BRIEFING

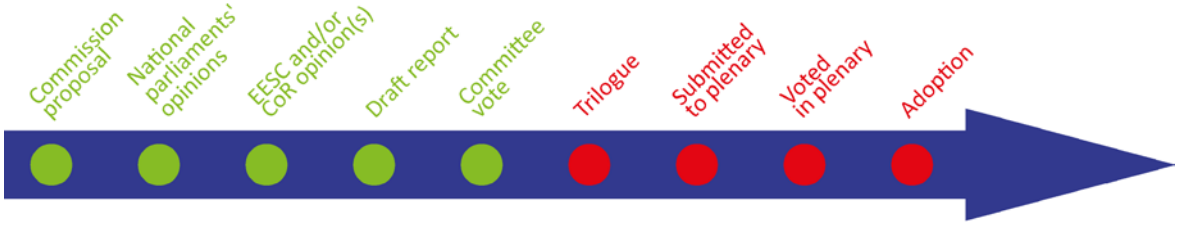
EU Legislation in Progress

Use of financial data for preventing and combatting serious crime

OVERVIEW

On 17 April 2018, the European Commission adopted a proposal for a directive intended to facilitate law enforcement authorities' access to and use of financial information held in other jurisdictions within the EU for investigations related to terrorism and other serious crime. In this sense, the proposed directive would grant competent authorities direct access to bank account information contained in centralised registries set up in each Member State, according to the provisions of the Fifth Anti-Money-Laundering Directive. The proposal also aims to strengthen domestic and cross-border exchange of information between EU Member States' competent authorities, including law enforcement authorities and financial intelligence units, as well as with Europol. Following the Council's adoption of its negotiating position in November 2018, on 3 December 2018, the European Parliament's Committee on Civil Liberties adopted its report and mandate in view of interinstitutional negotiations. This mandate was confirmed in plenary in December 2018.

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		
Committee responsible:	Civil Liberties, Justice and Home Affairs (LIBE)	COM(2018) 213 final 17.4.2018
Rapporteur:	Emil Radev (EPP, Bulgaria) Caterina Chinnici (S&D, Italy)	2018/0105(COD)
Shadow rapporteurs:	Helga Stevens (ECR, Belgium) Morten Helveg Petersen (ALDE, Denmark) Kostas Chrysogonos (GUE/NGL, Greece) Eva Joly (Greens/EFA, France) Ignazio Corrao (EFDD, Italy)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Trilogue negotiations	



EPRS | European Parliamentary Research Service

Author: Carmen-Cristina Cîrlig
Members' Research Service

PE 633.144 – January 2019

EN

Introduction

According to a 2017 Eurobarometer poll, a majority of Europeans consider terrorism (95 % of respondents) and organised crime (93 %) as important challenges to the EU's internal security. Furthermore, 92 % of the respondents agreed that national authorities should share information with the authorities of the other EU Member States to fight crime and terrorism more effectively. Against the background of new and complex security threats, the EU has emphasised the need for a more effective and coordinated response at EU level to support the fight against terrorism and organised crime, two core priorities of the 2015 European Agenda on Security. One important aspect linking the two priorities is the law enforcement authorities' (LEAs) focus on the finances of criminals and terrorists: tracking and analysing financial data and transactions can at the same time help address 'infiltration of the licit economy by organised crime' and serve to identify terrorist networks. In the February 2016 action plan on strengthening the fight against terrorist financing, the European Commission announced its intention to analyse the need for additional measures to facilitate LEAs' access to and use of financial information held in other jurisdictions within the EU for investigations related to terrorism and other serious crime, including to explore the possibility to broaden their access to national centralised bank account registries. Initiatives to improve cooperation between the EU Member States' financial intelligence units (FIUs) as well as with LEAs would also be considered. As part of the security union package presented on 17 April 2018, the Commission put forward a proposal for a directive to facilitate LEAs' access to and use of financial data.

Context

Financial information represents a valuable instrument for law enforcement authorities in the fight against crime and terrorism. As a basis for financial investigations, in particular in the area of money laundering and terrorist financing, financial data facilitates the identification of criminals and terrorists, the tracing of proceeds of crime in view of their freezing or confiscation and may serve as evidence in criminal proceedings. Financial data includes bank or financial accounts, records of transactions, as well as information collected through customer due diligence. It also covers mandatory 'suspicious transactions' reports (STRs) made by financial institutions and other companies (auditors, tax authorities etc.) on suspicious financial flows. Most financial information is held by private parties (e.g. banks, other financial institutions), but may be made available to law enforcement and other authorities under certain conditions, which vary across the EU.

Centralised bank account registries or data retrieval systems have facilitated the use of financial information by designated national authorities. However, centralised registries are not operational in all EU Member States and competent authorities have direct access in only a few of them. The practice of 'blanket' requests[1] sent to all financial institutions is therefore still widely used, leading to significant delays in obtaining the necessary data, missed opportunities in detecting, investigating and prosecuting crime, and negative consequences for cross-border cooperation.

Existing situation

Several EU legislative instruments contain provisions on access to financial information by law enforcement and other competent authorities and the cross-border exchange of such information.

Anti-money-laundering and terrorist financing (AML/CFT)

The EU participates in developing Financial Action Task Force (FATF) international standards, which are a basis for the implementation of legislation and other measures to combat money laundering and terrorist financing in its member countries. Successive anti-money-laundering directives (AMLD) have incorporated the FATF recommendations in EU law; they also provide the legal framework for a series of measures related to use and exchange of financial information by LEAs, FIUs and other competent authorities for money laundering or terrorist financing investigations.

The Third AMLD (repealed) introduced the obligation for EU Member States to set up national FIUs 'in order effectively to combat money laundering and terrorist financing' and redefined their role compared to previous instruments (such as Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between the Member States' financial intelligence units in respect of exchanging information). The FIUs were established as central national units, responsible for receiving (or requesting), analysing and disseminating to the competent authorities, information related to potential money laundering or terrorist financing.

The Fourth AMLD and the amending Fifth AMLD (both in force)[2] reinforced the powers of the FIUs. The Fourth AMLD sets out the role and competences of the FIUs, provides for the cooperation and exchange of information between EU FIUs and sets rules on the dissemination of information obtained from another FIU to domestic competent authorities. Among other things, the Fifth AMLD aimed to solve some problems related to the FIUs' powers: the FIUs' and other competent authorities' lack of (or delayed) access to information on the identity of bank and payment accounts' holders that hampered the detection of suspicious transactions, as well as the fragmentation of national data allowing the identification of bank/payment accounts belonging to one person.

Role and functions of EU FIUs

FIU's are central national units established in each EU Member State to prevent, detect and effectively combat money laundering and terrorist financing, and are responsible for receiving and analysing STRs and other information relevant to money laundering, associated predicate offences or terrorist financing. They are operationally independent and autonomous bodies. Member States must ensure FIUs have access, directly or indirectly, to the financial, administrative and law enforcement information needed for their tasks. FIUs may also respond to requests for information by law enforcement or other competent authorities in their Member State if these requests relate to money laundering, associated predicate offences or terrorist financing; however, the decision to analyse or disseminate information belongs to the FIU. There are no circumstances under which the FIU is obliged to comply with the request should that disclosure impact negatively on ongoing investigations or analyses or where, in exceptional circumstances, it may be disproportionate to the legitimate interests of natural or legal persons or irrelevant to the purpose of the request. FIUs also have the power to take urgent action, directly or indirectly, to suspend or withhold consent to a suspicious transaction, including at the request of another Member State's FIU. The FIUs may perform operational analyses (regarding individual cases) and strategic analyses (on trends and patterns in money laundering and terrorist financing).

Despite their common purpose and function, EU FIUs are quite varied. Broadly, they can be placed into three main categories: administrative, law enforcement (or judicial) and 'hybrid' (a combination of the two previous categories); even within each category, FIUs have been set up under various arrangements. The different nature and status of FIUs has had a significant impact on their functions and powers, as well as on domestic and international activities, including on FIU-to-FIU cooperation, as found by a 2016 report.

The Fifth AMLD introduced an obligation for all EU Member States to set up central registries or electronic data retrieval systems, enabling swift identification of bank and payment account and safe deposit box holders, and providing their FIUs and other AML/CFT competent authorities with full and immediate access to the financial information contained therein (see below).[3]

Central bank account registries or electronic data retrieval systems

Designated competent authorities will be able to use a centralised automated search query to identify all bank and payment accounts belonging to one person, leading to a faster detection of suspicious transactions. The Fifth AMLD instructs Member States to introduce a harmonised set of minimum information in the mechanism, consisting of: the name and other identification data required under the national provisions/ or a unique identification number for the customer-account holder, or the beneficial owner of the customer account holder, or the lessee of the safe deposit box; the IBAN number, and the date of opening and closing of the bank or payment account. Member States may include other information they deem necessary for preventing money laundering and terrorist financing. They will define the legal and technical requirements for access to such information, including rules for the protection of privacy and personal data.

The fifth AMLD also requires Member States to ensure their national FIU is able to provide information held in the centralised mechanism to any other EU FIU in a timely manner, and

establishes that an FIU should grant its prior consent to another FIU to forward the necessary information to competent authorities, regardless of the type of possible associated predicate offence (consent may be refused in certain circumstances). Member States must transpose the Fifth AMLD by 10 January 2020. The centralised registries must be set up by 10 September 2020.

Cross-border police cooperation and mutual legal assistance

Council Framework Decision 2006/960/JHA sets common rules aiming to simplify the procedures for LEAs to obtain information and intelligence concerning serious crime and terrorist acts (i.e. the 32 offences referred to in Article 2(2) of the 2002 European Arrest Warrant framework decision) from other EU Member States. Accordingly, Member States can exchange bank account information through police cooperation channels within eight hours for urgent requests, within one week for non-urgent requests related to the 32 offences, and up to two weeks in other cases.

When needed as evidence in criminal proceedings, financial data may also be requested through mutual legal assistance. Since May 2017, in this context, the European Investigation Order (EIO) also offers new possibilities for swifter access to the data, as it simplifies procedures for judicial authorities seeking to obtain evidence located in another EU Member State. An EIO may be issued to obtain details of bank and other financial accounts, as well as of banking and other financial operations executed during a defined period, of suspected or accused persons (or of any other person considered necessary by competent authorities in the course of criminal proceedings).

Criminal asset freezing and confiscation

Under a 2007 Council Decision, the asset recovery offices (AROs) established in all EU Member States are required to exchange information, including financial information, to trace and identify proceeds of crime that may become the object of a freezing or confiscation order.

Parliament's starting position

Parliament has repeatedly called for more effective exchange of information and closer coordination in the area of money laundering and terrorist financing between EU Member States' authorities, while ensuring the protection of personal data and privacy.

In its resolution on anti-terrorism measures from February 2015, Parliament strongly encouraged 'better exchange of information between Member States' law enforcement authorities and EU agencies'. Parliament also underlined the 'need for national law enforcement authorities and EU agencies to combat the main sources of revenue for terrorist organisations, including money laundering, human trafficking, and the illicit arms trade.'

In another resolution on the prevention of radicalisation and recruitment of European citizens by terrorist organisations (25 November 2015), Parliament also called for 'better cooperation between the Member States' FIUs and for the speedy transposition of the AML package'.

In its 6 July 2016 resolution on the strategic priorities for the Commission work programme 2017, the European Parliament called on the Commission, 'with a view to addressing the threats of terrorism and violent extremism, to monitor closely the transposition and implementation of EU counter-terrorism measures, including effective police and judicial cooperation, timely sharing of information among national authorities and through Europol and Eurojust, and measures to tackle emerging trends of terrorism financing.'

In December 2017, Parliament, the Council and the Commission agreed the Joint Declaration on the priorities of the EU's legislative agenda for 2018-2019. The first priority area (better protecting the security of our citizens) includes the Commission's commitment to present initiatives to facilitate cross-border access to and use of financial data by LEAs. The same month, following the inquiry on money laundering, tax avoidance and tax evasion, Parliament recommended that all Member States establish 'systems of bank account registries or electronic data retrieval systems which would

provide FIUs and the competent authorities with access to information on bank accounts'. The resolution further stressed 'the need for more effective communication between the relevant competent authorities at national level, but also between FIUs in different Member States' and the need to support the Member States' FIUs, particularly in cross-border cases.

On 1 March 2018, Parliament issued a recommendation on cutting the sources of income for jihadis – targeting the financing of terrorism, highlighting the need for 'comprehensive and preventive strategies based on the exchange of basic information and improved cooperation among FIUs, intelligence agencies and law enforcement agencies involved in combating the financing of terrorism'. In particular, Parliament welcomed the Commission's proposal to establish bank account registers and to facilitate access to them for FIUs and other competent authorities engaged in combating money laundering and the financing of terrorism. Parliament also noted the Commission's future proposal giving LEAs wider access to the registers. Parliament however underscored the need to observe the rules on police and judicial cooperation when exchanging bank account information, particularly in relation to criminal proceedings, and recalled that the protection of personal data and privacy were important fundamental rights in this context.

Council and European Council starting position

In December 2015, the European Council confirmed that the Council and the Commission were going to take swift further action against terrorist finance in all domains identified by the Council of 20 November 2015, which included stepping up law enforcement cooperation and information sharing in the area of counter-terrorism, as well as strengthening, harmonising and improving the powers of and the cooperation between FIUs, and ensuring 'their fast access to the necessary information in order to enhance the effectiveness and efficiency of the fight against money laundering and terrorist financing'. A year later, the European Council stated that special attention should be given to: improving information exchange and accessibility; strengthening operational cooperation and enhancing prevention and investigation of criminal acts, with a particular focus on organised financial crime and confiscation of criminal assets, and terrorist attacks. In June 2017, the European Council conclusions confirmed the 'resolve to cooperate at EU level', inter alia in order to 'thwart the financing of terrorism, facilitate swift and targeted exchanges of information between law enforcement authorities, including with trusted partners, and improve the interoperability between databases'. Finally, in May 2017, the Council identified the fight against criminal finances as one of the ten EU priorities of the EU policy cycle 2018-2021.

Preparation of the proposal

A series of reports and consultations with stakeholders fed into the European Commission proposal.

In December 2016, a joint mapping report carried out by the 28 EU FIUs emphasised the main obstacles to cooperation between FIUs, as well as between FIUs and competent authorities in EU Member States. For example, because some FIUs share their analysis with other authorities whose further use of that information is not regulated, other FIUs may refuse to share data with their counterparts to ensure control over it. The solutions identified were taken up by the Commission in a series of documents from June 2017. One report (with its accompanying staff working document), assessing the risks of money laundering and terrorist financing affecting the internal market and related to cross-border activities, found that cooperation between FIUs, despite having increased over the last decade, is still affected by weaknesses, turning it into a horizontal vulnerability common to all sectors identified in the report. Another staff working document reiterated that the rules on the cross-border dissemination of information to LEAs are not sufficiently clear, mostly due to Member States' diverse legal frameworks. Establishing minimum rules at EU level to provide for better information sharing and improved cooperation of FIUs with law enforcement and judicial authorities could therefore be considered. In September 2017, a Europol report concluded that significant barriers remain in the anti-money laundering and terrorist financing regime in relation to international cooperation and information exchange. In particular, 'the "symmetrical" exchange of

information between FIUs may prevent crucial information contained in STRs reaching authorities tasked with criminal investigations.'

The 11th progress report on the Security Union (October 2017) mentions the Commission has been 'consulting stakeholders and analysed the mechanisms through which competent authorities can currently access relevant information, particularly financial data stored in other Member States; the obstacles to doing so quickly and effectively; and possible measures to address these obstacles'. A public consultation on possible EU legislation on broadening law enforcement access to centralised bank account registries in order to disrupt the activities of organised crime groups and terrorists took place between 17 October 2017 and 9 January 2018. It was preceded by consultation on the Inception Impact Assessment (9 August-6 September 2017). In October 2017, the Commission announced in its work programme for 2018 that it would present initiatives to facilitate cross-border access to and use of financial data by LEAs in the second quarter of 2018. The 12th progress report on the Security Union (December 2017) mentions that the Commission was continuing work on initiatives to improve cooperation between FIUs as well as their cooperation with LEAs, to be finalised in spring 2018. Parallel efforts were aimed at 'assessing the necessity, technical feasibility and proportionality of any additional measures' to facilitate cross-border access to financial data by law enforcement authorities.

Stakeholder consultations carried out by the Commission include: a survey of the Member States' asset recovery offices and anti-corruption authorities (June 2016); an expert meeting on broadening law enforcement access to centralised bank account registries (October 2017); a high-level stakeholder meeting bringing together Member States and EU bodies to address the main obstacles to access financial transaction data held in other Member States for counter-terrorism investigations (November 2017); a consultation with the AROs during the EU AROs' platform meeting in December 2017; and a meeting to discuss cooperation between FIUs and LEAs (March 2018). The European Data Protection Supervisor (EDPS) and national data protection authorities, as well as banking associations provided input to the preparation of the proposal.

On 17 April 2018, the Commission presented a security package including the legislative proposal to improve cross-border access to financial information for investigations and prosecution for serious crimes, and to strengthen cooperation between FIUs and LEAs. The Commission's impact assessment accompanying the proposal for a directive identifies two main problems that affect domestic and cross-border financial investigations negatively:

- Lack of (or delayed) law enforcement authority access to financial information

The Commission argues that LEAs should be given access to the financial information in the centralised bank account registries and data retrieval systems set up under the Fourth and Fifth AMLD, for the wider purpose of fighting serious crime, rather than being limited to money laundering and terrorist financing. Such registries and systems have been set up in 16 Member States, but the rules granting access to competent authorities, including LEAs, vary from country to country. The Commission argues that direct access for LEAs would render redundant the practice of blanket requests, source of significant delays in investigations, of administrative burden on both the law enforcement and the banking sector, and of problems for personal data protection.

In most cases, LEAs cannot access the raw data or the full set of information held by FIUs or the financial entities, but may receive only the results of FIU analyses or the STRs received from banks. Also, FIUs have interpreted the obligation to respond to requests from LEAs restrictively, to cover only data already in FIUs' possession and not data they have the right to obtain. Moreover, requests to FIUs are limited to money laundering and terrorist financing purposes. Legal obstacles may also impede information exchange between administrative FIUs and law enforcement.

Finally, mechanisms for cross-border cooperation are insufficiently effective and efficient. When requests cannot be channelled through FIUs, LEAs must rely on rather lengthy mutual legal assistance procedures or on the EIO, if the requested FIU is administrative. Cross-border requests are not regulated by any specific instrument.

- Obstacles to FIU-to-FIU cooperation and to FIU access to information from LEAs

These stem from differences across Member States regarding the national FIU's possibilities for cooperation with other FIUs or with their national LEAs and access to information held by the latter. The problem is even more acute when an FIU (in particular an administrative one) needs information held by a LEA in another Member State. The implications are the same as described as above.

For each problem, the Commission analysed a number of policy options. Non-regulatory solutions (e.g. best practices at EU level) were discarded, as the problems are of a regulatory nature. The legislative possibilities envisaged were split into blocks of options for each issue identified: the types of crimes to be covered (option A); the modalities of access to the data (option B) and the categories of authorities to benefit from access to and exchanges of information (option C). To all the legislative options, the EU General Data Protection Regulation (GDPR) and the Data Protection Police Directive safeguards should apply. The preferred option retained was a directive which will give direct access to centralised bank account registries and data retrieval systems to competent authorities for the purpose of criminal investigations on all forms of serious crimes referred to in Article 3(1) of the Europol Regulation. Member States will designate the competent authorities with direct access; Europol will get indirect access through the Europol National Units. Obligations for the timely exchange of information between FIUs and with LEAs are introduced.

In June 2018, an EPRS initial appraisal of the Commission's impact assessment underlined the comprehensive analysis carried out by the Commission of the obstacles encountered by law enforcement and FIUs in accessing and exchanging financial data, and the real efforts to analyse the impacts of a new measure addressing those problems. However, the initial appraisal concluded that the Commission failed to perform a thorough analysis of the fundamental rights safeguards, in particular in view of the proposed extension of the scope to serious criminal offences.

The changes the proposal would bring

The Commission's proposal (17 April 2018) for a directive covers measures to facilitate the use of financial and other information in order to prevent and investigate serious crime more effectively across borders. It addresses two main aspects: giving direct and timely access to the competent authorities to the national centralised bank account registries or data retrieval systems; and improving cooperation between EU FIUs and between FIUs and law enforcement authorities. The proposal also aims to address the fundamental rights issues stemming from the increased interference with the right to privacy and protection of personal data. If adopted, the directive will repeal Council Decision 2000/642/JHA on arrangements for cooperation between FIUs.

The proposal is based on Article 87(2) of the Treaty on the Functioning of the European Union (TFEU) (measures for police cooperation between EU Member States' authorities), thus complementing the Fourth and Fifth AMLD (based on Article 114 TFEU: internal market) with the police cooperation aspects of the legal framework. The directive's implementation would be aligned with the Fifth AMLD: the Commission proposed a transposition deadline of 26 months after the entry into force of the Fifth AMLD (i.e. after 9 July 2018). Denmark is not taking part in the adoption of the directive, due to its Treaty opt-out, whereas the United Kingdom and Ireland opted in.

Six months after the proposed directive's entry into force, the Commission intends to establish a detailed programme for monitoring outputs, results and impact, based on data and comprehensive statistics received from the Member States. The Commission will also submit a report on the directive's implementation to the European Parliament and the Council, at the latest three years after its transposition and every three years after. Another evaluation report, including on the respect for fundamental rights as set out in the EU Charter, will be presented by the Commission six years from its transposition.

Authorities' access to centralised bank account registries

The proposed directive gives access to financial and bank account information contained in the centralised bank account registries to competent authorities for the purpose of preventing, detecting, investigating or prosecuting **serious criminal offences**, namely the offences listed in Annex I of the Europol Regulation or for supporting a criminal investigation, including the identification, tracing, freezing and confiscation of assets related to such investigations.

The **competent authorities** empowered to 'directly and immediately' access and search bank account information in these registries are to be designated by EU Member States, and include: LEAs; FIUs; tax authorities and anti-corruption authorities in their capacity to conduct criminal investigations under national law. AROs, in view of the possible freezing and confiscation of criminal assets, and the Europol national units must also figure among the designated authorities. **Europol** will get indirect access through the Europol national units, on a case-by case basis and within the limits of its responsibilities and for the performance of its tasks.

The proposal further defines the **conditions for access and search** of the centralised bank account registries by the designated competent authorities. Access and search may be performed only by specifically designated and authorised persons within each competent authority, on a case-by-case basis, under conditions ensuring the security of the data. **The bank account information** is defined according to the Fifth AMLD (the owner's or lessee's name, date of birth and bank account number, as explained above). Additional information included by Member States in the centralised registries under the Fifth AMLD will not be available for access and search under the proposal, nor will the bank accounts contents, balance, nor details of transactions.

Improving cooperation between FIUs and competent authorities

The proposal also aims to improve cooperation between FIUs and competent authorities, as well as between FIUs. As regards the FIUs, the provisions of the proposal 'should be without prejudice to the organisational status and role conferred to FIUs under the national law of Member States'. The proposed directive includes the obligation for:

- each FIU to reply to requests for financial information or financial analysis (both operational and strategic analysis) from a Member State's designated competent authorities, on a case-by-case basis (i.e. concerning a specific case under investigation), for the prevention, detection, investigation or prosecution of serious criminal offences;
- Member States' competent authorities to reply to requests for law enforcement information issued by an FIU, on a case-by-case basis and for the purpose of preventing and combatting money laundering, associate predicate offences and terrorist financing;
- Member States to ensure that their FIU can exchange financial information or analysis with any other EU FIU (regarding money laundering and terrorist financing). The proposal institutes **time limits** for such exchange of information: no later than three days after receipt of the request, extendable to maximum 10 days in duly justified cases; in exceptional and urgent cases, where an FIU already has the financial information/ analysis requested, the deadline drops to up to 24 hours after receipt of the request;
- For each Member State to ensure that its FIU replies to duly justified requests for financial information or analysis made by Europol through the Europol National Unit.

Fundamental rights

The Commission recognises the proposal's impact on the **right to privacy**, particularly in terms of the number of people that would be affected by access to data in the registries. However, it argues that the impact is not severe, as the accessible/searchable data in the registries is restricted to the information necessary to identify the banks where the subject of an investigation holds accounts.

As regards **personal data protection**, the Commission underlines that Directive (EU) 2016/680 (the Data Protection Police Directive) applies. Moreover, the exchange of information will be limited to specific cases under investigation (case-by-case) for an exhaustive list of serious criminal offences, and to the designated competent authorities entitled to request information. The proposal also confirms the application of the safeguards established by the Europol regulation (when Europol gets indirect access and when it exchanges data with FIUs). Only persons within Europol specifically designated and authorised for those tasks may process personal data.

The proposed directive also institutes an obligation on the national authorities managing the centralised registries to maintain logs of access by competent authorities to bank account information. The logs will be checked regularly by national data protection authorities, for the purpose of data protection monitoring only. They must be erased five years after their creation, unless necessary for monitoring already ongoing procedures.

Other provisions refer to the processing of personal data by FIUs and designated authorities when exchanging information:

- processing of 'sensitive personal data' may be authorised only if it is strictly necessary and relevant in a specific case; access to and processing of such data is restricted to persons specifically authorised, under the instruction of the data protection officer;
- restrictions to the data subjects' rights of access to their personal data under national laws are allowed only for the purpose of enabling the FIUs and the competent authorities to perform their tasks under the directive, as well as in order to avoid obstruction or risk to inquiries or investigations related to serious crime;
- requesting and responding entities must maintain records for five years following information requests, to allow the lawfulness of the personal data processing to be checked.

Finally, under the proposal, the exchange of data will no longer require judicial authorisation. National **procedural rights and safeguards** therefore apply to the exchanges of information between the national FIU and the national competent authorities.

Advisory committees

The European Economic and Social Committee (EESC) adopted an opinion on the proposed directive on 12 July 2018. While welcoming the Commission's initiative, it recommended that the proposal should strike a better balance between the individuals' fundamental rights and the need for better law enforcement. In this sense, the EESC takes the view that access to financial data in the centralised registries should be granted only to authorities responsible for investigating and prosecuting criminal offences, as well as to AROs, on the basis of a well-founded case. Access to these registries 'for preventive purposes should be allowed only for terrorism offences and drug trafficking or trafficking in human beings, and for the purposes of detecting, investigating, prosecuting, sanctioning, and recovering damages, both for the above crimes and for all other offences, as defined in the proposal'. Other suggestions relate to including financial information relating to the investment accounts of capital market investment managers in the centralised bank account registries; to demarcate more specifically and restrictively the list of crimes covered by the proposed directive; and to define 'law enforcement information'.

National parliaments

The deadline for the submission of reasoned opinions on the grounds of subsidiarity expired on 13 July 2018, with none of the parliaments raising subsidiarity concerns. However, some parliaments raised issues regarding the substance of the proposal. For example, the Belgian House of Representatives emphasised a number of contradictions between the proposal and the Fourth AMLD and called for guarantees for the specificity and operational autonomy of the FIUs. The UK House of Commons also pointed to a potential conflict with the EU's Fourth AMLD, in particular

regarding the FIUs' autonomy in deciding whether to share information, and the three day limit for responding to requests which is 'shorter than existing standards for such exchanges'.

Stakeholders' views[4]

The public consultation on the proposal received 24 replies. Most respondents agreed that protecting citizens from crime requires granting access to national centralised bank account registries to LEAs, AROs, national anti-corruption authorities and the EU anti-fraud office (OLAF), while some disagreed with giving access to tax authorities. One authority managing such a register considered access should be exclusive to LEAs. The issues of strict safeguards and conditions of access, and processing personal data according to the principle of purpose limitation, were also raised.

The **EU FIUs** welcomed the proposal; however, they raised a number of concerns in a paper submitted to the Commission, stating that the EU FIUs position was not reflected in the text:

1. *On domestic cooperation between FIUs and LEAs*: while the increase of information flows between FIUs and competent authorities is welcomed, this cooperation must respect the FIUs' specificity and role.
   - FIU access to law enforcement information: while welcoming the provisions empowering FIUs to obtain information from national LEAs, FIUs underline the proposal does not define 'law enforcement information' by identifying the types of data that should be available to FIUs. Moreover, should national procedural safeguards apply to such access, this element of conditionality would entail significant restrictions and discrepancies across national approaches, impacting negatively FIU-to-FIU cooperation;
   - LEA access to financial information via the FIUs: requests for information should be restricted to information exclusively held by the FIUs; LEAs should be granted the power to directly access financial information from the relevant sources (e.g. financial or banking institutions) and not through the services of the FIU;
   - The obligation on FIUs to answer requests for financial information or analysis from LEAs (and Europol): FIUs see this as a twofold obligation – to provide available information, based on a new type of **mandatory** 'dissemination' and to conduct financial analysis based on specific instructions and report on the outcomes – which would run counter to FIU organisational and operational autonomy and independence and the forms of dissemination permitted (**spontaneous** or **on request**), would impact the FIUs' budget and priorities; and may hamper ongoing investigations and FIU-to-FIU cooperation.
2. *On Europol's access to FIU information*: as above, the FIUs consider that the twofold obligation of providing Europol with financial information coming from banks or from related analysis, as well as of performing financial analysis as requested by Europol on identified cases and report the results to Europol, would not be in line with EU law and international standards.
   - It would conflict with the FIUs operational autonomy and independence and with established rules that the dissemination of information cannot be mandatory.
   - Moreover, the risk would increase as regards hampering or disrupting ongoing investigations, but also as regards impeding cooperation activities between the FIUs.
   - The impact on FIU resources, workload and priorities is again mentioned, as well as the fact that there is a lack of clarity as regards what Europol can do with the financial information or analysis received, as well as concerning a lack of reciprocity, as the FIUs could not request information from Europol nor receive feedback on the use of the data.
3. *On FIU-to-FIU cooperation*: the provisions setting short deadlines to respond to foreign requests may conflict with the Article 53 of the Fourth AMLD, covering the issue in a broader manner.

- The proposal does not take account of the work done on categorising the different types of requests and exchanges (FIUs must analyse the nature of the request to determine the most appropriate treatment), and does not define what constitutes a relevant response to a foreign request;
- The diversity of information sources that FIUs have to access to respond to requests means that the timeframe to obtain the data may vary depending on the source;
- When information is obtained from an obliged entity (defined in Article 2 of the Fourth AMLD) or from another agency through domestic cooperation under the Fourth AMLD, the proposal fails to set deadlines within which the entity or agency is required to respond to the FIU.

The **European Data Protection Supervisor (EDPS)** issued formal comments on the proposal, on 10 September 2018. While acknowledging that some of its previous suggestions were taken into account in the proposal, such as the detailed programme to monitor the outputs, results and impacts of the proposal, other specific data protection issues remain and the EDPS suggests:

- Making explicit reference in the articles of the proposed directive (not only in the recital) to the applicability of EU data protection law (GDPR and the Police Data Protection Directive) and mentioning explicitly that data must be processed by designated authorities and FIUs only where it is necessary and proportionate for the purpose of the directive.
- Better defining some terms, such as 'designated competent authorities (e.g. by referencing Article 3(7) of the Data Protection Police Directive); also clarifying when 'tax authorities' could be designated as competent authorities under the proposal, as tax crimes are not covered by the serious crimes enumerated in Annex I of the Europol Regulation. Anti-corruption authorities should also be defined in the text.
- Keeping records of all access by any user and applying the data minimisation principle: the logs database should only include the 'unique identifiers of the results', not the results of the query or search.
- Ensuring that staff dealing with centralised registers and staff of the national designated competent authorities are trained on data protection and confidentiality standards.
- Aligning with the Data Protection Police Directive on processing of sensitive data to be 'subject to appropriate safeguards for the rights and freedoms of the data subject'.
- Aligning with the formulations in the GDPR and the Police Data Protection Directive as regards the rights of data subjects to be informed about access to their personal data contained in the centralised bank account registers or about exchanges of their personal data. Although some restrictions may be justified, the right of access, set out in Article 8(2) of the EU Charter, 'should not be completely denied by the proposal'.

Legislative process

In Parliament, the proposal for a directive has been assigned to the Civil Liberties, Justice and Home Affairs Committee (LIBE) and the rapporteur appointed is Emil Radev (EPP, Bulgaria).

The members of the LIBE committee held a first exchange of views with EU Commissioner Julian King on the legislative proposal on 11 June 2018. On 28 September 2018, the rapporteur issued a draft report, discussed in a LIBE committee meeting on 15 October 2018. The draft report welcomes the Commission's proposal, in particular the provisions on providing access to national bank account registers or data retrieval systems to competent authorities for fighting serious crime. While the draft recognises the need to strengthen the exchange of information between FIUs and competent authorities, this must not jeopardise the FIUs' operational independence and autonomy. The FIUs' different structures and forms across the EU should also be taken into account. Therefore, the draft report proposes that FIUs should respond to requests for information or analysis from the competent authorities or the Europol national units, unless this would have a negative impact on ongoing investigations or analysis, or the disclosure of the information would be disproportionate

to the legitimate interests of a natural or legal person, or irrelevant with regard to the purpose for which it has been requested. The draft report also extends slightly the deadlines for FIU-to-FIU exchange of information. On data protection, the draft text 'aligns the data protection regime with existing legislation and removes text that results in the creation of new regimes'. The European Parliament Committee on Economic and Monetary Affairs (ECON) issued an opinion.

Discussions within the Council began on 27 April 2018. In its 16th progress report on the Security Union, the Commission called on the Parliament and Council to agree, as a priority, their negotiating mandates and to enter into interinstitutional discussions, in order to adopt the directive by the end of the legislature. The Council agreed its negotiating position on 21 November 2018. Following the consideration of amendments on 20 November 2018, the LIBE committee adopted its report and a mandate for interinstitutional negotiations on 3 December 2018. The mandate was confirmed by the European Parliament during the December plenary session.

EP SUPPORTING ANALYSIS

Scherrer A., Law enforcement access to financial data, Implementation Appraisal, EPRS, European Parliament, April 2018.

Eisele K. with van Heijst A., Access to financial data by law enforcement authorities, Initial Appraisal of the Commission Impact Assessment, EPRS, European Parliament, June 2018.

OTHER SOURCES

Use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, Legislative Observatory (OEIL), European Parliament.

Report on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, COM(2017) 340 final, and the staff working document accompanying the report, SWD(2017) 241 final, 26 June 2017.

ENDNOTES

[1] When an investigator lacks access to a centralised registry and cannot thus contact the bank(s) concerned directly, a request to all banks – or 'blanket request' is sent. The investigator then needs to wait for all the banks to reply to his request in order to obtain complete information on the bank accounts owned/operated by the investigated person.

[2] Directive (EU) 2015/849 (the Fourth AMLD) entered into force in June 2015 and had a deadline for transposition in national legislation of 26 June 2017. Directive (EU) 2018/843 (the Fifth AMLD), in force since July 2018, must be transposed in Member State legislation by 10 January 2020.

[3] While this type of mechanism was already in place in a number of Member States, as also encouraged by the Fourth AMLD, it is the Fifth AMLD that introduced the obligation for all EU Member States to establish them.

[4] This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'EP supporting analysis'.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

First edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.