Law enforcement access to financial data

This briefing is one in a series of ‘implementation appraisals’, produced by the European Parliamentary Research Service (EPRS), on the operation of existing EU legislation in practice. Each briefing focuses on a specific EU law which is likely to be amended or reviewed, as foreseen in the European Commission’s annual work programme. Implementation appraisals aim at providing a succinct overview of publicly available material on the implementation, application and effectiveness to date of specific EU law, drawing on input from EU institutions and bodies, as well as external organisations. ‘Implementation appraisals’ are provided by the EPRS’ Ex-Post Evaluation Unit, to assist parliamentary committees in their consideration of new European Commission proposals, once tabled.

Summary
Access to financial data by law enforcement authorities is seen as critical for preventing crime. This briefing looks at the specific provisions contained in EU instruments that have facilitated this access, and examines the exchange of financial data at EU level but also with non-EU countries. It shows that such access has significantly broadened in the last decades. The private sector, which collects most of these data, has been increasingly regulated; as a result, the sources of information available to the competent authorities have multiplied. The exchange of these data at EU level has been furthermore considerably simplified. However, law enforcement authorities still see significant challenges to accessing and exchanging financial information. The Commission plans to address these challenges through a number of initiatives that it announced in its 2018 work programme. On the other hand, such broadened access does not occur without debates and controversies, in particular in relation to efficiency at the operational level, adequate scrutiny and fundamental rights compliance.

1. Background
‘Follow the money trail’ has become a widely used strategy in criminal investigations. Enquiries into financial affairs related to criminal conduct – commonly referred to as financial investigations – are recognised as particularly useful for identifying criminal networks, tracing the proceeds of crime subject to confiscation and developing evidence that can be used in criminal proceedings.¹ These enquiries have been specifically launched in relation to criminal assets-freezing and confiscation, money laundering and terrorist financing (ML/TF), and, more recently, tax crimes.²

Financial investigations require having access to financial data, including bank or financial accounts, or other records of personal or business financial transactions.³ These data come in a variety of forms: paper, electronic, etc. Ownership and control of the different data types also varies. Financial data are mostly held by private third parties, such as banks. Furthermore, following the risk-based approach adopted in the field of ML/TF at both EU and international level, financial data can also include reports compiled by regulated private entities (these include financial institutions, but also cover a wide range of professions).⁴ These

² For an overview of the evolution of financial investigation/intelligence, see: A. Scherrer, Fighting tax crimes: Cooperation between Financial Intelligence Units, EPRS Study, March 2017: see in particular section 2 (written by A. Amicelle), and section 1.1.
⁴ Regulated entities include, for instance, auditors, accountants, tax advisors, notaries, trust or company service providers and real estate agents.
The way in which such financial information can be provided to the competent authorities differs from one EU Member State to another.\(^6\) In principle, law enforcement authorities can obtain access to financial data through the authorisation of a judge or a prosecutor, or in some cases, directly, without prior authorisation.\(^7\) Direct access is often provided in the framework of investigations related to ML/TF. In some Member States, access has been made easier with the establishment of centralised registries, such as bank account registries. The national authorities that are allowed to access the information contained in these registries – whether directly or indirectly – can include a broad range of actors, such as police and prosecuting authorities, criminal asset recovery offices (AROs), tax/customs administrations and/or financial intelligence units (FIUs).\(^8\) In some Member States, special units dedicated to dealing with financial crimes can involve some or all of these actors. As a result, various actors have access to financial information, for various purposes, such as collecting evidence in the course of an investigation, fighting ML/TF or tax evasion, and/or gathering financial intelligence.

The fact that most financial data are held by private third parties, and that multiple authorities can access them, raises a number of questions. As financial data can be considered personal data, in the sense that they are related to an identified or identifiable individual,\(^9\) they are often regarded as highly sensitive and confidential. This explains why the modalities governing access to and processing of financial data at national and EU level include specific legal requirements used for ensuring that personal data are processed lawfully, are collected for specific, explicit and legitimate purposes, and are not excessive in relation to the purpose for which they are processed.\(^10\) In other words, these modalities should be compliant with the EU data protection regime and its core principles of necessity, proportionality and purpose limitation. These requirements are critical to enable cooperation between the Member States. Access to such data can interfere with the right to data protection, but also with other fundamental rights enshrined in the EU Charter of Fundamental Rights (EU Charter), such as the right to privacy, and to some extent the principle of the presumption of innocence. As the following sections show, these tensions between law enforcement and fundamental rights considerations have been at the heart of all debates related to data processing for law enforcement purposes.

2. Overview of the current legislative instruments

This section provides an overview of the legislative instruments that include provisions aimed at facilitating law enforcement authorities’ access to financial data and that are of direct relevance to the Commission’s future initiatives in this domain. While it is currently not known what the proposals related to these initiatives will entail in detail (see section 9),\(^11\) they will probably have an impact on several legislative instruments.

2.1. EU instruments that facilitate access to financial data in cross-border investigations

In criminal matters in general, mutual legal assistance (MLA) instruments are used for cross-border cooperation for the purpose of gathering and exchanging information. In force since May 2017, the European Investigative Order (EIO) Directive is the overarching EU tool for improving MLA at EU level and simplifying the work of judicial authorities wishing to obtain evidence located in another EU country. The EIO covers the whole process, from the collection of evidence to the transfer of existing evidence. This includes checks of

---

\(^5\) FATF guidance report on financial investigations, 2012, paragraph 55.

\(^6\) International Centre for Migration Policy Development (ICMPD), Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments, 2010; E. Thirion and A. Scherrer, Member States’ capacity to fight tax crimes, EPRS Study, July 2017.


\(^8\) E. Thirion and A. Scherrer, op.cit., p. 31 and seq.

\(^9\) See: ’What is personal data?’, European Commission website.

\(^10\) FATF guidance report, op.cit.

\(^11\) Proposals related to the Commission’s initiatives are schedules in the List of the ‘point prévus’ on the 17 of April.
the bank accounts and financial operations of suspected or accused persons. In addition, EU provisions facilitating the exchange of information in criminal matters include the 'Swedish Initiative' (Decision 2006/960/JHA), which provides a common legal framework for the effective and expeditious exchange of existing information and criminal intelligence between Member States' law enforcement authorities.12

2.2. EU instruments specifically related to money laundering and terrorist financing
As regards the specific areas of money-laundering and terrorist financing (ML/TF), the EU has developed several dedicated instruments, namely the successive anti-money laundering directives (AMLDs).13 In particular, the third AMLD placed the requirement on Member States to set up financial intelligence units (FIUs) for receiving and analysing a special type of reports, the 'suspicious transaction reports' (STRs). These reports are compiled by the regulated private sector entities (also called 'obliged entities'),14 which are most commonly banks and financial institutions, but also include other designated non-financial professions. The reports contain information about financial flows these entities have detected that could be related to ML/TF. The FIUs’ access to financial data and the conditions on which such data can be shared at EU level were further regulated in the fourth AMLD, which entered into force in June 2017. The amended Directive on administrative cooperation (the DAC Directive), adopted in 2016, also granted tax authorities access to anti-money-laundering information held by the competent authorities.

2.3. EU instruments facilitating the tracing and identification of proceeds of crime
The ARO Decision, adopted in 2007, provides a framework for the cooperation between EU asset recovery offices (AROs). On the basis of this instrument, each Member State has designated AROs in place to facilitate the tracing and identification of proceeds of crime that may become the object of a freezing, seizure or confiscation order made by a competent judicial authority in the course of criminal or civil proceedings. National AROs are obliged to exchange information (including financial data) with each other.

2.4. Agreements that facilitate data exchange with third countries
On the basis of Articles 24 and 38 of the Treaty on European Union (TEU), agreements between the EU and third countries provide for further MLA instruments with non-EU countries. At the time of writing, the EU had agreements of this type with Iceland and Norway, the US and Japan. While the agreement with Iceland and Norway does not specifically refer to the exchange of financial data (but refers broadly to the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union), the ones concluded with the US and Japan explicitly include the exchange of bank information. As regards the US, a second agreement – the EU-US TFTP Agreement – in force since 2010, has been facilitating the exchange of financial data for the purposes of the US Terrorist Finance Tracking Program (TFTP). The latter is a classified US government programme that was set up following the terrorist attacks of 11 September 2001 to identify and pursue terrorists and their networks by tracking related money flows. The programme provided access to the transactions database of SWIFT, the world’s leading provider of secure financial messaging services, based in Belgium. Press revelations about the TFTP led to heated debates related to privacy concerns, including at the level of the European Parliament (see section 10). In a landmark resolution from February 2010, the Parliament rejected the conclusion of an agreement allowing US authorities access to European financial transactions data. In May 2010, the Commission started negotiating a new agreement with the aim of ensuring better data protection safeguards. In July 2010, Parliament gave its approval to the conclusion of a revised agreement.15 In its revised form, the agreement gives Europol the responsibility for

---

12 In particular, it lays down time limits for replying to requests for exchange of information: eight hours for urgent requests and in cases where the requested information or intelligence is held in a database that is directly accessible by a law enforcement authority; one week for non-urgent requests for information and intelligence regarding serious offences, in cases where the requested information or intelligence is held in a database that is directly accessible by a law enforcement authority; two weeks in all other cases (database not directly accessible and/or request not related to a serious crime). The initiative was proposed by Sweden.


14 Obliged entities are, in accordance with Article 2 of the third AMLD, credit institutions; financial institutions; auditors, external accountants and tax advisors; notaries and other independent legal professionals; trust or company service providers; real estate agents; and other natural or legal persons trading in goods and casinos.

receiving a copy of each US data request submitted and for assessing its compliance with EU privacy laws.16 Once such a request is approved, SWIFT is required to provide the data to the US Treasury. In the same manner, information obtained through the TFTP, including the name and account number of the payee, the name and bank details of the beneficiary, the amount transferred and the currency, is also made available to the law enforcement bodies of the Member States, Europol and Eurojust.17 Information can also be provided spontaneously – and shared with EU Member States – by the US Treasury. Europol can also initiate a series of requests to the US. In addition to its role in the application of the EU-US TFTP Agreement, Europol is also entitled to conclude cooperation agreements with non-EU countries. These include strategic agreements (limited to the exchange of general intelligence) and operational agreements that allow for the exchange of information, including financial data.18 At the time of writing, 17 operational agreements were in place.19

2.5. Law enforcement processing of data and data protection
In 2016, Directive 2016/680 on data protection in the field of Justice and Home Affairs was adopted as part of the data protection reform package. The directive is to be transposed by the Member States by May 2018 and requires, inter alia, that the data collected by law enforcement authorities be processed lawfully and fairly; be collected for specified, explicit and legitimate purposes and processed only in line with these purposes; and be adequate, relevant and not excessive in relation to the purpose for which they are processed. Furthermore, Member States are to establish time limits for erasing the personal data or for making a regular review of the need to store such data. The directive also assures that individuals have the right to have certain information made available to them. It replaces Framework Decision 2008/977/JHA, which was limited to the processing of data transmitted between the authorities of different Member States, therefore excluding the processing of domestic data. In addition, protection of data exchanges with non-EU countries for law enforcement purposes has been covered by dedicated agreements, such as the EU-US 'Umbrella Agreement', in force since February 2017.20

Apart from the existing legislative instruments outlined above, related provisions/instruments are currently being negotiated at EU level, notably: a proposed regulation on the protection of individuals with regard to the processing of personal data by the EU institutions (which would include EU agencies such as Europol or Eurojust); a July 2016 proposal to further amend the fourth AMLD (fifth AMLD); and the revision of the Cash Control Regulation.

3. Commission evaluations
This section gives an overview of the most recent Commission evaluations and analyses on the implementation of EU instruments facilitating law enforcement authorities' access to financial data, as detailed above.

3.1. Financial Intelligence Units
In June 2017, the Commission submitted its first supranational risk assessment (SNRA) of the risks of ML/TF affecting the internal market. It was accompanied by a document21 dedicated to financial intelligence units (FIUs). This was largely based on the findings of the EU FIUs Platform's mapping exercise conducted in 2016.22 The report identifies several obstacles faced by FIUs, including in relation to operational cooperation and access, exchange and use of information. While the mapping shows that the majority of FIUs have access to bank information via requests to individual banks or 'blanket request' to banks in their territory, it is argued

16 The role of Europol in the context of this agreement has been detailed in a report released in April 2011 (File No 2566-566).
18 The transfer of personal data to a third country is governed in the Europol Regulation that entered into force in May 2017 (Article 25). The categories of personal data that can be collected and processed include economic and financial information, such as data related to bank accounts, cash assets, property data, tax position (see Annex II of the Regulation).
19 The list of operational agreements in force are available on the Europol website. The Commission is due to assess the provisions contained in these cooperation agreements by 14 June 2021.
22 The Mapping Exercise was carried out by a dedicated Team led by the Italian FIU and members from the FIUs of France, Poland and Romania. The UK FIU contributed to the Project in its initial phase.
that this capacity could be improved through the use of central registries holding information on bank accounts.\textsuperscript{23} However, the SNRA report considers some of these weaknesses to be mitigated by both the entry into force of the fourth AMLD and the ongoing negotiations related to the fifth AMLD. On the one hand, the fourth AMLD introduces new requirements expanding the sources of financial information available to the FIUs and the competent authorities in the area of AML/combating the financing of terrorism (CTF). The list of obliged entities that are required to transmit STRs to the FIUs now includes providers of gambling services and traders accepting cash payments above €10 000. On the other hand, should the fifth AMLD be adopted, FIUs would be allowed to request information more easily from obliged entities. In addition, all Member States would be required to establish centralised bank and payment account registries, to which FIUs and the competent authorities would be granted access. The interactions between the fourth AMLD and the amended DAC Directive (see section 2.2) would also expand tax authorities' de facto access to these registries. Finally, virtual currencies exchange platforms and wallet providers would also become obliged entities. The latter provisions are linked to increasing concerns raised in the SNRA on the use of cash transactions for ML/TF purposes, which led the Commission to submit several proposals, including the revision of the Cash Control Regulation.\textsuperscript{24} The Council and the Parliament reached a provisional agreement on the fifth AMLD in December 2017, which does not substantially affect the above-mentioned provisions proposed by the Commission. The adoption of the text is scheduled for the April 2018 plenary part-session.

3.2. EU asset recovery offices

It has been estimated that while the annual value of confiscated assets in the EU is around €1.2 billion, this represents only 1.1% of criminal assets.\textsuperscript{25} Asset recovery offices (AROs), established in 2007 across the EU Member States (see section 2.3), are the national bodies responsible for facilitating the tracing and identification of proceeds of crime. In 2011, the Commission reported on the implementation of AROs across the Member States. The report noted that all Member States had established their AROs or were in the process of doing so. According to the assessment, the individual Member States’ AROs were generally satisfied with the degree of cooperation with each other. However, the report identified significant challenges that hamper their work, including a lack of resources and access (direct or indirect) to relevant information, notably bank account information.

3.3. The EU-US Terrorist Financing Tracking Programme Agreement and an EU equivalent

Joint reviews of the EU-US TFTP Agreement (see section 2.4) are regularly published. In its latest report, released in January 2017 and evaluating the 22 months between 1 March 2014 and 31 December 2015, the Commission claims that the essential safeguards and controls laid down in the agreement are being properly implemented. According to the Commission, TFTP-related data have given ‘key insights into the financial support for networks of terrorist organisations, helping to identify persons involved in the US, the EU and elsewhere’.\textsuperscript{26} The next review is scheduled for this year. However, ever since its adoption, the EU-US TFTP Agreement has remained controversial, including as regards the lack of transparency surrounding its evaluation (see sections 10 and 11). On the other hand, Article 11 of the EU-US TFTP Agreement explicitly mentions the possibility for the establishment of an equivalent EU system. An EU terrorist finance tracking system (EU TFTS) has subsequently been assessed in view of the principles of necessity, proportionality, cost-effectiveness and respect of fundamental rights. In its communication of 27 November 2013, the Commission concluded that while in terms of benefits, ‘an EU system could increase the EU and its Member States’ capacities to access relevant data’, such a system would not be proportionate or bring added value compared to the existing mechanisms. However, based on the Commission’s claims that the situation as regards threats to internal security is rapidly evolving,\textsuperscript{27} such a system is currently being re-assessed (see section 9).

\textsuperscript{23} Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information: pp. 87-90. In early 2017, it was estimated that approximately 10 EU Member States had a central registry for all holders of bank accounts. See: A. Scherrer, Fighting tax crimes, op.cit.

\textsuperscript{24} The proposal enables authorities to act on amounts lower than the current declaration threshold of €10 000, where there are suspicions of criminal activity. For state of play on this proposal, see legislative train schedule, European Parliament.

\textsuperscript{25} Europol, 2016 survey on criminal asset recovery in the EU.

\textsuperscript{26} The mechanism by the Member States and the EU is said to have increased significantly, generating 8 998 investigative leads provided to the Member States and Europol as compared to 3 929 leads in the previous reporting period.

4. Court of Justice of the European Union

While not specific to the processing of financial data, the rulings of the Court of Justice of the EU (CJEU) highlight its position as regards the processing of personal data for law enforcement purposes in a broader context. These rulings are all relevant as concerns the processing of financial data, since they show to what extent security measures pass the necessity and proportionality tests. In particular, they clarify critical aspects as regards data retention and transfers of data to non-EU countries.

As concerns data retention, in 2015, in the Digital Rights Ireland case, the CJEU invalidated Directive 2006/24/EC (the Data Retention Directive), which aimed to harmonise continued storage of data by telecommunication companies in order to ensure that these data are available for law enforcement purposes. In this case, the CJEU took the view that, by requiring the retention of such data and by allowing the competent national authorities to access them, the directive interfered in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data (set out respectively in Articles 7 and 8 of the EU Charter). While recognising that the retention of data genuinely satisfies an objective of general interest (namely, the fight against serious crime), the CJEU underlined that the provisions of the directive exceed the limits imposed by compliance with the principle of proportionality, whereby the content and form of EU action must be in keeping with the aim pursued (Article 5 TEU).

As regards transfers of personal data to non EU-countries, the CJEU has interpreted several provisions of EU agreements in this field. These have proved particularly controversial as regards data collected by airline companies (referred to as ‘passenger name records’, or PNR) for the purpose of facilitating exchange of reservation information (including names, travel dates, itineraries and contact details of passengers). In 2004, in the context of the war on terror, an Agreement between the European Community and the US on the processing and transfer of PNR data by air carriers to the US was reached, after the adequacy of US data protection mechanisms had been approved (the Decision on adequacy). Both instruments were adopted on the basis of Community law related to the functioning of the internal market. In 2006, an action initiated by the European Parliament led to the annulment by the CJEU of both instruments. The CJEU took the view that these instruments were not founded on an appropriate legal basis. As the purpose of the agreement was clearly to prevent and combat terrorism, it should have been adopted as part of the third pillar. This need for further clarification on the purpose of PNR data processing was supplemented by an opinion requested by the European Parliament and released in July 2017. In the context of the preparations for an agreement envisaging an exchange of PNR records between the EU and Canada, the CJEU declared that the draft agreement did not meet the requirements stemming from the fundamental rights of the EU (such as privacy and data protection laws), and thus may not be concluded in its current form.

Relevant CJEU rulings as regards the transfer of data to non-EU countries also include Schrems v Data Protection Commissioner, a 2015 case related to the transfer of Facebook data to the US authorities. In the light of the revelations made by Edward Snowden in 2013 concerning the activities of the US intelligence services, Mr Schrems took the view that the US authorities did not offer sufficient data protection against surveillance and, as some or all of the data provided by Facebook subscribers residing in the EU are transferred from Facebook's Irish subsidiary to servers located in the US, challenged the transfer of data from the EU to the US. In this context, the CJEU investigated the validity of the Safe Harbour Decision – the EU-US agreement meant to protect EU citizens’ data if transferred by US companies to the US. The CJEU found that the US Safe Harbour mechanism did not provide a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU, and as a result declared the Safe Harbour Decision invalid. The replacement of the Safe Harbour – the EU-US Privacy Shield – was agreed on 2 February 2016.

---

28. Article 52(1) of the EU Charter states: ‘Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.’

29. These data were to be retained for periods of not less than six months and not more than two years from the date of the communication.

30. EU privacy law forbids the movement of its citizens’ data outside of the EU, unless they is transferred to a location which is deemed to have ‘adequate’ privacy protection in line with that of the EU.

5. European Economic and Social Committee
The European Economic and Social Committee (EESC) has supported both the EU AML strategies and the initiatives to improve tax authorities' access to anti-money-laundering information. It nevertheless raised some concerns as regards data protection and fundamental rights of certain EU provisions on AML/CTF. In its 2016 opinion on Implementing the European Agenda on Security, the EESC stressed that the principle of proportionality was 'absolutely fundamental' and must be respected. In relation to controls of cash movements, the EESC recalled in its 2016 opinion on Terrorism financing – Controls of cash movements, that data protection should be strengthened 'due to the increase in the amount of data being collected and exchanged between authorities'.

6. European Banking Authority / European Securities and Markets Authority / European Insurance and Occupational Pensions Authority
In 2017, the European supervisory authorities (ESAs) issued a Joint Opinion on the risks of ML/TF affecting the EU financial sector. The opinion acknowledges that problems exist in key areas such as firms understanding of the ML/TF risks and the effective implementation of customer due diligence policies and procedures. It also points to difficulties associated with the lack of timely access to intelligence that might help identify and prevent terrorist financing, and considerable differences in the way competent authorities discharge their functions. In addition, the European Central Bank (ECB) issued an Opinion on the proposed fifth AMLD (see section 3.1). As regards central registries of bank and payment accounts, the ECB considers the task of establishing a central registry to 'clearly be a government task'. As a consequence, and with a view to safeguarding the financial independence of the ECB members and dispelling the monetary financing concerns associated with carrying out a government task, it emphasises that, in taking up the task of operating a central registry of accounts, the national legislation implementing the proposed directive should include a cost-recovery mechanism with explicit procedures for monitoring, allocating and invoicing all costs incurred by the national central banks that are associated with operating and granting access to the central registry.

7. European Data Protection Supervisor
The European Data Protection Supervisor (EDPS) has on numerous occasions expressed its view on the collection, storage and exchange of data for law enforcement purposes. In particular, it has made specific recommendations as regards data protection in the police and justice sectors in the context of the adoption of Directive 2016/680 (see section 2.5). The EDPS also gave its comments on the EU TPTS system in April 2014. It welcomed the Commission's efforts to analyse the principles of safeguarding fundamental rights, necessity, proportionality and cost-effectiveness, in its assessment (see section 3.3). However, it underlined that further assessment of the impact any EU tracking system would have on the existing EU-US TFTP Agreement would be welcome. On the other hand, in its opinion issued in February 2017, the EDPS raised severe concerns as regards the proposed fifth AMLD (see section 3.1). In particular, it noted that, as the proposal clearly targets tax evasion in addition to ML/TF, it introduces policy purposes other than countering ML/TF. This raises two issues: that of purpose limitation and that of the principle of proportionality. The EDPS also observed that various controllers are foreseen to process personal data (competent authorities in charge of investigating ML/TF or tax evasion, FIUs, etc.). As a result, the proposed amendments introduce a 'significant degree of uncertainty as to the purposes pursued and on the controllers entrusted with them'. The EDPS also emphasised that the provision related to the expansion of FIUs' access to financial data could lead to data mining and go well beyond targeted investigations. Overall, it deplored that the Commission

---

32 See: EESC Opinion on the Commission's proposal for a fourth AMLD; see also the EESC’s Opinion on the Anti-Money Laundering Package, submitted in 2013.
33 The three European supervisory authorities (ESAs) are the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA).
34 See, inter alia: Opinion on the EU-US TFTP, 22 June 2010; Opinion on the AMLD proposal, 4 July 2013; and Opinion on AML/CFT data processing, 13 May 2015.
35 ‘Data mining’ is the process of extracting patterns or trends from large amounts of information. Data mining rests on the creation of ‘profiles’, thus bearing the risk of discrimination against certain groups of people. See: D. Korff, ‘Passenger Name Records, data mining & data protection: the need for strong safeguards’, report prepared for the Council of Europe consultative committee of the Convention for the protection of individuals with regard to automatic processing of personal data, June 2015. In the EU, the principle of non-discrimination is guaranteed by Article 21 of the EU Charter.
has opted for 'blanket measures' with what it sees as major consequences in terms of personal data protection.

8. EU Justice and Home Affairs agencies
The above-mentioned concerns of the EDPS have been shared on many occasion by the EU Fundamental Rights Agency (FRA), which has regularly recommended to better embed fundamental rights in the security agenda. In particular, the FRA argues that such an approach would lead to more sustainable and thus more effective policies capable of passing the necessity and proportionality tests undertaken by the Court of Justice (see section 4).

On the other hand, Europol has various roles as regards the exchange of financial data at EU level. Europol hosts law enforcement information exchange platforms/networks, supports the use of the secure information exchange systems at EU level and monitors agreements with third countries (see section 2.4). Europol is also responsible for compliance with the data protection principles. As regards financial data, Europol is a key promoter of their exchange at EU level. In a 2015 report, Europol claimed that the use of cash by criminals remains 'one of the biggest threats reported by Law Enforcement in the area of money laundering, as well as one of the most significant barriers to successful investigations and prosecution'. The report included recommendations, including on how to make better use of the information contained in cash declarations and on the creation of an EU database for suspicious cross-border cash movements. Furthermore, in a 2017 report on financial intelligence, Europol recommended to allow greater access to financial intelligence across crime areas.

Eurojust also plays a key role in resolving some of the difficulties that arise in cross-border investigations. It has provided opinions on draft instruments related to the freezing and confiscation of proceeds of crime and on the European Investigation Order (EIO). In relation to access to financial data, Eurojust practitioners have underlined that the fact that some EU AROs do not have access to relevant databases for tracing and identifying assets is a major issue, supplemented by the fact that central bank registries for the identification of assets are lacking.

9. European Commission proposals
In October 2017, the European Commission presented its anti-terrorism package to better protect EU citizens, which includes initiatives to improve cross-border access by law enforcement to financial data. In its 2018 work programme, it announced its intention to propose an initiative as regards 1) improving cooperation among FIUs and facilitating their access to central bank account registries; 2) extending the access to bank account registries to law enforcement authorities; and 3) facilitating access to financial transaction data held in EU jurisdictions for counter-terrorism investigations. For what concerns the first initiative, proposals for improving cooperation among FIUs are included in the proposed fifth AMLD currently under negotiation (see section 3.1).

As regards the second initiative, the Commission is considering a self-standing legislative instrument to allow for broader access to centralised bank and payment account registries. The Commission published an inception impact assessment on this initiative in the summer of 2017. Access would not be restricted to

---

36 These include the AROs platform, co-chaired by the Europol Criminal Assets Bureau (ECAB). ECAB also holds the Secretariat of the Camden Asset Recovery Inter-Agency Network (CARIN) and of the Anti-Money Laundering Operational Network (AMON). See: Council of the EU, Implementation 2018-2021 EU Policy Cycle for organised and serious international crime, 12811/17, 4 October 2017.
37 Such as SIENA and FIU.net. While SIENA enables the swift exchange of information among various actors (Europol’s liaison officers, analysts and experts, Member States, and third parties with which Europol has cooperation agreements), FIU.net is a decentralised computer network enabling the exchange of information and cooperation between EU FIUs.
38 The EDPS is responsible for monitoring the processing of personal data by Europol (Article 43 of the Europol regulation). Furthermore, Member States’ national parliaments and the European Parliament have also set up a Joint Parliamentary Scrutiny Group (JPSG) and the EP’s consent is required before the adoption of operational agreements.
39 Europol, From suspicion to action – Converting financial intelligence into greater operational impact, 2017, p. 40
40 See: Interview with the chair of the Eurojust Financial and Economic Crime Team, pp. 14-15
FiUs and competent AML/CTF authorities, but would also be granted to other law enforcement and other authorities, such as AROs or anti-corruption authorities (ACAs). Whereas AROs are covered by EU legislation directly (see sections 2 and 3), ACAs are not. A targeted consultation of AROs and ACAs was conducted in June 2017, and the public consultation was closed on 9 January, 2018.

The third strand included in the Commission's 2018 work programme is related to additional measures to facilitate access to financial transaction data held in EU jurisdictions for counter-terrorism investigations. In February 2016, the EU Action plan for strengthening the fight against terrorist financing called for a new assessment of a possible EU TFTS in order to fill possible gaps, especially for what concerns transactions that are excluded from the EU-US TFTP Agreement, i.e. intra-EU payments in euro. Despite the prior negative assessment of the feasibility and opportunity for an EU TFTS (see section 2.3), a roadmap was published in October 2016 on 'a possible European system complementing the existing EU-US TFTP agreement'. According to the Commission's third progress report towards an effective and genuine Security Union, this renewed interest in a European tracking system is justified by a 'rapidly evolving pattern of terrorist financing'. Since the publication of this report, the Commission has been consulting stakeholders and has analysed the mechanisms through which competent authorities can currently access relevant information, particularly financial data stored in other Member States, and possible measures to address the gaps.

10. European Parliament position
This section provides an overview of selected EP resolutions and written questions by MEPs to the Commission of the current legislature, related to law enforcement authorities' access to financial data.

10.1. Resolutions
The European Parliament has generally supported law enforcement capabilities in the field of ML/TF, including efficient sharing of relevant data and information. However, it has also recalled on numerous occasions the need to establish adequate data protection and privacy safeguards. The latter concerns are particularly voiced where agreements with non-EU countries are concerned.

In its resolution of 11 February 2015 on anti-terrorism measures, the Parliament strongly encouraged a better exchange of information between Member States' law enforcement authorities and EU agencies. It also called for more effective operational cooperation among Member States and third countries (including through the use of the TFTP Agreement). In March 2018, Parliament adopted an own-initiative report recommending the setting up of a 'European counter-terrorism financial intelligence platform' with 'a joint database for data on physical and legal persons and suspicious transactions'. Parliament also recommended to oblige banks to monitor pre-paid debit cards (so as to ensure that they can only be reloaded through bank transfers and personally identifiable accounts) and called for an assessment of the role of virtual and crypto currencies, block chain and FinTech technologies in TF, and the extent to which these should be regulated at EU level.

In relation to tax evasion, in December 2017 and in concluding its inquiry into money laundering, tax avoidance and tax evasion, Parliament adopted a resolution in which it encouraged all Member States to put in place systems of bank account registries or electronic data retrieval systems that could be accessed by the FIUs and the competent authorities. It also recommended considering the standardisation and interconnection of national bank account registries containing all accounts linked to legal or natural persons for the purpose of easy access by law enforcement.

Parliament has also recalled on numerous occasions that law enforcement activities are subject to data protection and privacy safeguards. In its December 2014 resolution on renewing the EU Internal Security Strategy, Parliament underlined the utmost importance of the adoption of Directive 2016/680 (see section 2.5). This concern was confirmed in the July 2015 resolution on the European Agenda on Security, in which

---

42 In the area of corruption, the EU has contested competence and it is the Group of States against Corruption (GRECO), which operates at the level of the Council of Europe that monitors states' compliance with the anti-corruption standards. See here the GRECO list of ACAs at national level.

Parliament stressed that security measures should always be pursued in accordance with the protection of fundamental rights. As regards EU agreements with non-EU countries, the TFTP has remained controversial. After having initially rejected the EU-US TFTP Agreement amid concerns for privacy, proportionality and reciprocity (see section 3.3), the Parliament once again questioned this agreement in the light of Edward Snowden’s revelations on the alleged practices of the US government (in particular the NSA) related to mass surveillance, which included data extracted from the SWIFT database. It did so in its October 2013 resolution on the suspension of the agreement, then in its March 2014 resolution on the electronic mass surveillance of EU citizens, and then again in its follow-up resolution from October 2015. These resolutions go hand in hand with increasing demands of some MEPs for more transparency related to TFTP-related negotiations and implementation.44

10.2. MEPs’ questions
The questions addressed to the European Commission during the current legislature can be clustered around three key areas: EU cooperation related to exchange of information; data protection and security in data processing; latest initiatives as regards the regulation of bitcoins and cash for AML/CTF purposes.

The development of financial investigations and intelligence at EU level has been supported by MEPs, first and foremost in the field of ML/TF,45 assets freezing and confiscation,46 but also in relation to other serious crimes, such as human trafficking or other criminal activities.47 Inadequate implementation of the existing requirements under the AMLD has been stressed by MEPs, including in relation to the proper application of these requirements by the banking system48 and in relation to the exchange of information, for which Member States show a lack of willingness.49 Some MEPs have also asked for clarifications concerning the establishment of a European intelligence unit, contemplated by Commission President Jean-Claude Juncker in his 2017 State of the Union speech.50 In its reply, the Commission underlined the added value brought by the existing European Counter Terrorism Centre (ECTC) (hosted by Europol) and confirmed that the Commission was working ‘towards a future European Intelligence Unit’.

The idea to extend to law enforcement authorities the right to handle personal data processing without providing at the same time sufficient data protection safeguards, has nonetheless been questioned. The issue of exchange of information in the absence of reasonable suspicion has notably been brought to the attention of the Commission – in particular as regards the legal basis for such exchange as affects data protection.51 In its reply, the Commission recalled that the processing of personal data by law enforcement is covered by EU legislation, including Directive 2016/680 that will soon enter into force. Also related to data protection, several questions show recurrent concerns as regards the EU-US agreements, and notably the Umbrella Agreement (see section 2.5).52 In this regard, the Commission has specified that this agreement sets high data protection standards for personal data transferred to the US. In 2016, concerns were also raised as regards data breaches, in relation to reported leaks of sensitive information and data held by Europol on a number of terrorism-related investigations.53 In its reply, the Commission clarified that an

44 In 2012, the CJEU ruled on a complaint filed by Sophie in’t Veld (ALDE) that certain classified documents related to the TFTP must be partly disclosed. In 2013, a complaint to the EU’s Ombudsperson Emily O’Reilly related to Europol’s refusal to grant public access to a document related to the implementation of the TFTP Agreement was also submitted. Following her inquiry, Mrs O’Reilly concluded that Parliament should ensure that any future TFTP agreement, or any other similar agreements to be entered into in future, should contain a specific provision to ensure adequate scrutiny of EU executive action by EU control bodies. See: M. Wesseling, An EU Terrorist Finance Tracking System, Royal United Services Institute for Defence and Security Studies, September 2016.

45 See, inter alia: E-006947-15, 29 April 2015 (Aldo Patriciello, PPE); E-006045-16, 25 July 2016 (Mariya Gabriel, PPE); E-001855-17, 20 March 2017 (David Casa, PPE).

46 See, inter alia: E-015870-15, 16 December 2015 (Tomáš Zdechovský, PPE); E-008997-16, 30 November 2016 (Nuno Melo, PPE).

47 See, inter alia: E-010687-14, 12 December 2014, Roberta Metsola (PPE); E-007960-15, 19 May 2015, Ivan Jaković (ALDE).

48 E-001386-17, 21 March 2017 (Jeppe Kofod, S&D).

49 See, inter alia: E-000503-16, 25 January 2016 (Mariya Gabriel, PPE); E-003413-16, 27 April 2016 (Elissavet Vozemberg-Vronidi, PPE); P-009145-16, 1 December 2016 (Gérard Deprez and Louis Michel, ALDE).

50 See, inter alia: E-005863-17, 21 September 2017 (Rachida Dati, PPE); E-006712-17, 27 October 2017 (Richard Sulik, ECR); E-003936-18, 24 January 2018 (Doru-Claudian Frunzulicić, S&D).

51 P-004765-16, 9 June 2016 (Sophia in ’t Veld, ALDE).


53 The breach concerned 21 messages containing data that dated back to 2009. See: E-009043-16, 30 November 2016 (Jeroen Lenaers, PPE); E-009565-16, 19 December 2016 (Miriam Dalli, S&D).
investigation carried out by Europol revealed that such data breaches had occurred before 2009 and that since that time, Europol had introduced numerous technical measures to prevent further incidents.

As regards the **risks that some financial sectors would be used for ML/TF purposes**, questions have been raised related to the Commission's initiative on virtual currencies (VCs).\(^{54}\) In particular, the reliability of information showing that terrorist groups have been using bitcoins has been questioned.\(^{55}\) In its reply, the Commission referred to the findings of a FATF report from 2015 as justification for its proposal to bring anonymous currency exchanges under the control of the competent authorities by extending the scope of the AMLD (see section 3.1). Finally, it should be noted that some MEPs have raised concerns as regards a growing number of initiatives to **regulate and restrict cash payments** for AML/CTF purposes at EU level.\(^{56}\)

### 10.3. Petitions

In petitions related to law enforcement authorities' access to and exchange of information, concerns have particularly been raised in relation to **data protection** and the **right to privacy**. For example, one petitioner expressed worries as regards banking information being made available to the US through a private business.\(^{57}\) This was echoed in several petitions related to the alleged surveillance programmes carried out in the US affecting EU citizens' rights.\(^{58}\)

### 11. Academic literature

Law enforcement authorities' access to financial data has prompted numerous debates among scholars, notably as regards fundamental rights and lack of oversight mechanisms on data processing.

For instance, the extent to which the **EU-US TFTP Agreement** interferes with fundamental rights (thus echoing the concerns of the CJEU and the EDPS, see sections 4 and 7 above) has been consistently underlined.\(^{59}\) Some scholars have concluded that the agreement, even in its current form, **fails to comply with all the requirements laid down in the Charter**.\(^{60}\) *The rights of individuals* to access their data, to rectify them, and to obtain judicial redress are also considered as far too limited in practice.\(^{61}\) The potential added value of an equivalent EU system has also been reviewed. Some scholars have emphasised that if an EU TFTP were to be introduced because it would arguably provide benefits in terms of intelligence or efficiency, this would likely be the **subject of intensive debate** at EU level, in particular in terms of fundamental rights and oversight.\(^{62}\)

Furthermore, the **extension of the EU anti-money laundering regime** to include terrorist financing and more recently tax crime (thus allowing for greater access to an increasing number of data by multiple actors) has also raised concerns, as this 'catch-all' approach may prove ineffective and furthermore undermines the core principle of purpose limitation.\(^{63}\) Related to this, it is noted that the distinction **between financial investigation** – during which data are collected for evidence purposes – and **financial intelligence**, in the course of which data are collected on the basis of suspicion, is increasingly blurred.\(^{64}\) Broadening the purposes for which data are collected and processed not only raises the issue of the **presumption of innocence**, but it can also be **counterproductive because it hampers good cooperation**. In the case of FIUs, for instance, cooperation with other FIUs is based on purpose limitation. In principle, FIUs exchange data

---

54 See, *inter alia*: E-004086-17, 20 June 2017; (Marlene Mizzi, S&D); E-005169-17, 3 August 2017 (Roberta Metsola, PPE).
55 E-005169-17, 3 August 2017 (Roberta Metsola, PPE).
56 E-000720-17, 1 February 2017 (Othmar Karas, PPE); E-000929-17, 9 February 2017 (Pascal Arimont, PPE); E-001461-17, 2 March 2017 (Dubravka Šuica, S&D).
57 Petition 0193/2013.
61 Blasi Casagran, op.cit.
64 The increasing confusion between intelligence and evidence in the field of anti-terrorism and the challenges this raises for legal certainty and safeguards has been noted in particular in: D. Bigo et al., *National security and secret evidence in legislation and before the courts*, Study for Policy Department C, European Parliament, 2014.
exclusively for analytical purposes and intelligence. As such, these data cannot be used in the context of investigations, prosecutions or legal proceedings and cannot be exchanged for that purpose. Therefore, blurring the distinction between data collected for intelligence purposes and for investigative purposes is recognised to have a negative impact on the cross-border cooperation of FIUs.65 This aspect is echoed by FIU officials themselves.66

Concerns are also raised as regards the role of Europol as responsible for verifying compliance regarding the exchange of data in the framework of the TFTP Agreement: Europol is not a judicial authority and its role of impartial controller is challenged.67 Furthermore, Europol's effective power to perform a strict scrutiny of the US requests has also been examined.68 Europol's operational agreements with non-EU countries other than the US have moreover been the subject of debates. Some scholars have raised doubts about the adequacy of data protection in the exchange of data these agreements allow,69 while others have insisted on the positive impact these agreements have had in raising data protection standards in third countries.70 The lack of transparency surrounding EU-level informal law-enforcement networks – especially those hosted by Europol and where exchange of data occurs – has also been pointed out.71 At a more general level, in contexts where law enforcement access to data, be it financial, commercial, or other, is increasingly maximised,72 the need for proper oversight at national and EU level has been emphasised.73

Table: Initiatives to facilitate cross-border access to and use of financial data by law enforcement authorities

<table>
<thead>
<tr>
<th>EP committees responsible at the time of adoption of the relevant pieces of EU legislation: LIBE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of adoption of original legislation in plenary: The Commission’s initiatives will have an impact on several existing EU instruments in the field of cross-border investigation and cross-border exchange of data, which are related in particular to money laundering and terrorist financing.</td>
</tr>
<tr>
<td>Planned dates for review: 17 April 2018.</td>
</tr>
</tbody>
</table>

To contact the Ex-Post Evaluation Unit, please e-mail: EPRS-ExPostEvaluation@ep.europa.eu


This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.


65 A. Amicelle, ‘Comparative analysis of FIUs in Canada, France, Switzerland and United Kingdom’, in A. Scherrer, Fighting tax crimes: Cooperation between Financial Intelligence Units. EPRS Study, March 2017.
66 In the 2016 Mapping exercise on FIUs (op.cit.), it is noted that the delimitation of intelligence and investigation is not sufficiently clear and has a negative impact on the cross-border cooperation of FIUs (see p. 140).
67 See: M. Tzanou (op.cit.), ‘The role of Europol under the TFTP: a fox guarding the henhouse?’, p. 200 and seq.
68 This was also echoed in a Joint Scrutiny Board (JSB) report from 2011 that underlined that some information had been exchanged ‘orally’ between the US staff and Europol, thus making verifications impossible.