BRIEFING

Initial Appraisal of a European Commission Impact Assessment

European Parliament

Access to financial data by law enforcement authorities

Impact assessment (SWD(2018) 114, SWD(2018) 115 (summary)) accompanying a Commission 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

This briefing provides an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) accompanying the above-mentioned proposal, submitted on 17 April 2018 and referred to Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE). According to the IA, groups committing serious crimes, including terrorists, often operate cross-border and their funds are usually located across the EU Member States or outside of the EU.[1] In order to finance their hostile activities, terrorists may potentially use existing financial infrastructures.[2] Sharing financial information[3] effectively among national law enforcement authorities (LEAs) and financial intelligence units (FIUs)[4] is considered key to enable a quick and proportionate response to prevent and fight crime and terrorism. The proposal is included in the 2018 Commission work programme and also in the Joint Declaration on the EU's legislative priorities for 2018-2019.

Problem definition

According to the Commission, modalities as to how FIUs and LEAs access and exchange financial information vary across Member States, resulting in diverging practices in the EU. This is problematic, not just because inefficient procedures negatively affect domestic and cross-border financial investigations, but also due to the impact on procedural safeguards, which are important to protect fundamental rights (IA, pp. 10-15). The IA identifies two main problems:

1. LEAs are hindered by the lack of or delayed access to financial information

Under the fourth and fifth anti-money laundering directives (AMLD), LEAs do not have direct access to financial information stored in centralised bank account registries (CBAR) or data retrieval systems (DRS), and the use of the data is limited to fighting money laundering and terrorist financing. The Commission argues that LEAs should have direct access to this data, even if it were to be used in a wider context of fighting all serious crime (IA, p. 19). Currently, LEAs have to issue 'blanket requests' concerning a person of interest in order to obtain financial information from financial institutions. This procedure, which may take a long time, can result in inefficient investigations impeding the effective fight against terrorism and crime. In addition, the practice of issuing blanket requests poses a great administrative burden on both the banking sector and LEAs. The current practice is also problematic because it entails the untargeted dissemination of personal information, such as an individual's name, to the private sector. This is unsatisfactory, according to the European Data Protection Supervisor (EDPS) (IA, pp. 12-13).

Furthermore, current legislation does not give LEAs efficient and effective access to other types of financial information, 'which is necessary for their tasks' (IA, p. 20). While the fourth and fifth AMLD provide that FIUs must be able to respond to requests for information from LEAs (Article 32), the

Author: Katharina Eisele with Anne van Heijst
Ex-Ante Impact Assessment Unit
PE 621.827 – June 2018

following issues remain: (i) LEAs can only request such information for combating money laundering and terrorist financing, yet it is considered necessary for all types of serious offences; (ii) the issue of cross-border requests for information is not regulated; (iii) Article 32 only covers information that is already in the possession of a FIU and does not cover information that FIUs can obtain without coercive measures under their powers; and (iv) when FIUs are administrative in nature, they have legal difficulties to respond to requests from LEAs.

2. Obstacles to cooperation between FIUs and to their accessing information from LEAs

Although the fourth and fifth AMLD require that the information received by an FIU from another FIU or LEA should be used to process or analyse information relating to the specific purpose of money laundering or terrorist financing and to the natural or legal person involved, there are no rules as to how this should be achieved. As a result, FIUs face obstacles in collecting information and exchanging it with other FIUs and LEAs in the EU, such as: differences concerning the methods for requesting and exchanging information due the various status and powers granted to FIUs nationally;[5] the need to use law enforcement cooperation channels; and the identification and type of associate predicate offences that give rise to money laundering (IA, p. 20). Cooperation is also hampered by a lack of common rules that ensure sufficient, adequate and proportionate safeguards, resulting in uncertainty as to what information can be exchanged, under which conditions, with which limitations and confidentiality, whilst ensuring compliance with fundamental rights (IA, p. 21).

Objectives of the initiative

The **general policy objective** of the legislative proposal is to increase security in the EU by:

- providing the relevant public authorities for the prevention, investigation and prosecution of crimes with an improved access to financial information;
- enhancing the ability of FIUs to more effectively combat money laundering and terrorist financing;
- defining the conditions for access and exchange of information between the various authorities and providing for adequate procedural and data protection safeguards.

These general objectives are translated into the following **specific policy objectives**:

- Enable LEAs to get timely access, under well-defined conditions and for specified purposes, to information contained in the CBAR and DRS.
- Reduce the administrative burden both for LEAs and the private sector in getting/providing access to the information in the CBAR and DRS.
- Improve LEAs' access to financial information for the purposes of preventing, investigating, enforcing and prosecuting serious crime, without prejudice to national procedural safeguards.
- Facilitate FIUs' access to law enforcement information to enable them to carry out their current tasks under the fourth and fifth AMLD, without prejudice to national procedural safeguards.
- Remove obstacles to the cooperation and exchange of information between FIUs, without prejudice to the provisions of the fourth and fifth AMLD.
- Provide the competent authorities with adequate tools to trace and identify criminal assets.
- Set out specific, adequate and harmonised safeguards for the protection of privacy and personal data.

The IA points out that the envisaged EU measures would not aim to amend the fourth and fifth AMLD, but rather complement it. According to the Commission's Better Regulation Guidelines, the general objective should be Treaty-based; while this is the case ('increase security'), the general objective is formulated in quite specific terms and, in places, is phrased almost identicallly to the specific objectives. The **operational objectives** are listed in the section of the IA on monitoring and

evaluation, after the selection of the preferred option, which is in line with the Better Regulation (BR) Guidelines (IA, p. 72).

Range of options considered

The baseline scenario is based on the current national, EU and international framework for cooperation between FIUs and LEAs. Under the baseline, the risk of fragmentation at national level concerning law enforcement access to national bank registries would be likely to persist (IA, pp. 28-29). The Commission lists three categories of policy options (A/B/C, see table below). Non-legislative options were discarded because they would not solve the problems, which are regulatory in nature (IA, pp. 29-31, 37). The Commission furthermore discarded the option of a central EU FIU (already dismissed in the IA accompanying the fifth AMLD)[6] and the option of granting Europol direct access to CBARs as disproportionate (IA, p. 38).

Options Block A: the ´WHEN´: in what cases should the relevant authorities have access to or exchange information?	
A.1	Only in cases of money laundering and terrorist financing, LEAs get access to CBAR and DRS
A.2	In cases concerning ´Eurocrimes´ as laid down in Article 83(1) TFEU
A.3	In cases concerning crimes under Article 3(1) of the Europol Regulation[7]
Options Block B: the ´HOW´: how should public authorities access and exchange information?	
B.1	LEAs are provided with access to national CBAR/DRS: B.1.A: Direct access, under well-defined conditions as explained in the IA B.1.B: Indirect access, under well-defined conditions as explained in the IA
B.2	LEAs are provided with all other financial information, meaning all types of information from obliged entities under the fourth AMLD (e.g. banks) or held by FIUs, including transaction data: B.2.A: Direct access from the financial institutions B.2.B: Indirect access via the FIUs
B.3	The measures to facilitate access to and exchange of information will set out the conditions and safeguards for the exchange of information between FIUs and for FIUs' access to and exchange of information that LEAs hold: B.3.A: Direct cooperation between FIUs B.3.B: Establish a central EU FIU
Options Block C: the ´WHO´: to which public authorities do the conditions apply?	
C.1	The authorities as defined in Article 3(7)(a) of Directive (EU) 2016/680 (Data Protection Directive for Police and Criminal Justice Authorities)
C.2	The authorities in option C.1 and in addition: C.2.A: the Asset Recovery Offices (AROs) C.2.B: the European Agency for Law Enforcement Cooperation (Europol) C.2.C: the European Anti-Fraud Office (OLAF)

While the Commission's inception impact assessment indicated the additional option of providing direct access to Anti-Corruption Authorities (ACAs), this was not considered in the IA. The Commission indicates a preferred combination of options. Regarding the problems encountered by LEAs, the **preferred options** are: **A.3** (cases of crimes under Article 3(1) of the Europol Regulation), **B.1.A** (LEAs are provided with direct access to national CBAR/DRS), and **C.2.A** (authorities as defined in Article 3(7)(a) of the Data Protection Directive for Police and Criminal Justice Authorities and AROs).

Regarding the problems encountered by FIUs, the **preferred options** are: **A.1** (LEAs get access to CBAR and DRS only in cases of money laundering and terrorist financing), **B.2.B** (LEAs are provided with indirect access to all other financial information via the FIUs), **B.3** (the measures to facilitate access to and exchange of information will set out the conditions and safeguards for the exchange of information between FIUs and for FIUs access to and exchange of information that LEAs hold) and **C.2.B** (authorities as defined in Article 3(7)(a) of Data Protection Directive for Police and Criminal Justice Authorities and Europol)(IA, pp. 66-67).

Regarding the access of competent authorities to additional financial information, the **preferred options** are: **A.3** (cases of crimes under Article 3(1) of the Europol Regulation), **B.2.B** (LEAs are provided with indirect access to all other financial information via the FIUs), and **C.2.B** (authorities as defined in Article 3(7)(a) of the Data Protection Directive for Police and Criminal Justice Authorities and Europol) (see IA executive summary, p. 1).

However, the Commission's overall preferred option based on these combinations, and how they would co-exist, is not clear. Moreover, the preferred combination of options in the IA's executive summary does not entirely correspond to those indicated in the IA report itself.

Scope of the impact assessment

The Commission assesses the economic, social and fundamental rights impacts of the policy options. The IA is mostly qualitative because of a lack of comprehensive and reliable data, about which the Commission is open. Environmental impacts are considered irrelevant (IA, p. 38).

With regard to economic impacts, the Commission notes in more general terms that 'the more effective the fight against serious and transnational crime, the greater are the positive impacts on the economy' (IA, p. 38). Although it acknowledges that the causal effects of the options on the Member States' economies are difficult to assess, it attempts to quantify the effects by considering the current practices. The administrative costs of the blanket request practice range between €94 000 and €245 000 000 per year (IA, p. 39), which is a very wide range. Regarding the access to CBAR and DRS registries, the Commission argues that the broader the list of crimes for which access can be requested, the greater would be the savings on investigative costs (Block A, IA, p. 40). Options in Block B are assessed according to the type of connection they entail to the national centralised bank account registry or data retrieval system, which can be either direct or indirect. The basic cost of a direct connections to a system (option B.1.A) varies between €5 000 and €30 000 per authority (to be multiplied by the number of authorities connected to the network) (IA, p. 41). The more authorities that have access to the registries, the greater the savings (Block C, IA, p. 42).

The Commission considers that any improvement in the capacity of responsible authorities to fight serious and cross-border crime would have a positive social impact, such as improved deterrence for criminals, better protection of victims, improved security for EU citizens and increased public confidence in crime disruption mechanisms (IA, p. 46). Although hard data is absent, the Commission takes the view that the broader the list of crimes, the more effective and efficient would be the investigations (Block A, IA, p. 46). Likewise, the more direct the access to registries, the more successful would be the criminal investigations (Block B, IA, p. 47). The more authorities have access to these registries, the greater would be the impact on investigating crimes (Block C, IA, p. 48).

Concerning the impact on fundamental rights, the Commission observes that the measures proposed imply interference with the right to privacy and the right to data protection as guaranteed

by Articles 7 and 8 of the EU Charter on Fundamental Rights (IA, p. 52). The IA states that due to the limited scope of the specific data under consideration and the fact that the authorities would not be able to access information on transactions or bank balances (but rather, for instance, on the name of a bank account holder or IBAN number), the interference with the right to privacy would be 'relatively limited' (IA, p. 53). The IA could have explained more clearly how the rights of people affected would be protected in an investigation concerning serious crimes (Block A, IA, p. 54). This was also underlined by the EDPS in relation to the proposed fifth AMLD referring to the principle of purpose limitation (e.g. problematic multiplication of different data controllers).[8] The IA acknowledges that direct access to the registries by competent authorities would have a substantial impact on data protection, and lists a series of safeguards (Block B, IA, p. 55). The Commission highlights that the new Data Protection Directive for Police and Criminal Justice Authorities and the General Data Protection Regulation (GDPR) will be applicable (Block C, IA, p. 56). On cooperation between FIUs and between FIUs and LEAs, the IA admits that adding more types of crimes (under option A.3) will have a big impact on fundamental rights. It mentions a number of guarantees, which specify, for example, purpose limitation and grounds for refusal of requests to access or exchange data (Block A and B, IA, pp. 57-58).[9] The IA details a set of additional data protection parameters (such as lawful collection of data, storage limitation, etc.) that have to be implemented for all options examined (IA, pp. 59-61). The presentation of the impacts is not always clear. For example, it is not clear what safeguards are referred to in the IA (IA, pp. 57-58). The IA finally compares the options considered in terms of their effectiveness/social impacts, efficiency, fundamental rights impacts, and coherence (IA, pp. 61-66).

Subsidiarity / proportionality

The Commission considers Article 87(2) TFEU as the appropriate legal basis.[10] The IA states that 'it is necessary to act at a European level because of the cross-border dimension of crime, including organised crime and terrorism and the international nature of financial services, which allows criminals and terrorists to move funds across the EU' and that 'the problems and limitations related to the FIUs' access to, and use of, financial information can only be effectively dealt with by an EU instrument' (IA, p. 25). The Commission regards the added value of EU action to be: i) a formal and harmonised obligation on FIUs to cooperate amongst themselves and with LEAs; ii) a formal and harmonised access of FIUs to law enforcement information for the purpose of fulfilling their tasks; and iii) an effective and efficient access by LEAs to valuable financial information for the purpose of preventing, investigating, enforcing and prosecuting serious crime. Also, action at the EU level would help to ensure harmonised provisions, including for safeguarding data protection (IA, p. 26).

The IA considers the proposed measures to be proportionate – interference with the right to the protection of personal data and privacy will be kept to a minimum and in most cases is considered to be neutral in view of the safeguards applicable to the criminal investigations. The IA explains that direct access will be allowed to the central bank account registries and retrieval systems since they contain limited information. Access to other types of financial information will be possible via the FIUs. The above parameters ensure that the preferred option does not go beyond what is necessary to achieve the objective identified for the EU intervention, and at the same time qualifies as the least intrusive legislative instruments that could be adopted at EU level (IA, p. 69).[11] No reasoned opinions on the proposed directive have been submitted by national parliaments at the time of writing; the deadline for submission is 13 July 2018.

Budgetary or public finance implications

The Commission points out that the proposal has no implications for the EU budget (explanatory memorandum of the proposal, p. 10). The costs of implementing direct access to CBARs and DRS and of the access to financial information via the FIUs will impact on national budgets and administrations. However, these costs should be offset by a reduction in the current administrative and financial costs of competent authorities, as well as by cost savings due to a more efficient cooperation between FIUs and with competent authorities (IA executive summary, p. 2).

SME test / Competitiveness

The IA notes that the impact for economic operators could not be quantified for the purposes of this IA, and that it 'may be the most burdensome for SMEs and newly designated obliged entities. Nevertheless, the preferred EU measures would also contribute to legal certainty and transparency in the relationship between public authorities and economic operators, by pursuing the most proportional option in terms of compliance costs (kept to a minimum) and ensuring accountability on the side of the public authorities' (IA, p. 68). By contrast, the executive summary of the IA states that 'no specific impacts are expected on SMEs and micro-enterprises' (p. 2).

Simplification and other regulatory implications

The Commission explains that the proposal is in line with Union policy aims and with the case law of the CJEU. The proposal is part of the 2015 European Agenda on Security, complements the preventive side of the AMLD and reinforces the legal framework on police cooperation. The proposal also reinforces the Union criminal law framework on the fight against serious offences. The proposal repeals Council Decision 2000/642/JHA (explanatory memorandum to the proposal, pp. 3-4, 9).

Quality of data, research and analysis

The Commission points out that the consultation process was the 'primary source of evidence used in the impact assessment' (IA, Annex 1, p. 77). Other sources included the IA accompanying the fifth AMLD and the 'second updated report on the establishment of centralised bank account registers as an effective tool for financial investigations and asset recovery' of the Asset Recovery Offices (ARO) Platform sub-working group on centralised bank account registers of 2 March 2016.[12] The Commission admits that the calculations of costs and benefits were limited due to the lack of data. It highlights that it made 'significant efforts' to collect data, or at least estimates, from public authorities on the costs associated with the preparation of blanket requests, their handling and the processing of answers. It also attempted to collect financial estimates on the costs related to the establishment of direct access to the national centralised bank account registry or data retrieval system. As this information was not available, assumptions have been made on the basis of the establishment of connections to EU systems, such as Europol's Secure Information Exchange Network Application (SIENA) or Business Registers Interconnection System (BRIS). The assumptions are explained (see for example IA, p. 41). Similarly, the Commission managed to collect statistics on the number of requests for information from the national bank account registries or data retrieval systems or the number of blanket requests sent by the different authorities (IA, p. 77; see Annex 4 of the IA on analytical methods).

Stakeholder consultation

The IA identifies the stakeholders affected by the initiative, including individuals, the banking sector, LEAs, as well as the authorities managing registries or data retrieval systems (IA, Annex 3). Generally speaking, the Commission appears to have consulted widely. An open online public consultation on broadening law enforcement access to centralised bank account registries was conducted from 17 October 2017 to 19 January 2018. It only received 21 valid replies (IA, Annex 2, pp. 80-81). In addition, the Commission disseminated a questionnaire on access to centralised bank account registers to the Asset Recovery Offices (AROs) and ACAs of the Member States and Switzerland in June 2016. About 90 % of all authorities replying (25 AROs and 13 ACAs), having access to registers or not, consider that access to such registers facilitates (or would facilitate) substantially the execution of their tasks. The Commission also organised an expert meeting and an ARO platform meeting in 2017 (IA, Annex 2, pp. 83-88). As far as removing obstacles to cooperation between FIUs and enforcement authorities is concerned, the Commission consulted the FIUs' Platform in a mapping exercise and also created an online EU survey in 2016, to which all 28 EU FIUs responded. Further meetings were held in this regard (IA, Annex 2, pp. 87-93). Finally, the IA refers to a Eurobarometer survey of December 2017,[13] according to which a significant majority of respondents

in all Member States agree on the need to share information within the EU to better fight crime and terrorism (IA, Annex 2, pp. 88-93). While the IA provides information on the stakeholder views in accordance with the BR Guidelines, it does not systematically detailed which group supports which specific option.

Monitoring and evaluation

The Commission will prepare regular implementation reports (the first one is envisaged three years after the entry into force of the legislation) and an evaluation no sooner than six years after the date of the transposition. A monitoring programme will be set up by the Commission, and Member States are required to report on an annual basis (see Article 16 on monitoring of the proposal). The IA identifies monitoring indicators, which were in general taken over in the proposal (IA, pp. 69-72).

Commission Regulatory Scrutiny Board

The European Commission's Regulatory Scrutiny Board (RSB) issued a negative opinion on 23 February 2018. The RSB identified 'important shortcomings', pointing out that: (1) the report does not adequately explain to what extent the initiative is going beyond the commitments under the anti-money laundering legislation; (2) the need to act for the EU in domains where Member States may be competent is not sufficiently explained; (3) the design and content of the options are not sufficiently clear; (4) the impacts are not well analysed, especially with regard to data protection safeguards and other fundamental rights. In its second opinion, marked 'positive with reservations', of 23 March 2018, the RSB acknowledges the changes undertaken, but still notes 'significant shortcomings' indicating that (1) the scope of the initiative is not well defined; (2) the precise content of the preferred option remains unclear; (3) the impacts on fundamental rights are not comprehensively examined, in particular given the extension of the scope to serious crimes. The Commission explains how the RSB's concerns in its second opinion were addressed in the final IA (IA, Annex 1, pp. 74-76), in line with the BR Guidelines. Efforts were clearly made to integrate the RSB's comments, however, some could have been addressed more thoroughly, such as the content of the preferred option.

Coherence between the Commission's legislative proposal and IA

According to the Commission, the proposal corresponds to the preferred policy options considered in the IA (explanatory memorandum of the proposal, p. 9). However, as explained above, the IA does not clearly present the *overall* design of the preferred line of action, and so it is difficult to assess the full extent of coherence.

Conclusions

The general impression is that the IA examines comprehensively the problems encountered by LEAs and FIUs, and makes a real attempt to analyse the impacts of a new measure that would improve their capabilities to collect and exchange financial data needed for cross-border criminal investigations. A more thorough analysis of the safeguards on fundamental rights would have been useful, in particular as regards the inclusion of serious crimes in the scope of the proposal. The Commission admits that the calculations of costs and benefits were limited due to a lack of data. Despite its apparently keen efforts to consult, there were only 21 valid replies to the open public consultation. Finally, the overall preferred option remains unclear and the preferred combination of options in the IA's executive summary does not entirely correspond to those indicated in the IA report itself.

ENDNOTES

[1] See also A. Scherrer, Law enforcement access to financial data, implementation appraisal, EPRS, European Parliament, April 2018.

[2] See also W. van Ballegooij and P. Bakowski, The Fight against Terrorism - Cost of Non-Europe Report, EPRS, European Parliament, May 2018.

[3] The IA defines financial information as data about financial assets and transactions of legal entities and natural persons, primarily stored by economic operators, such as credit and financial institutions, see IA, p. 10, footnote 25.

[4] FIUs are operationally independent and autonomous units with the authority and capacity to take autonomous decisions to analyse, request and disseminate their analyses to competent authorities, where there are grounds to suspect money laundering, associated crimes or terrorist financing (IA, p. 6, footnote 16).

[5] Member States have developed three main models: judicial FIUs, administrative FIUs and hybrid FIUs, see A. Scherrer, Fighting tax crimes – Cooperation between Financial Intelligence Units, Ex-Post Impact Assessment, EPRS, European Parliament, March 2017, pp. 37-39.

[6] European Commission impact assessment accompanying proposal for a directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, SWD(2016) 223, 5 July 2016, see C. Collovà, Prevention of the use of the financial system for the purposes of money laundering or terrorist financing, initial appraisal, EPRS, European Parliament, October 2016.

[7] See Annex I of Regulation (EU) 2016/794 for a list of crimes referred to in Article 3(1).

[8] European Data Protection Supervisor, EDPS Opinion 1/2017 on a Commission proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC, 2 February 2017, pp. 8-11.

[9] According to the principle of purpose limitation, data is to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, see Article 5(1)(b) of the General Data Protection Directive.

[10] Article 87(2) TFEU empowers the EU to establish measures concerning the collection, storage and exchange of relevant information and common investigative techniques in relation to the detection of serious forms of organised crime, for the purpose of establishing police cooperation involving all the Member States' competent authorities.

[11] However, with regard to the proposed fifth AMLD, the EDPS raised concerns regarding the principle of proportionality in the proposal, see European Data Protection Supervisor, EDPS Opinion 1/2017 on a Commission proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC, 2 February 2017, pp. 11-14.

[12] This report does not appear to be publicly avaliable at the time of writing.

[13] Special Eurobarometer 464b: Europeans' attitudes towards security, December 2017.

This briefing, prepared for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), analyses whether the principal criteria laid down in the Commission's own Better Regulation Guidelines, as well as additional factors identified by the Parliament in its Impact Assessment Handbook, appear to be met by the IA. It does not attempt to deal with the substance of the proposal.

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)