EUROPEAN
COMMISSION

Strasbourg, 17.4.2018
COM(2018) 213 final

2018/0105 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

{SWD(2018) 114 final} - {SWD(2018) 115 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Criminal groups, including terrorists, operate across different Member States and their assets, including bank accounts, are usually located across the EU or even outside of it. They make use of modern technology that allows them to transfer money between several bank accounts and between different currencies in a matter of hours.

Timely information is essential for criminal investigations on serious crimes. Lack of financial information may result in missed opportunities to investigate serious crimes, disrupt criminal activities, stop terrorist plots, and detect and freeze proceeds of crime. Lack of information on all accounts belonging to a suspect may lead to only partial freezing of assets which may alert the suspect, who is then able to remove the undetected funds from the other accounts. Many investigations come to a dead end because of failure to secure timely, accurate and comprehensive access to the relevant financial data.[1]

The current mechanisms for accessing and exchanging financial information are slow compared to the fast pace at which funds can be transferred across Europe and globally. Too much time is required to obtain financial information, reducing the effectiveness of investigations and prosecutions. There is a need to find quicker and more effective ways to access and exchange information on bank accounts, financial information and financial analysis. An increased number of successful criminal investigations will result in an increased number of convictions and asset confiscations. This will contribute to disrupting criminal activities and increasing the security in the Member States and across the Union.

On 2 February 2016, the Commission adopted an Action Plan on strengthening the fight against terrorist financing[2] which presented how the Commission would seek to upgrade the the 4th Anti-Money Laundering Directive (4AMLD).[3] Furthermore, the plan also called for a mapping of obstacles to the access to, exchange and use of information and to the operational cooperation between FIUs to be followed up by legislative proposals if appropriate.

The Union co-legislators agreed in December 2017 on a number of significant changes to the 4AMLD (5th Anti-Money Laundering Directive (5AMLD)). They include the mandatory establishment of national centralised bank account registries or data retrieval systems in all Member States, to which Financial Intelligence Units (FIUs) and anti-money laundering authorities would have access.

However, the Money Laundering Directives, due to their legal basis in Article 114 of the Treaty on the Functioning of the European Union (TFEU), do not set out the precise conditions under which Member States' authorities and bodies competent for the prevention, detection, investigation or prosecution of criminal offences (hereafter competent authorities) can use financial and other information for the prevention, detection, investigation or

---

1 The Europol Report "From suspicion to action: converting financial intelligence into greater operational impact", which was published in 2017, highlighted these problems and the need for better access of law enforcement authorities to financial information.

2 COM(2016) 50 final.

3 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 of 5.6.2015, p. 73).

prosecution of certain criminal offences. Instead, they mostly deal with the preventive efforts to address money laundering, associated predicate offences and terrorist financing, and the thrust of the obligations they lay down are directly linked to the "obliged entities", i.e. economic operators, undertakings and professionals.

Most competent authorities currently do not have direct access to the information on the identity of bank account holders, held in the centralised bank account registries or data retrieval systems. Such registries and systems are currently operational in 15 Member States, while only in 6 Member States competent authorities (and not all of them) have direct access. Therefore, they usually request the information either via blanket requests sent to all financial institutions in their Member State or, if they have been granted indirect access, via a request to an intermediary.

A blanket request implies that the competent authority has to wait for a reply from each financial institution. This carries the real risk of significant delays which may prejudice criminal investigations. This has also implications for cross-border cooperation. The time needed to obtain financial information from banks in different Member States often varies and may further delay cooperation. Article 32a(4) of the 5AMLD requires the Commission to submit, by June 2020, a report to the European Parliament and to the Council assessing the possible future interconnection of centralised bank account registries. The Commission will present its assessment and findings by mid-2019.

This proposal therefore provides for direct access to the national centralised bank account registries or data retrieval systems to competent authorities. The competent authorities to which access is provided for also include tax authorities and anti-corruption authorities in their capacity to conduct criminal investigations under national law. They also include the Asset Recovery Offices which are responsible for the tracing and identification of criminal assets in view of their possible freezing and confiscation. In order to ensure that “crime does not pay” and that criminals are deprived of their profits,[4] it is necessary to ensure that Asset Recovery Offices are provided with adequate tools to access information which is required for the execution of their tasks. Europol will also be provided with indirect access through Member States' National Units. Europol does not conduct criminal investigations, but supports actions by the Member States. Having no access to financial information, including the one contained in the national centralised bank account registries and data retrieval systems, prevents Europol from exploiting the full potential of its analytical capabilities. These limitations were stressed and explained in the Europol Report "From suspicion to action" published in 2017.

As regards the cooperation between FIUs and between FIUs and competent authorities despite the fact that this is already regulated under the 4th Anti-Money Laundering Directive (4AMLD) both FIUs and competent authorities continue to be faced with obstacles in their interactions. The 28 FIUs[5] within the EU presented a joint mapping report in December 2016 to identify which are these obstacles and propose solutions. The Commission's Staff Working

[4] In the report, “Does crime still pay?: criminal asset recovery in the EU" (2016), Europol estimated that, between 2010 and 2014, the value of the assets frozen or seized in the European Union represented 2.2% of the estimated proceeds of crimes, while the value of the assets confiscated represented about 1.1% of such estimated proceeds. https://www.europol.europa.eu/newsroom/news/does-crime-still-pay

[5] FIUs are operationally independent and autonomous units with the authority and capacity to take autonomous decisions to analyse, request and disseminate their analyses to competent authorities, where there are grounds to suspect money laundering, associated crimes or terrorist financing.

Document on improving cooperation between FIUs, published in June 2017[6], takes stock of the results of the mapping report and identifies issues that could be addressed through guidance and enhanced cooperation as part of the work carried out by the EU FIUs' Platform and other issues that would require regulatory solutions.

In addition, the European Parliament, expressing regret at "the lack of greater harmonisation in Member States' approaches to fighting financial crime", called for the Union to tackle the need for more effective exchange of information and closer coordination between national authorities concerned in order to achieve better results, including by enacting the necessary Union legislation.

This proposal therefore provides for measures to facilitate the use of financial and other information in order to prevent and combat serious crime more effectively, including across borders. More specifically, it increases the competent authorities' timely access to information contained in the centralised bank account registries or data retrieval systems as established by the 4AMLD. It also maintains a high level of protection of fundamental rights, in particular the right to the protection of personal data, and reduces the administrative burden, related to the procedure of blanket requests, for both competent authorities and the banking sector. Direct access is the most immediate type of access to financial information.

The proposal also facilitates cooperation between FIUs and between FIUs and competent authorities. It defines what type of information (financial information, financial analysis, law enforcement information) can be requested by competent authorities and FIUs respectively as well as the exhaustive list of criminal offences for which each authority can exchange information always on a case-by-case basis, which means for a specific case under investigation. It provides for deadlines within which FIUs should exchange the information and requires the use of a secure channel of communication so as to improve and speed up their exchanges. Finally, it requires Member States to designate all the competent authorities entitled to request information. It ensures a broader and more effective but at the same time proportionate exchange of information.

In this context, the Commission stresses the need to provide Financial Intelligence Units with adequate resources to fulfil their tasks, as required by the 4AMLD. Moreover, as required by Article 65(2) of the 5AMLD, the Commission will, by June 2019, assess the framework for FIUs cooperation with third countries and obstacles and opportunities to enhance cooperation between FIUs in the Union, including the possibility of establishing a coordination and support mechanism.

- **Consistency with existing policy provisions in the policy area**

The current proposal for a Directive is part of the European Agenda on Security adopted in April 2015[7] that called for additional measures in order to disrupt serious and organised crime and its follow up Action Plan on strengthening the fight against terrorist financing.

As stated above, the 4AMLD and 5AMLD are based on an internal market legal basis and deal with preventive efforts to address money laundering, associated predicate offences and terrorist financing. This proposal complements and builds on the preventive side of the Money Laundering Directives and reinforces the legal framework from the point of view of police cooperation.

---

6 SWD (2017)275.

7 COM (2015) 185 final of 28 April 2015.

Furthermore, this proposal for a Directive reinforces and builds the Union criminal law framework with regard to the fight against serious offences, in particular Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol)[8].

- **Consistency with other Union policies**

The proposed Directive is in line with policy aims pursued by the Union, and in particular the reformed data protection regime, stemming from Directive (EU) 2016/680, and in line with the relevant case law of the Court of Justice of the European Union.

This legislative initiative is also consistent with the aims of the Union's internal market development, in particular the single market for payments establishing a safer and more innovative payment services across the EU, namely rules laid down in Directive (EU) 2015/2366[9].

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The power to act is conferred by Article 87 (2) TFEU which enables the European Union to establish measures on police cooperation involving all the Member States' competent authorities (including police, customs and other specialized law enforcement services), in particular concerning the collection, storage and exchange of information relevant for the prevention, detection and investigation of criminal offences (letter a) and common investigation techniques in relation to the detection of serious forms of organised crime (letter b).

- **Subsidiarity (for non-exclusive competence)**

According to Article 67 TFEU, it is the Union's objective to provide citizens with a high level of security by preventing and combating crime. Action of the Union in this field should be taken only if, and in so far as, this objective cannot be sufficiently achieved by the Member States and can be better achieved by the Union.

In accordance with the principle of subsidiarity as set out in Article 5(3) of the Treaty on European Union (TEU), the objectives of the proposal cannot be sufficiently achieved by Member States and can therefore be better achieved at the Union level. The proposal does not go beyond what is necessary to achieve those objectives. In line with existing rules, under this proposal Member States have the right to adopt or retain measures that are more stringent than those set out in Union law.

The perpetrators of criminal offences are often active across various Member States. In particular, organised crime groups are often set up internationally and operate with financial assets across borders. Due to their transnational nature, the terrorist and criminal threats affect the EU as a whole and, therefore, require a European response. Criminals may exploit, and will benefit from, the lack, or the lack of an efficient use, of financial information by competent authorities.

---

[8] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

[9] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010.

Union action aims to generate added value by providing a harmonised approach that would strengthen domestic and cross-border cooperation in financial investigations on serious crimes and terrorism. In addition, action at the Union level will help to ensure harmonised provisions, including on data protection, whereas if Member States are left to legislate independently, a harmonised level of safeguards will be difficult to achieve.

- **Proportionality**

In accordance with the principle of proportionality, as set out in Article 5(4) TEU, this proposal is limited to what is necessary and proportionate in order to facilitate the use and sharing of relevant financial and other information by the public authorities that have a duty to protect Union citizens.

The proposed initiative aims to grant certain competent authorities with direct access to the national centralised bank account registries and data retrieval systems. It requires Member States to designate, among its authorities competent for the prevention, detection, investigation or prosecution of criminal offences, competent authorities empowered to access and search these registries. They shall include the Asset Recovery Offices and the Europol National Units. In addition, Europol will be granted indirect access, only on a case-by-case basis, to the information held in the national centralised bank account registries and data retrieval systems, in order to fulfil its tasks in accordance with its mandate.

Access to the national centralised bank account registries and data retrieval systems will be granted solely to a limited set of information (e.g. the owner's name, date of birth, bank account number) which is strictly necessary to identify in which banks the subject of an investigation holds bank accounts. The authorities will not be able to access the content of the bank accounts; neither the balance of the accounts nor details on the transactions. Once the competent authorities identify in which financial institution the subject of an investigation holds a bank account, in most cases they will have to approach the respective institution and request further information, e.g. a list of transactions (usually on the basis of a judicial authorisation).

The proposed measures will not bring any changes to the core functions or the organisational status of the FIUs, which will continue to perform the same functions as set out in national and Union legislation already in force.

The proposal facilitates the cooperation between FIUs as well as cooperation between FIUs and competent authorities. This framework for exchange of information is granted under specific conditions and is limited to specific crimes (money laundering and predicate offences, financing of terrorism) as well as to serious crimes. It contains a number of safeguards for protection of privacy and personal data, always with a view to improve domestic and cross-border cooperation and exchange of information and to prevent criminals from exploiting the differences between national legislations to their advantage. The cases and conditions where exchange of financial data is permitted are also limited to an exhaustive list of competent authorities. Those competent authorities will only be enabled to access and exchange financial data in respect to a set list of criminal offences and subject to national procedural safeguards and privacy safeguards.

- **Choice of the instrument**

This proposal takes the form of a Directive, so as to only set out a goal that Member States must achieve, while allowing them to devise their own laws on how to reach these goals. Other means would not be adequate because the aim of the measure is the approximation of the Member States' legislation on which authorities shall be granted access to the national

centralised bank account registries and data retrieval systems. Hence, no instrument other than a Directive would be appropriate.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

As regards the access of competent authorities to centralised bank account registries:

The following authorities were consulted by the Commission in respect of this proposal: law enforcement authorities, the Asset Recovery Offices, the national authorities that investigate corruption and financial crime cases, Financial Intelligence Units, OLAF and Europol, national Data Protection Authorities and the European Data Protection Supervisor (EDPS), banks, financial institutions, banking associations at national or EU level, the authorities responsible for managing the existing centralised bank account registries and data retrieval systems (or entrusted with their development where none have been established yet), and the general public.

The methods and tools used included:

- the consultation on the Inception Impact Assessment (launched on 9 August 2017 until 6 September 2017, where any interested party could provide feedback);
- a public consultation (open to feedback from any interested party for 12 weeks from 17 October 2017 to 9 January 2018);
- a targeted survey addressed to the Asset Recovery Offices and Anti-Corruption Authorities of the Member States in June 2016;
- an expert meeting on broadening law enforcement access to centralised bank account registries, which took place on 25-26 October 2017;
- as a follow-up of the expert meeting on broadening law enforcement access to centralised bank account registries the Commission sent additional questions to several delegations;
- a consultation with the Asset Recovery Offices during the EU Asset Recovery Offices' Platform meeting on 12-13 December 2017;
- a high level meeting assessing the need for additional measures to facilitate access to financial information – 20 November 2017;
- a meeting to discuss cooperation between FIUs and law enforcement authorities, on 6-7 March 2018.

As regards access to centralised bank account registries, the law enforcement authorities fully supported the initiative and confirmed that:

- swift access to information on bank accounts is crucial for the effective performance of their tasks;
- the current practice of issuing “blanket requests” is highly unsatisfactory from an “efficiency” point of view; results in a considerable administrative burden for both the banks and themselves and slows down investigations;

- different approaches are deployed in the Member States regarding law enforcement access. In some Member States, a number of police authorities, Asset Recovery Offices and anti-corruption agencies have access, whereas in others they do not.

The banking associations reiterated their full commitment to the fight against money laundering and terrorist financing and argued that:

- the decision whether a system should be centralised or decentralised should be taken at the national level;
- the initiative should duly take care not to harm the individuals' fundamental rights to data privacy.

The EDPS and the national data protection authorities emphasised that:

- the practice of sending blanket requests is not satisfactory from a data protection point of view;
- there is a need for a strong justification to broaden access and the necessary safeguards have to be provided;
- any future legislative proposal needs to be fully compliant with the European data protection framework.

This input was duly taken into account in preparing the proposal.

As regards the exchange of information between FIUs and competent authorities:

Consultation of FIU and competent authorities

The Commission organised in March 2018 a meeting to discuss cooperation between FIUs and law enforcement authorities. Member States were consulted and provided input on the following issues:

(i) FIU access to law enforcement authorities information domestically, where it seems that all FIUs have access, whether direct or indirect (through liaison officers of the police sitting in the FIUs). The main difference in Member States is to the type of information that FIUs have access. FIUs acknowledged that harmonisation of the types of information they have access to would be important;

(ii) competent authorities access to financial information via the FIUs, where it seems that no FIU gives direct access to competent authorities to its databases. However, the police FIUs are able to easily respond to requests for information from competent authorities. For administrative FIUs it is not so easy;

(iii) Diagonal cooperation, i.e. cooperation between an FIU in one Member States with competent authorities in another Member States, which can be direct or indirect (i.e. via the FIU in the Member State of the requesting competent authorities), where all Member States opposed to the idea of direct diagonal cooperation and all were in favour of indirect diagonal cooperation;

(iv) Cooperation with Europol, where 8 FIUs already exchange information with Europol. FIUs in general expressed an interest in exchanging information with Europol, on the condition that exchanges are reciprocal.

- **Collection and use of expertise**

A mapping exercise has been conducted within the Union FIUs' Platform to identify practical obstacles to access to, exchange and use of information as well as operational cooperation, with a view to provide results before the end of 2016.

The consultation started with an online EUSurvey that was launched on 14 April 2016 to gather information from FIUs. This survey was divided into nine thematic areas, ranging from FIUs' domestic features to the capacity to engage in FIU-to-FIU cooperation in its various forms and comprised of 290 questions.

The final report adopted in December 2016 is made public on the website for the "Register Commission of expert groups and other similar entities" as an annex to the meeting minutes of the 31st meeting of the EU FIUs' Platform at http://ec.europa.eu/transparency/regexpert/.

The Commission also relied on a Report by the Financial Intelligence Group of Europol, "From suspicion to action: converting financial intelligence into greater operational impact", issued in 2017.

- **Impact assessment**

This proposal is supported by an impact assessment which assessed the ways to expand access to financial information for competent authorities for the investigation of crimes, looking at two issues: the issue of access of competent authorities to centralised bank account registries or retrieval systems, and the issue of enhancing cooperation between Financial Intelligence Units and competent authorities.

An impact assessment report was submitted to the Regulatory Scrutiny Board on 31 January 2018. The Regulatory Scrutiny Board issued a positive opinion with reservations on 26 March 2018.

The Impact Assessment examined the following options:

(1) Baseline Option.

(2) Non-legislative Option – Option 0.

(3) Legislative Options:

- Option A related to the types of crimes for the prevention and combat of which the competent authorities would be able to access and exchange information.

  Option A.1 was limited to the prevention and combat of money laundering, the associated predicated offences and terrorism financing.

  Option A.2 was limited to the prevention and combat of Eurocrimes.

  Option A.3 was limited to the prevention and combat of serious crimes as per the Europol Regulation.

- Option B examined the modalities of access to the data.

  Option B.1 related to modalities of access of competent authorities to the central bank account registries with Option B.1.a providing for direct access and Option B.1.b providing for indirect access.

Option B.2 related to the modalities of access of competent authorities to all financial information with Option B.2.a providing for a direct access to information from financial institutions and Option B.2.b with an indirect access via the Financial Intelligence Units.

Option B.3 related to the exchange of information between Financial Intelligence Units and for requests for information by Financial Intelligence Units to the competent authorities, of which Option B.3.a examined a direct cooperation, whilst Option B.3.b examined the option of establishing a central EU FIU.

- Option C examined the categories of authorities which would benefit from access to and exchanges of information. Option C.1 included the competent authorities of the Data Protection Police Directive, while Option C.2 extended the cooperation with other authorities, namely the Asset Recovery Offices, Europol and OLAF.

The options were assessed against economic, social and fundamental rights impacts.

This proposal corresponds to the preferred policy options considered in the Impact Assessment.

The preferred option, as far as access to centralised bank account registries is concerned, is the adoption of an EU legislative instrument which would give direct access to competent authorities. This access should be given for the purposes of criminal investigations on all forms of serious crimes referred to in Article 3(1) of the Europol Regulation. Europol's access should be an indirect access, but investigations supported by Europol would also benefit from an access to information held in centralised bank account registries.

Direct access to the central bank account registries and retrieval systems is allowed under the preferred option since they contain limited information. The interference with the right to the protection of personal data will be kept to the minimum under the preferred option. The access rights are limited and are targeted only to the authorities necessary in each case, thereby ensuring proportionality in the interference with the protection of personal data.

The preferred option would also include provisions in order to facilitate the exchanges of data between FIUs, as well as reciprocally between FIUs and competent authorities. The possibility of Europol to also request information from FIUs would also be regulated. Given the sensitivity of the information, the preferred option would foresee strict data protection safeguards.

- **Regulatory fitness and simplification**

In October 2000, Council Decision 2000/642/JHA was adopted concerning arrangements for cooperation between FIUs of Member States with respect to exchanging information. The subject-matter of this Council Decision is regulated by other Union acts and the Council Decision has therefore currently no added value. Therefore, this proposal repeals the Decision.

- **Fundamental rights**

This initiative will provide competent authorities with access to mechanisms that centralise personal data relating to natural persons or from which personal data can be retrieved. This will have an impact on the fundamental rights of the data subjects. In particular, it will interfere with the right to privacy and the right to the protection of personal data, respectively under Articles 7 and 8 of the EU Charter of Fundamental Rights.

With respect to the right to privacy under Article 7 of the Charter, although the scale of the impact is significant given the number of people that would be affected, the interference will be relatively limited in terms of gravity as the accessible and searchable data does not cover financial transactions or the balance of the accounts. It will only cover a limited set of information (e.g. the owner's name, date of birth, bank account number) which is strictly necessary to identify in which banks the subject of an investigation holds bank accounts.

Regarding the right to the protection of personal data under Article 8 of the Charter, bank account information as well as other type of financial information constitutes or can constitute personal data and access to this data in accordance with this legislative initiative constitutes processing of personal data. All provisions in the Data Protection Police Directive apply.

The proposal specifies the purposes for processing personal data and requires a list of designated competent authorities entitled to request information. Exchanges of information will be limited on a case-by-case basis, meaning only where relevant to a specific case for the purpose of combating an exhaustive list of specified serious criminal offences.

The proposal also sets specific provisions regarding logging, records of information requests, restrictions to rights and processing of special categories of personal data ("sensitive data").

Europol through the European National Units will also be granted indirect access to the information held in the national centralised bank account registries and data retrieval systems and offered the possibility to exchange data with Financial Intelligence Units, for the purpose of fulfilling its tasks (support and strengthen action by Member States to prevent, detect, investigate and prosecute specific offences within its competence) in accordance with its mandate. All safeguards foreseen in Chapters VI and VII of Regulation (EU) 2016/794 apply.

As regards procedural rights, removing the need for judicial authorisation that exists in some Member States would have a very serious impact. Therefore the exchanges of information between Financial Intelligence Units and competent authorities will be subject to national procedural safeguards.

4. BUDGETARY IMPLICATIONS

The proposal has no implications for the EU budget.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The proposal provides for reporting to the European Parliament and the Council on the implementation of the Directive, three years after the date of transposition, and every three years thereafter.

The Commission will also evaluate the effectiveness, efficiency, relevance, coherence and EU added value of the resulting legal framework, no sooner than six years after the date of the transposition to ensure that there is enough data relating to the functioning of the Directive. The evaluation shall include stakeholders' consultations to collect feedback on the effects of the legislative changes. The benchmark against which progress will be measured is the baseline situation when the legislative act enters into force. The Commission will present a report on the functioning of the Directive to the European Parliament and the Council. The report shall also include an evaluation of how fundamental rights and principles recognised by the EU Charter of Fundamental Rights of the European Union have been respected.

In order to ensure an effective implementation of the measures foreseen and monitor its results, the Commission will work closely with relevant stakeholders from national authorities of the Member States. The Commission will adopt a programme for monitoring the outputs, results and impacts of this Directive. The monitoring programme shall set out the means by which and the intervals at which the data and other necessary evidence will be collected. Member States should report to the Commission on an annual basis, some information that is considered essential to effectively monitor the application of this Regulation. The annual reporting from Member States should cover, in particular, the number of searches the designated national competent authorities carried out for the purposes of obtaining bank account information from the national centralised bank account registries and/or data retrieval systems, as well as the conditions for issuing a request, the grounds for refusal, the conditions for further use, the time limits for responding to a request, the application of safeguards when processing personal data, and an account of the international cooperation and information exchange between Financial Intelligence Units and competent authorities.

For the purposes of reporting, the Commission shall take into account the specific statistics that Member States will be required to submit.

- **Explanatory documents (for directives)**

The proposal does not require explanatory documents for transposition.

- **Detailed explanation of the specific provisions of the proposal**

Article 1 sets out the subject matter, indicating that the act facilitates access by competent authorities to financial information and bank account information for the prevention, detection, investigation or prosecution of serious criminal offences. It also sets out that the act facilitates access by Financial Intelligence Units to law enforcement information.

Article 2 provides definitions of terms used in the proposal.

Article 3 provides for an obligation to Member States to designate which are their competent authorities empowered to access and search the national centralised bank account registries and to request and receive information. The Article also provides for the publication of such competent authorities in the *Official Journal of the European Union*.

Article 4 provides for a direct access to the registries for the designated competent authorities and sets out the purposes for which direct access and search is provided, namely for preventing, detecting, investigating or prosecuting the offences listed in Annex I of Regulation (EU) 2016/794, the Europol Regulation, or supporting a criminal investigation, including the identification, tracing, freezing and confiscation of the assets related to such investigations.

Article 5 lays down the conditions for the access and search by the designated competent authorities.

Article 6 requires Member States to monitor the access and search by the designated competent authorities. Any access in accordance with this Directive has to be logged by the authorities operating the centralised bank account registries, and particular elements of the logs are listed.

Article 7 provides for an obligation to ensure that each Financial Intelligence Unit is required to reply to requests for financial information or financial analysis by a Member State's designated competent authorities. National procedural safeguards apply to this procedure.

Article 8 provides for an obligation to ensure that a Member State's designated competent authorities are required to reply to requests for law enforcement information issued by a Financial Intelligence Unit. National procedural safeguards apply to this procedure.

Article 9 provides for the exchange of information between Financial Intelligence Units of different Member States, including time limits to reply and secure channels for exchanging the information.

Article 10 lays down the conditions for access by Europol to bank account information and for the exchange of information between Europol and Financial Intelligence Units.

Article 11 provides an obligation that the processing of personal data be performed only by the persons within Europol that have been specifically designated and authorised to perform these tasks.

Article 12 sets out the scope of application of Chapter V.

Article 13 provides for the conditions for the processing of sensitive personal data.

Article 14 provides for an obligation for Member States to maintain records relating to all requests under the proposal.

Article 15 sets out conditions for limiting the data subject's rights of access to personal data in certain cases.

Article 16 sets out that the Commission will establish a detailed programme for monitoring the outputs, results and impacts of this Directive. It requires that Member States will provide the Commission with this information with a view to assist the Commission in the exercise of the duties under Article 18. This provision also provides for an obligation on Member States to maintain specific statistics relating to this proposal and to communicate them to the Commission.

Article 17 provides for the relationship of this proposal with bilateral or multilateral agreements either by the Member States or the Union.

Article 18 provides for an obligation on the Commission to report on the implementation of this Directive to the European Parliament and the Council three years after the transposition and every 3 years thereafter.

Article 19 sets out the periods for the transposition of this Directive.

Article 20 repeals Council Decision 2000/642/JHA, which is currently redundant given the 4 AMLD.

2018/0105 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 87(2) thereof,

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Facilitating the use of financial information is necessary to prevent, detect, investigate or prosecute serious crimes.

(2) In order to enhance security in the Member States and across the Union, it is necessary to improve access to information by Financial Intelligence Units and public authorities responsible for the prevention, detection, investigation or prosecution of serious forms of crimes, to enhance their ability to conduct financial investigations and to improve cooperation between them.

(3) In its Action Plan to strengthen the fight against terrorist financing[3], the Commission committed to explore the possibility of a dedicated legal instrument to broaden the access to centralised bank account registries by Member States' authorities, namely authorities competent for the prevention, detection, investigation or prosecution of criminal offences, Asset Recovery Offices, tax authorities, anti-corruption authorities. Moreover, the 2016 Action Plan also called for a mapping of obstacles to the access to, exchange and use of information and to the operational cooperation between Financial Intelligence Units.

(4) Directive (EU) 2015/849[4] requires Member States to establish centralised bank account registries or data retrieval systems allowing the timely identification of the persons holding bank and payment accounts and safe deposit boxes.

---

1 OJ C , , p. .

2 OJ C , , p. .

3 COM (2016) 50 of 2.2.2016.

4 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

(5) Pursuant to Directive (EU) 2015/849, the information held in those registries is directly accessible to Financial Intelligence Units and is also accessible to national authorities competent for the prevention of money laundering, its predicate offences and terrorist financing.

(6) Immediate and direct access to the information held in centralised bank account registries is often indispensable for the success of a criminal investigation or for the timely identification, tracing and freezing of the related assets in view of their confiscation. Direct access is the most immediate type of access to the information held in centralised bank account registries. This Directive should therefore lay down rules granting direct access to information held in centralised bank account registries to designated Member States' authorities and other bodies competent for the prevention, detection, investigation or prosecution of criminal offences.

(7) Given that in each Member States there are numerous authorities or bodies which are competent for the prevention, detection, investigation or prosecution of criminal offences, and in order to ensure a proportionate access to financial and other information under the present Directive, Member States should be required to designate which authorities should be empowered to have access to the centralised bank account registries and request information from Financial Intelligence Units for the purposes of this Directive.

(8) Asset Recovery Offices should be designated among the competent authorities and have direct access to the information held in centralised bank account registries when preventing, detecting or investigating a specific serious criminal offence or supporting a specific criminal investigation, including the identification, tracing and freezing of assets.

(9) To the extent that tax authorities and anti-corruption agencies are competent for the prevention, detection, investigation or prosecution of criminal offences under national law, they should also be considered authorities that can be designated for the purposes of this Directive. Administrative investigations should not be covered under the present Directive.

(10) The perpetrators of criminal offences, in particular criminal groups and terrorists, often operate across different Member States and their assets, including bank accounts, are often located in other Member States. Given the cross-border dimension of serious crimes, including terrorism, and of the related financial activities, it is often necessary for competent authorities carrying out investigations to access information on bank accounts held in other Member States.

(11) The information acquired by competent authorities from the national centralised bank account registries can be exchanged with competent authorities located in a different Member State, in accordance with Council Framework Decision 2006/960/JHA[5] and Directive 2014/41/EU[6] of the European Parliament and the Council.

(12) Directive (EU) 2015/849 has substantially enhanced the Union legal framework that governs the activity and cooperation of Financial Intelligence Units. The powers of

---

repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141 of 5.6.2015, p. 73.

5 Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386 of 29.12.2006, p. 89.

6 Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130 of 1.5.2014, p. 1.

Financial Intelligence Units include the right to access the financial, administrative and law enforcement information that they require to combat money laundering, the associated predicate offences and terrorist financing. Nevertheless, Union law does not lay down all specific tools and mechanisms that Financial Intelligence Units must have at their disposal in order to access such information and accomplish their tasks. Since Member States remain entirely responsible for the setting up and deciding the organisational nature of Financial Intelligence Units, different Financial Intelligence Units have varying degrees of access to regulatory databases which leads to an insufficient exchange of information between law enforcement or prosecution services and Financial Intelligence Units.

(13) In order to enhance legal certainty and operational effectiveness, this Directive should lay down rules to strengthen the Financial Intelligence Units' ability to share information with their designated competent authorities for all serious criminal offences.

(14) This Directive should also set out a clearly defined legal framework to enable Financial Intelligence Units to request relevant data stored by designated competent authorities in order to enable them to prevent and combat money laundering, the associated predicate offences and terrorist financing effectively.

(15) Sharing information between Financial Intelligence Units and with competent authorities should only be permitted where it is necessary on a case-by-case basis, either for the prevention, detection, investigation or prosecution of serious criminal offences or for money laundering, the associated predicate offences and terrorist financing.

(16) In order to prevent and combat money laundering, the associated predicate offences and terrorist financing more effectively and to reinforce its role in providing financial information and analysis, a Financial Intelligence Unit should be empowered to exchange information or analysis already in its possession or which can be obtained from obliged entities at the request of another Financial Intelligence Unit or of a competent authority in its Member State. This exchange should not hamper a Financial Intelligence Unit's active role in disseminating its analysis to other Financial Intelligence Units where that analysis reveals facts, conduct or suspicion of money laundering and terrorist financing of direct interest to those other Financial Intelligence Units. Financial analysis covers operational analysis which focuses on individual cases and specific targets or on appropriate selected information, depending on the type and volume of the disclosures received and the expected use of the information after dissemination as well as strategic analysis addressing money laundering and terrorist financing trends and patterns. However, this Directive should be without prejudice to the organisational status and role conferred to Financial Intelligence Units under the national law of Member States.

(17) Time limits for exchanges of information between Financial Intelligence Units are necessary to ensure quick, effective and consistent cooperation. Sharing information necessary to solve cross-border cases and investigations should be carried out with the same celerity and priority as for a similar domestic case. Time limits should be provided to ensure effective sharing of information within reasonable time or to meet procedural constraints. Shorter time limits should be provided in duly justified cases, where the requests relate to specific serious criminal offences, such as terrorist offences and offences related to a terrorist group or activities as laid down in Union law.

(18) The use of secure facilities for the exchange of information, in particular the decentralised computer network FIU.net (the 'FIU.net'), which is managed by Europol since 1 January 2016, or its successor and the techniques offered by FIU.net, should be used for exchanges of information between Financial Intelligence Units.

(19) Given the sensitivity of financial data that should be analysed by Financial Intelligence Units and the necessary data protection safeguards, this Directive should specifically set out the type and scope of information that can be exchanged between Financial Intelligence Units and with designated competent authorities. This Directive should not bring any changes to currently agreed methods of data collection.

(20) Under its specific competences and tasks as laid down in Article 4 of Regulation (EU) 2016/794 of the European Parliament and of the Council[7], Europol provides support to Member States' cross-border investigations into the money laundering activities of transnational criminal organisations. According to Regulation (EU) 2016/794, the Europol National Units are the liaison bodies between Europol and the Member States' authorities competent to investigate criminal offences. To provide Europol with the information necessary to carry out its tasks, Member States should provide that their Financial Intelligence Unit replies to requests for financial information and financial analysis made by Europol through the respective Europol National Unit. Member States should also provide that their Europol National Unit replies to requests for information on bank accounts by Europol. Requests made by Europol have to be duly justified. They have to be made on a case-by case basis, within the limits of Europol's responsibilities and for the performance of its tasks.

(21) This Directive should also be mindful of the fact that, in accordance with Article 43 of Regulation (EU) 2017/1939[8], the European Delegated Prosecutors of the European Public Prosecution Office (EPPO) are empowered to obtain any relevant information stored in national criminal investigation and law enforcement databases, as well as other relevant registries of public authorities, including centralised bank account registries and data retrieval systems under the same conditions as those that apply under national law in similar cases.

(22) To achieve the appropriate balance between efficiency and a high level of data protection, Member States should be required to ensure that the processing of sensitive financial information that could reveal a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation should be allowed only to the extent that it is strictly necessary and relevant to a specific investigation.

(23) This Directive respects the fundamental rights and observes the principles recognised by Article 6 of the Treaty on European Union and by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private and family life (Article 7) and the right to the protection of personal data (Article 8), by international law and international agreements to which the Union or all the Member States are party, including the European Convention for the Protection of

[7] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53.

[8] Council Regulation (EU) 2017/1939 of 12 October 2017, implementing enhanced cooperation on the establishment of the European Public Prosecution Office ("the EPPO"), OJ L 283 of 31.10.2017, p. 1.

Human Rights and Fundamental Freedoms, and in Member States' constitutions in their respective fields of application.

(24) It is essential to ensure that processing of personal data under this Directive fully respects the right to protection of personal data. Any such processing is subject to Directive (EU) 2016/680 of the European Parliament and of the Council and to Regulation (EU) 2016/679 of the European Parliament and of the Council[9], in their respective scope of application. As far as the access of Asset Recovery Offices to centralised bank account registries and data retrieval systems is concerned, Directive (EU) 2016/680 applies while Article 5(2) of Council Decision 2007/845/JHA should not apply. As far as Europol is concerned, Regulation (EU) 2016/794 applies. Specific and additional safeguards and conditions for ensuring the protection of personal data should be laid down in this Directive in respect of mechanisms to ensure the processing of sensitive data and records of information requests.

(25) Personal data obtained under this Directive should only be processed by competent authorities where it is necessary and proportionate for the purposes of prevention, detection, investigation or prosecution of serious crime.

(26) Furthermore, in order to respect the right to the protection of personal data and the right to privacy and limit the impact of the access to the information contained in centralised bank account registries and data retrieval systems, it is essential to provide for conditions limiting the access. In particular, Member States should ensure that appropriate data protection policies and measures apply to the access to personal data from competent authorities for the purposes of this Directive. Only authorised persons should have access to information containing personal data which can be obtained from the centralised bank account registries or through authentication processes.

(27) The transfer of financial data to third countries and international partners, for the purposes laid down in this Directive should only be allowed under the conditions laid down in Chapter V of Directive (EU) 2016/680 or Chapter V of Regulation (EU) 2016/679.

(28) The Commission should report on the implementation of this Directive three years after its date of transposition, and every three years thereafter. In accordance with paragraphs 22 and 23 of the Interinstitutional Agreement on Better Law-Making[10] the Commission should also carry out an evaluation of this Directive on the basis of information collected through specific monitoring arrangements in order to assess the actual effects of the Directive and the need for any further action.

(29) This Directive aims at ensuring that rules are adopted to provide Union citizens with a higher level of security by preventing and combating crime, pursuant to Article 67 of the Treaty on the Functioning of the European Union. Due to their transnational nature, the terrorist and criminal threats affect the Union as a whole and require a Union wide response. Criminals may exploit, and will benefit from, the lack of an efficient use of bank account information and financial information in a Member State, which can have consequences in another Member State. Since the objective of this Directive cannot be sufficiently achieved by the Member States, but can rather be

[9] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[10] Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016; OJ L 123, 12.5.2016, p. 1–14.

better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve this objective.

(30) Council Decision 2000/642/JHA should be repealed since its subject matter is regulated by other Union acts and is not needed anymore.

(31) [In accordance with Article 3 of Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on the European Union and to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland have notified their wish to take part in the adoption and application of this Directive.]

(32) [In accordance with Articles 1 and 2 of Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, the United Kingdom and Ireland are not taking part in the adoption and application of this Directive and are not bound by it or subject to its application.]

(33) In accordance with Articles 1 and 2 of Protocol (No 22) on the position of Denmark annexed to the Treaty on the European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application.

(34) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001[11] of the European Parliament and of the Council [and delivered an opinion on …[12]],

HAVE ADOPTED THIS DIRECTIVE:

Chapter I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Directive lays down measures to facilitate access by competent authorities to financial information and bank account information for the prevention, detection, investigation or prosecution of serious criminal offences. It also provides for measures to facilitate access by Financial Intelligence Units to law enforcement information and to facilitate the cooperation between Financial Intelligence Units.

2. This Directive is without prejudice to:

   (a) the provisions of Directive (EU) 2015/849 of the European Parliament and of the Council and the related provisions in the national law of Member States,

[11] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies on the free movement of such data, OJ L 8, 12.1.2001, p. 1.

[12] OJ C …

including the organisational status conferred to Financial Intelligence Units under national law;

(b) the powers of competent authorities to exchange information between them or to obtain information from obliged entities under Union law or the national law of Member States.

Article 2

Definitions

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

(a) 'centralised bank account registries' means the centralised automated mechanisms, such as central registries or central electronic data retrieval systems, set up in accordance with Article 32a(1) of Directive (EU) 2015/849;

(b) 'Asset Recovery Offices' means the national offices designated by the Member States pursuant to Article 8(1) of Council Decision 2007/845/JHA for the purposes of the facilitation of the tracing and identification of proceeds of crime and other crime related property in view of its possible freezing, seizure or confiscation based on an order issued by a competent judicial authority;

(c) 'Financial Intelligence Unit' means the body established in each Member State for the purposes of Article 32 of Directive (EU) 2015/849;

(d) 'obliged entities' means the entities set out in Article 2 of Directive (EU) 2015/849;

(e) 'financial information' means any type of information or data which is held by Financial Intelligence Units to prevent, detect and effectively combat money laundering and terrorist financing, or any type of information or data which is held by public authorities or by obliged entities for those purposes and which is available to Financial Intelligence Units without the taking of coercive measures under national law;

(f) 'law enforcement information' means any type of information or data which is held by competent authorities to prevent, detect, investigate or prosecute criminal offences or any type of information or data which is held by public authorities or by private entities for those purposes and which is available to competent authorities without the taking of coercive measures under national law;

(g) 'bank account information' means the following information contained in the centralised bank account registries:

(a) for the customer-account holder and any person purporting to act on behalf of the customer: the name, complemented by either the other identification data required under the national provisions transposing Article 13(1)(a) of Directive (EU) 2015/849 on identifying the customer and verifying the customer's identity, or a unique identification number;

(b) for the beneficial owner of the customer-account holder: the name, complemented by either the other identification data required under the national provisions transposing Article 13(1)(b) of Directive (EU) 2015/849 on identifying the beneficial owner and verifying the beneficial owner's identity, or a unique identification number;

(c) for the bank or payment account: the IBAN number and the date of account opening and closing;

(d) for the safe deposit box: name of the lessee complemented by the other identification data required under the national provisions transposing Article 13 (1) of Directive (EU) 2015/849 on the identification of the customer and the beneficial owner and verification of his/her identity, or a unique identification number and the duration of the lease period.

(h) 'money laundering' means the conduct defined in Article 3 of Directive (EU) 2018/XX[13];

(i) 'associated predicate offences' means the offences set out in Article 2 of Directive (EU) 2018/XX;

(j) 'terrorist financing' means the conduct defined in Article 11 of Directive (EU) 2017/541[14];

(k) 'financial analysis' means the operational and strategic analysis carried out by the Financial Intelligence Units for the performance of their tasks pursuant to Directive (EU) 2015/849;

(l) 'serious criminal offences' means the forms of crime listed in Annex I to Regulation (EU) 2016/794 of the European Parliament and of the Council.

Article 3

Designation of competent authorities

1. Each Member State shall designate among its authorities competent for the prevention, detection, investigation or prosecution of criminal offences the competent authorities empowered to access and search the national centralised bank account registries set up by the Member States in accordance with Article 32a of Directive (EU) 2015/849. They shall include the Europol National Units and the Asset Recovery Offices.

2. Each Member State shall designate among its authorities competent for the prevention, detection, investigation or prosecution of criminal offences the competent authorities empowered to request and receive financial information or financial analysis from the Financial Intelligence Unit. They shall include the Europol National Units.

3. Each Member State shall notify the Commission its designated competent authorities in accordance with paragraphs (1) and (2) by [6 months from transposition date] at the latest, and shall notify the Commission of any amendment thereto. The Commission shall publish the notifications and any amendment thereto in the Official Journal of the European Union.

---

13 Directive 2018/XX/EU on countering money laundering by criminal law, OJ … .

14 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 of 31.3.2017, p. 6.

Chapter II

ACCESS BY COMPETENT AUTHORITIES TO BANK ACCOUNT INFORMATION

Article 4

Access and search by competent authorities to bank account information

1. Member States shall ensure that the competent authorities designated pursuant to Article 3(1) shall 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, including the identification, tracing and freezing of the assets related to such investigation.

2. The additional information that Member States may deem essential and include in the centralised bank account registries in accordance with Article 32a(4) of Directive 2018/XX/EU shall not be accessible and searchable by competent authorities according to this Directive.

Article 5

Conditions for the access and search by competent authorities

1. The access and search of bank account information in accordance with Article 4 shall be performed only by the persons within each competent authority that have been specifically designated and authorised to perform these tasks and on a case-by-case basis.

2. Member States shall ensure that the access and search by competent authorities is supported by technical and organisational measures ensuring the security of the data.

Article 6

Monitoring the access and search by competent authorities

1. Member States shall ensure that the authorities operating the centralised bank account registries keep a log of any access by competent authorities to bank account information. The logs shall include, in particular, the following elements:

   (a) the national file reference;

   (b) the date and time of the query or search;

   (c) the type of data used to launch the query or search;

   (d) the results of the query or search;

   (e) the name of the authority consulting the registry;

   (f) the identifiers of the official who carried out the query or search and of the official who ordered the query or search.

2. The logs shall be regularly checked by the data protection officers of the centralised bank account registries and by the competent supervisory authority established in accordance with Article 41 of Directive (EU) 2016/680.

3. The logs referred to in paragraph 1 shall be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security. They shall be protected by appropriate measures against unauthorised access and shall be erased five years after their creation, unless they are required for monitoring procedures that are already ongoing.

Chapter III

EXCHANGE OF DATA BETWEEN COMPETENT AUTHORITIES AND FINANCIAL INTELLIGENCE UNITS, AND BETWEEN FINANCIAL INTELLIGENCE UNITS

Article 7

Requests for information by competent authorities to the Financial Intelligence Unit

1. Subject to national procedural safeguards, each Member State shall ensure that its national Financial Intelligence Unit is required to reply to requests for financial information or financial analysis by its designated competent authorities referred to in Article 3(2), where that financial information or financial analysis is necessary, on a case-by-case basis, for the prevention, detection, investigation or prosecution of serious criminal offences.

2. The financial information and financial analysis received from the Financial Intelligence Unit may be processed by the competent authorities of the Member States for the specific purposes of preventing, detecting, investigating or prosecuting serious criminal offences other than the purposes for which personal data are collected in accordance with Article 4(2) of Directive (EU) 2016/680.

Article 8

Requests of information by a Financial Intelligence Unit to competent authorities

Subject to national procedural safeguards, each Member State shall ensure that its designated national competent authorities are required to reply to requests for law enforcement information by the national Financial Intelligence Unit, on a case-by-case basis, where the information is necessary for the prevention and combating of money laundering, associate predicate offences and terrorist financing.

Article 9

Exchange of information between Financial Intelligence Units of different Member States

1. Each Member State shall ensure that its Financial Intelligence Unit is enabled to exchange financial information or financial analysis with any Financial Intelligence Unit in the Union where that financial information or financial analysis is necessary

for the prevention and combating of money laundering, associate predicate offences and terrorist financing.

2. Member States shall ensure that where a Financial Intelligence Unit is requested pursuant to paragraph 1 to exchange financial information or financial analysis, it shall do so as soon as possible and in any case no later than three days after the receipt of the request. In exceptional, duly justified cases, this time limit may be extended by a maximum of 10 days.

3. Member States shall ensure that, in exceptional and urgent cases, and by way of derogation from paragraph 2, where a Financial Intelligence Unit is requested pursuant to paragraph 1 to exchange financial information or financial analysis already in its possession that relates to specific investigations concerning an act or conduct qualified as a serious criminal offence, a Financial Intelligence Unit shall provide that information or analysis no later than 24 hours after the receipt of the request.

4. Member States shall ensure that a request issued pursuant to this Article and its response shall be transmitted by using the dedicated secure electronic communications network FIU.net or its successor. That network shall ensure the secure communication and shall be capable of producing a written record under conditions that allow ascertaining authenticity. In the event of technical failure of the FIU.net, the financial information or financial analysis shall be transmitted by any other appropriate means ensuring a high level of data security.

Chapter IV

EUROPOL

Article 10

Access by Europol to bank account information and exchange of information between Europol and Financial Intelligence Units

1. Each Member State shall ensure that its Europol National Unit replies to duly justified requests related to bank account information made by the Agency for Law Enforcement Cooperation established by Regulation (EU) 2016/794 of the European Parliament and of the Council (‘Europol') on a case-by-case basis within the limits of its responsibilities and for the performance of its tasks.

2. Each Member State shall ensure that its Financial Intelligence Unit replies to duly justified requests related to financial information and financial analysis made by Europol through the Europol National Unit within the limits of its responsibilities and for the performance of its tasks.

3. Exchange of information under paragraphs 1 and 2 shall take place electronically through SIENA and in accordance with Regulation (EU) 2016/794. The language used for the request and the exchange of information shall be that applicable to SIENA.

Article 11

Data protection requirements

1. The processing of personal data related to bank account information, financial information and financial analysis referred to in Article 10(1) and (2) shall be performed only by the persons within Europol who have been specifically designated and authorised to perform those tasks.

2. Europol shall inform the data protection officer appointed in accordance with Article 41 of Regulation (EU) 2016/794 of each exchange of information pursuant to Article 10 of this Directive.

Chapter V

ADDITIONAL PROVISIONS RELATED TO THE PROCESSING OF PERSONAL DATA

Article 12

Scope

This Chapter shall only apply to designated competent authorities and Financial Intelligence Units in the exchange of information pursuant to Chapter III and in respect of exchanges of financial information and financial analysis involving the Europol National Units pursuant to Chapter IV.

Article 13

Processing of sensitive data

1. The processing of information revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation may only be allowed to the extent that it is strictly necessary and relevant in a specific case

2. Only persons specifically authorised may access and process the data referred to in paragraph 1 under the instruction of the data protection officer

Article 14

Records of information requests

Member States shall ensure that the requesting and the responding authorities maintain records relating to requests for information pursuant to this Directive. Those records shall contain at least the following information:

(a) the name and contact details of the organisation and personnel member requesting the information;

(b) the reference to the national case in relation to which the information is requested;

(c) the requests made pursuant to this Directive and their executing measures.

The records shall be kept for a period of five years, and shall be used solely for the purpose of verification of the lawfulness of the processing of personal data. The authorities concerned shall make all records available, upon request, to the national supervisory authority.

Article 15

Restrictions to data subjects rights

Member States shall adopt legislative measures restricting, in whole or in part, the data subject's right of access to personal data relating to him or her processed under this Directive in order to:

(a) enable the Financial Intelligence Unit or the competent national authority to fulfil its tasks properly for the purposes of this Directive;

(b) avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of this Directive and to ensure that the prevention, investigation and detection of money laundering, terrorist financing or other serious criminal offences is not jeopardised.

Chapter VI

FINAL PROVISIONS

Article 16

Monitoring

1. Member States shall review the effectiveness of their systems to combat serious criminal offences by maintaining comprehensive statistics.

2. By [6 months after the entry into force] at the latest, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Directive.

   The monitoring programme shall set out the means by which and the intervals at which the data and other necessary evidence will be collected. It shall specify the action to be taken by the Commission and by the Member States in collecting and analysing the data and other evidence.

   Member States shall provide the Commission with the data and other evidence necessary for the monitoring.

3. In any event, the statistics referred to in paragraph 1 shall include the following information:

   (a) the number of searches carried out by designated competent authorities in accordance with Article 4;

   (b) data measuring the volume of requests issued by each authority covered by this Directive, the follow-up given to those requests, the number of cases investigated, the number of persons prosecuted, the number of persons convicted for serious criminal offences, where such information is available;

   (c) data measuring the time it takes an authority to respond to a request after the receipt of the request;

(d) if available, data measuring the cost of human or IT resources that are dedicated to domestic and cross border requests falling under this Directive.

4. Member States shall organise the production and gathering of the statistics and shall transmit the statistics referred to in paragraph 3 to the Commission on an annual basis.

Article 17

Relationship to other instruments

1. Member States may continue to apply bilateral or multilateral agreements or arrangements between themselves on the exchange of information between competent authorities that are in force on the date of entry into force of this Directive, in so far as such agreements or arrangements are compatible with this Directive.

2. This Directive is without prejudice to any obligations and commitments of Member States or of the Union by virtue of bilateral or multilateral agreements with third countries.

Article 18

Evaluation

1. By [OJ please insert date: three years after the date of transposition of this Directive] at the latest, and every three years thereafter, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and to the Council. The report shall be made public.

2. No sooner than six years after the date of transposition of this Directive, the Commission shall carry out an evaluation of this Directive and present a report on the main findings to the European Parliament and the Council. The evaluation shall be conducted according to the Commission's better regulation Guidelines. The report shall also include an evaluation of how fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union have been respected.

3. For the purposes of paragraphs 1 and 2, Member States shall provide the Commission with necessary information for the preparation of the reports. The Commission shall take into account the statistics submitted by Member States under Article 16 and may request additional information from Member States and supervisory authorities.

Article 19

Transposition

1. Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive by XXYY [26 months after the date of entry into force of Directive (EU) (…)/2018: OJ please insert number of Directive amending Directive (EU) 2015/849] at the latest. They shall forthwith communicate to the Commission the text of those provisions.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 20

Repeal of Decision 2000/642/JHA

Decision 2000/642/JHA is repealed with effect from [*the date of transposition of this Directive*].

Article 21

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 22

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Strasbourg,

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