be processed by staff authorised by the controller and under the guidance of the data protection officer and has to be specifically trained. That requirement that only authorised staff that has received a specific training may process sensitive personal data is **not always reflected in national law**. Such transposition gaps might derive from the fact that, while Directive (EU) 2016/680 that predates the Directive already provides for the general requirement to provide for appropriate safeguards in the processing of sensitive data, it does not explicitly refer to such requirement for specifically trained and authorised staff. It is to be noted that such a specific requirement is not laid down in other more recent Union Acts that govern information exchanges that are similar to the ones laid down in the Directive. It is therefore necessary to take into account the impact of different rules for authorities that handle similar data, i.e. one set of rules for sensitive data in general situations and another one when handling sensitive data in the context of financial information or when Financial Intelligence Units are exchanging information in urgent cases related to terrorism.

In addition, **Article 17 of the Directive requires Member States to ensure that, for each of the exchanges of information, records are kept** of the name and contact details of the organisation and of the officer requesting the information, of the national case reference, of the subject matter of the request, and of any executing measures of such requests. Such records are to be kept for five years and are to be made available to the national supervisory authority upon request. **Several issues have been encountered with regard to the transposition of this provision by Member States**, such as the absence of an explicit reference in law to record keeping – even where such records are kept in practice – or the limitation of the records to some of the exchanges but not to others (e.g. in one Member State only the requests made by the Financial Intelligence Unit are recorded).

Those issues appear to have derived, in some instances, from the fact that the requirements laid down in Article 17 of the Directive are **more specific than the general framework for data protection rules applying to law enforcement authorities**, which only requires to keep logs when using automated processing systems. In addition, to better understand the impact Article 17 of the Directive, it needs to be considered that the requirements laid down in that Article go beyond other more recent Union Acts that regulate information exchanges among authorities, such as Directive (EU) 2024/1260, the new AML Directive, or Directive (EU) 2023/977, which contain less detailed requirements for record-keeping, requiring the Single Point of Contacts to deploy a single electronic case management system. Among other aspects, it should be clarified whether such case management systems already record some of the information exchanges referred to in the Directive, insofar as law enforcement authorities often share data on financial activities together with other relevant information related to the investigation.

It is also necessary to take into account that the requirement laid down in Article 17 of the Directive to keep records creates an administrative burden. The records to be kept cover the exchanges among 26 Financial Intelligence Units and a total of around 200 designated competent authorities, some of which - such as judicial or law enforcement authorities - are in turn composed of hundreds of divisions or departments.

Finally, Article 19 of the Directive requires Member States to collect and provide the Commission with **statistics on the number of searches in the centralised bank account registry**, data measuring the volume of requests for information issued by each authority under the Directive and data on the follow-up given to those requests, information measuring the response time to such requests and data measuring the cost of human or IT resources dedicated to domestic and cross-border requests.

Overall, the provisions of this chapter continue to raise a number of transposition issues, often linked to the interaction between multiple legislative instruments. In several instances, compliance has been observed in practice, despite the absence of explicit references in national law.

## 3. ASSESSMENT ON THE NEED FOR, AND PROPORTIONALITY OF, EXTENDING THE DEFINITION OF FINANCIAL INFORMATION

This section assesses whether it is necessary and proportionate to extend the definition of financial information contained in the Directive and, ultimately, the scope of information available to law enforcement authorities pursuant to the Directive.

Directive 2019/1153 establishes a system whereby in every Member State the Financial Intelligence Unit shall be able to provide to a set of designated competent authorities, upon request, financial information, defined as "any type of information or data, such as data on financial assets, movements of funds or financial business relationships, which is already held by FIUs". Competent authorities can then share this information with their counterparts in other Member States. **Article 21(3)** of the Directive **requires** the Commission to **report** to the European Parliament and to the Council **on the need for, and proportionality of, extending the definition of financial information** to any type of **information or data which are held by public authorities or by obliged entities and which are available to Financial Intelligence Units without the taking of coercive measures** under national law.

In order to address this requirement, this section assesses whether it is necessary for competent authorities to be able to obtain not only the information that Financial Intelligence Units already hold, but also other relevant information, e.g. from private companies and from other authorities, in particular through the Financial Intelligence Unit.

This assessment builds on questionnaires sent by the European Commission to obtain the views of Financial Intelligence Units and law enforcement authorities, to which 16 Financial Intelligence Units and 19 law enforcement agencies of 13 Member States replied, and on the discussions held at a meeting in November 2024 with law enforcement experts from all Member States to explore how to strengthen efforts against criminal finances. The outcome of the questionnaire was discussed at the EU FIU's Platform in June 2025.

Overall, the feedback from stakeholders shows that **there has been significant progress in recent years in the capacity of law enforcement to access financial data**. This is thanks to the implementation of Directive 2019/1153, and in particular the direct access it gives law enforcement to bank account registries. It is also due to increased awareness by Member States, that leads to increased resources, technical developments and enhanced cooperation among national authorities. The latter is particularly the case between law enforcement and Financial Intelligence Units: all Financial Intelligence Units can provide information already in their possession to competent authorities upon request, notably information previously transmitted by obliged entities to the Financial Intelligence Units as part of their reporting activity and by counterpart Financial Intelligence Units.

Such provision of information is subject to certain conditions, with notably the possibility for the Financial Intelligence Unit, in line with the principle of autonomy enshrined in Articles 33 and 34 of the new AML Directive, to refuse a request in line with the refusal grounds provided by the Directive and to limit the use of the information provided "for intelligence purposes only", excluding any possible use as evidence in a criminal proceeding. Several law enforcement agencies, referring to at that time to art. 55 of the Fourth Anti-Money Laundering Directive[16], **signalled that the limitation for using the information only for intelligence purposes constitutes a relevant hindrance**[17]. In addition to being able to share the

[16] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, pp. 73, ELI: http://data.europa.eu/eli/dir/2015/849/oj).

[17] This limitation derives, among other reasons, from the fact that Financial Intelligence Units deal with the analysis of suspicious facts but are not normally in a position to assess if crimes are being or have been committed. The exchange of evidentiary material is thereafter carried out by means of ad-hoc law

information they hold, half of the Financial Intelligence Units responding to the questionnaire indicated that they can also provide law enforcement certain information held by obliged entities or other public authorities, mostly in the course of criminal proceedings and with judicial approval.

Beyond the request/response logic of the Directive, practitioners have pointed to practices outside the scope of the Directive that would play a crucial role in improving **inter-agency cooperation** with Financial Intelligence Units, such as the posting of liaison officers from law enforcement authorities to the Financial Intelligence Unit and vice-versa, long-term or ad hoc inter-agency cooperation structures, as well as public-private partnerships. These various **models**, developed over the last few years, **allow for an exchange of information that is often faster and more effective than simple responses to requests for information**.

**Europol has also reported considerable benefits** from the Directive provisions enabling it to request competent authorities and Financial Intelligence Units for bank account and financial information, **with more than 160 requests over the years 2023/2024 and a response rate of 75%**. This information, enriched with additional cross-checks, has proven essential to identify previously unknown high-profile suspects, to uncover hidden connections, to map criminal financial circuits, and to freeze and recover illicit assets. At the same time, Europol still observes some **delays in the responses**, with an average of a 50-days response delay undermining the effectiveness of cross-border financial investigations.

As regards the **challenges in obtaining information from obliged entities**[18], several issues remain. Some of these problems are common to the intelligence gathering phase and during criminal proceedings: faced with large amounts of financial data to process, authorities have pointed to the need for a common format of the information financial entities provide to authorities, technological solutions to process information from various sources and export/import systems to automate the request and receipt of financial information through secure channels.

In addition, when building up a case, law enforcement authorities cannot usually request information directly from obliged entities in the pre-investigative phase. Considering the difficulties that this poses to law enforcement agencies, especially in cases such as economic crimes where the financial trail is key to establish whether criminal acts have been committed, more than two thirds of law enforcement authorities consulted called for having the possibility of directly exchanging information with obliged entities at an early stage of the investigations, mostly for reasons of speed. At the same time, some law enforcement authorities preferred to maintain the intermediary role of Financial Intelligence Units in exchanges with obliged

---

enforcement or judicial cooperation mechanisms and channels. See EU FIUs Platform, 'Mapping Exercise and Gap Analysis on FIUs' Powers and Obstacles for Obtaining and Exchanging Information' (2016) at https://ec.europa.eu/transparency/expert-groups-register/core/api/front/expertGroupAddtitionalInfo/33583/download.

A similar issue, encountered with regard to the exchange of tax information, was resolved after the entry into force of Council Directive (EU) 2023/2226 of 17 October 2023 amending Directive 2011/16/EU on administrative cooperation in the field of taxation, which provided that such information "may be used for the assessment, administration and enforcement of the national law of Member States concerning the taxes referred to in Article 2 as well as […] anti-money laundering and countering the financing of terrorism" (Article 16 (1) consolidated version of Directive 2011/16/EU).

[18] Entities that are obliged to take appropriate steps to identify and assess the risks of money laundering and terrorist financing pursuant to the Anti-Money Laundering rules, such as credit institutions, financial institution, certain professionals (e.g. notaries, lawyers, auditors, external accountants, etc.), trust or company service providers, estate agents, traders, football clubs, etc.

entities in this phase, on the basis that this ensures confidentiality of law enforcement investigations.

Moreover, **insofar as the power for law enforcement to request information from obliged entities is limited to criminal proceedings, this implies the use of the European Investigation Order (EIO) for exchanging information across borders**[19]. According to some law enforcement authorities, this represents a considerable challenge: the EIO can take up to 30 days to be recognised, while criminals move money across borders in the matter of minutes if not seconds. By contrast, some Member States where law enforcement authorities can directly exchange with obliged entities at an early investigative stage have signalled that they are also able to exchange information quicker across borders. At the same time, it is important to remind that the limitation of such power to the investigative stage and the requirement of judicial authorisation in most Member States reflects the importance of protecting the sensitive information which financial transaction data is.

**Another challenge** often raised in relation to cooperation with obliged entities is **accessing information on crypto assets**. Several Member States have highlighted the lack of replies to law enforcement requests from virtual asset service providers based in third countries but offering services within the EU. This is a considerable issue considering that the criminal exploitation of cryptocurrency as a payment method is encountered not only in cybercrimes but also increasingly in crime areas such as drug trafficking or migrant smuggling[20]. Among the **best practices** flagged by Member States to address some of the challenges when cooperating with obliged entities is the establishment of public-private partnerships among obliged entities, Financial Intelligence Units and competent authorities, where dynamic flows of information travel both ways to enable closer and targeted collaboration on concrete cases. While about half of Member States present some form of public-private cooperation, in most cases it is limited to the exchange of typologies and trends. Where the partnerships allow for the exchange of operational information, authorities and financial actors can work together in a secure environment to uncover and disrupt illicit financial schemes, delivering valuable information for investigators[21].

Overall, the capacity of law enforcement authorities to obtain and process financial information has increased, thanks to the improvements brought by the Directive as well as by other developments in the area of public-private cooperation and inter-agency collaboration. At the same time, a number of challenges remain, such as the insufficient capacities for processing large amounts of data, the barriers for authorities to exchange with obliged entities when building up the case, and the cross-border challenges, considering the speed at which money can be transferred across borders. Some of the models developed over the last years, notably public-private partnerships, help in addressing these challenges, while the recent legislative instruments adopted, such as the new Anti-Money Laundering rules and Directive (EU) 2024/1260, will also contribute to a better access by competent authorities to financial information. Considering the need to implement these important initiatives, **it is not possible to conclude, at this point in time, about the need and proportionality for extending the definition of financial information.**

[19] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1, ELI: http://data.europa.eu/eli/dir/2014/41/oj).

[20] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

[21] Policy-Summary-EFIPPP-Practical-Guide-operational-cooperation-1.pdf

## 4. CONCLUSION

Directive 2019/1153 has largely contributed to improving the capacity of law enforcement authorities to access financial and other information for preventing, detecting, investigating and prosecuting criminal offences. **Although some gaps remain and should be addressed, the majority of Member States have transposed the Directive in a way that ensures compliance with the aims and level of safeguards provided for in the Directive**. Without prejudice to any enforcement action that could be taken to remedy remaining breaches, the Commission will continue working with the Member States to ensure that Directive 2019/1153 is applied effectively. As a first step, the Commission plans to adopt, in 2026, an implementing act to ensure that financial entities provide transaction records in a common format across the EU, a long-standing demand of law enforcement authorities, as required by the amendment to the Directive adopted in May 2024[22].

At the same time, the Directive is part of a broader toolbox of instruments aimed at fighting money laundering and criminal finances, some of which have been recently reinforced. Considering **the European Commission's policy of simplification and burden reduction**, this report presents the links of the Directive with these instruments, and with other pieces of legislation, and the practical implications of some of the Directive's provisions, as well as their relevance for ensuring adequate safeguards. Those findings can be a basis for further discussions with stakeholders to address some of the challenges in terms of administrative burden and regarding potential discrepancies with other legislative instruments.

Finally, it is too soon to conclude on the need and proportionality of extending the definition of financial information. Apart from the measures introduced by the Directive, there is still a variety of factors with an impact on the ability of law enforcement authorities to obtain and process financial information that remain to be improved, such as the capacity of law enforcement to process large amounts of data, the use of public-private partnerships in financial investigations or swift cross-border exchange of information. Moreover, the full extent of the improvements brought by recent legislation on financial investigations has not unfolded yet, given that relevant legislation is still in the process of being transposed or entering into force.

[22] Article 6a of Directive (EU) 2019/1153.