Institutiones Administrationis – Journal of Administrative Sciences Vol. 2 (2022) No. 2, 23–34
DOI: 10.54201/iajas.v2i2.49

IV. AML Directive: Problems related to exchange of information between Financial Intelligence Units

Yana Daudrikh*

* Researcher, Comenius University Bratislava, Faculty of Law, Department of Financial Law. E-mail: yana.daudrikh@flaw.uniba.sk

Abstract

The presented paper is devoted to application problems in the field of ensuring international cooperation between Financial Intelligence Units. In accordance with the set goal, the author further analyses the existing application problems related to the exchange of information between the Financial Intelligence Units of the European Union. A special part of the paper focuses on the issue of the absence of uniform regulation at the level of the European Union in the area of information exchange between the European Union Financial Intelligence Units and the Financial Intelligence Units of third countries. In addition, the author further analyses the use of communication channels between the Financial Intelligence Units related to the assurance of sufficient protection of personal data.

Keywords

IV. AML Directive, Financial Intelligence Unit, data protection, FIU.net.

1 Introduction

The Financial Intelligence Unit of a Member State of the European Union (EU FIU) serves as the national centre for receiving and analysing reports of suspicious business transactions, as well as other reports related to money laundering and terrorist financing and for reporting the results of its analysis to the competent authorities. All Member States have set up FIUs to collect and analyse information received under the provisions of Directive 91/308/EEC with the aim of establishing links between suspicious financial transactions and underlying criminal activity in order to prevent and to combat money laundering.[1] The legal requirement for the establishment of FIUs in the EU Member States was stipulated by Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[1] Recital 2 of Council Decision (2000/642/JHA) concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.

The creation of the FIU framework was primarily designed to support law enforcement agencies and courts, which play an equally important role in the investigation of money laundering and terrorist financing. When considering the creation of the FIU, it was authoritative to create a central collection point for receiving and analysing reports on suspicious transactions. The reason for creating a single institution was to promote trust in the system of combating money laundering.

The functions rendered by the EU FIU can be divided into primary and secondary ones. The definition of the primary function is further specified in the recommendation of the Financial Action Task Force (FATF, 2012-2022, 24), which became the basis for Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (AML IV Directive), which has been fully transposed.[2] The primary (core) function of the EU FIU is thus the reception, analysis, and provision of information to the competent authorities. The reception of information by the EU FIU includes collecting and gathering information related to money laundering and terrorist financing from obliged entities. These include, credit institutions, financial institutions, auditors, notaries, gambling service providers, wallet service providers, and the like.[3] Obliged entities have the duty to communicate all suspicious business transactions carried out by their clients to the EU FIU. While the core function of the EU FIU is directly mandated by the AML IV Directive, its secondary functions may include different tasks depending on the FIU model chosen by the Member State (IMF, 2004, 34). We believe that the most important secondary function of the EU FIU is its supervisory role, which includes conducting audits of compliance with the relevant legal regulations by the obliged entities and to impose sanctions whenever failures are identified (imposition of sanctions function). In addition, the FIU's secondary function includes developing guidelines (relating to the submission of opinions on the practical application of the relevant legislative regulations), producing national risk assessments, and performing international cooperation tasks (Dražková, 2021, 64).

Moreover, FIU is responsible for exercising a national risk assessment which is one of the key requirements to identify, assess, and understand the money laundering and terrorist financing risks at the national level of individual member states. The risk assessment takes into account risk factors, as well as the risk assessment developed by the authorities of the European Union and other international institutions. The national risk assessment is updated mainly taking into account the developments and trends of the money laundering and terrorist financing risks. The Financial Intelligence Unit will provide the results of the national risk assessment to the Council of Europe, the European Commission, the participants of the European System of Financial Supervision and other member states for the purpose of preventing the money laundering and financing of terrorism. The Financial Intelligence Unit publishes the final national risk assessment report on its website. The Financial Intelligence Unit continuously informs obliged entities about the risks identified in the national risk assessment and about the measures taken to mitigate them.

It is clear that the entire EU FIU function cannot be defined accurately, mainly due to significant variances between the different EU FIU models. Although the AML IV Directive directly

[2] For more details see: Nanyun & Nasiri (2021).

[3] Article 2 of AML IV Directive.

regulates the obligation for Member States to ensure the greatest possible degree of cooperation between EU FIUs – notwithstanding their model (organizational structure) – we continue to examine a number of application problems at present, which, in our view, are directly linked to the heterogeneity of EU FIU models.

The list of authorities designated as competent for the AML/CTF supervision of financial institutions in the EU is maintained by the European Banking Autority.[4]

It follows from the above that we consider the absence of uniform legislation at the EU level comprehensively regulating the uniform position of FIUs across the EU Member States to be a fundamental obstacle. It led to divergent national legislation on the position of EU FIUs since EU Member States were given the freedom to choose their own FIU model. As a result, the following EU FIU models currently exist: administrative, law enforcement (police), judicial (prosecutor), or hybrid (Brewczyńska, 2021, 2). The inconsistency of the EU FIU models causes various types of issues, related in particular to the response time to information requests and disclosures within the framework of international cooperation between national EU FIUs, or related to the establishment of additional duties for FIUs. There is also still a lack of uniform regulation in the area of information exchange between EU and third-country FIUs. The lack of FIU harmonization across the EU has also caused significant data protection difficulties.

This paper aims to provide a comprehensive analysis of the currently persistent application problems in the field of information exchange between EU FIUs and between EU and third-country FIUs. To pursue this objective, this paper also includes an analysis of the adequacy of the personal data protection regulation at the EU level and the related issue of using communication channels to exchange information between FIUs. These analyses form the theoretical basis for formulating conclusions regarding the inadequacy of the existing legislation in the field of ensuring international cooperation between FIUs. The following methods were used in the paper: induction, deduction, analysis, synthesis, abstraction, and comparison.

2 Exchange of information between EU FIUs

Under Article 53 of the AML IV Directive, EU FIUs are obliged to carry out information-sharing. In this context, we can speak of international cooperation between EU FIUs, which is carried out on a reciprocal basis, i.e. each EU FIU acts both as a recipient of the information and as a provider of information. With regard to this task, EU FIUs act as clearing houses (Panevski et al., 2021, 244), their main task being to ensure the receipt and independent analysis of information relevant to the area of money laundering and terrorist financing. As such, we can think of them as serving the "intermediary" role between law enforcement and judicial authorities.

It is important to emphasize that Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 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 Directives 2009/138/EC and 2013/36/EU ("AML V Directive") directly distinguishes between competent authorities supervising credit and financial institutions in the area of money laundering and financing of terrorism and supervisors conducting prudential supervision. For example, in the Slovak Republic, the competence of the National Bank of Slovakia to carry out supervision in the field of money laundering and financing of terrorism is thus derived from its power to prudentially regulate and supervise financial market participants (European Banking Authority, 2021, 5).

[4] Online: https://bit.ly/3iP7hox

The provision of information by one EU FIU to an EU FIU from another EU Member State shall be carried out in one of the following ways (Mouzakiti, 2020, 359):

- At the initiative of the EU FIU;
- Expeditious transfer of information from an EU FIU to another EU FIU from another Member State;
- At the request of an FIU from another EU Member State.

Disclosure of information at the initiative of the EU FIU includes information and analysis that – at the EU FIU's own discretion – may be relevant for the purpose of processing or analysing information by an FIU from another EU Member State in relation to money laundering or terrorist financing.[5] It follows from the above that the information provided in this way must clearly be relevant and related to money laundering and terrorist financing. In this case, we see application problems related to the interpretation of the above concepts. While the concept of laundering the proceeds of crime and financing terrorism is further regulated in Article 1 of the AML IV Directive, the question of what is meant by relevance remains ambiguous. EU Member States' FIUs may thus interpret this criterion very differently and hence, at their discretion, not forward information that may have been relevant for another EU Member State. In this context, the European Commission has attempted to define this concept further, stressing that this form of disclosure is primarily used for reports containing a piece of cross-border information, but has still failed to explain the concept in greater detail. With the application of the relevance criterion, the European Commission considers that the analysis of the information received from the obliged entity should not be performed by the disclosing EU FIU but instead by the receiving EU FIU, which can then carry out its own analysis (European Commission, 2019a, 7–8). It is clear from the above that the information provided should contain data directly relevant to another EU Member State, which may be important for the proper functioning of the combating money laundering and terrorist financing framework.

The duty to provide information to an FIU from another EU Member State promptly is primarily linked to reporting any suspicious business transaction that has been submitted to a non-competent EU FIU. The duty to report a suspicious business transaction is generally imposed on obliged entities under the control of the relevant EU FIUs. These include banks, insurance companies, securities dealers, and the like.[6] In line with the territorial principle, the competent EU FIU shall be the FIU of the EU Member State in the territory of which the disclosing obliged entity is located.[7] The exchange of information is thus carried out on the basis of objective factors, consisting of determining that the suspicious business transaction report submitted by the obliged entity is addressed to another competent EU Member State. In this case, the disclosing EU FIU has no power to carry out any analysis or to decide on the justification of the report submitted (European Commission, 2019a, 7). The process of "forwarding" a suspicious transaction report (the STR) is linked to the existence of an application problem related to the duty of the EU FIU to provide feedback to the obliged entity and the disclosing EU FIU on the effectiveness of the submitted STR and the follow-up procedures related thereto.[8] Thus, the duty to provide feedback applies to the EU FIU that received the information from the non-competent EU FIU. Despite its existence, this duty is quite often underestimated by the

[5] Article 53 (1) of AML IV Directive.

[6] Article 2 of AML IV Directive.

[7] Article 33 (2) of AML IV Directive.

[8] Article 46 (3) of AML IV Directive.

relevant EU FIUs, which means that they provide less feedback to obliged entities. The situation is even worse when it comes to the communication between the disclosing EU FIU and the receiving EU FIU, where feedback is virtually non-existent (European Commission, 2019a, 6).

The provision of information at the request of an FIU from another EU Member State is – similarly to the provision of information at its own initiative – subject to its relevance to and connection with money laundering and terrorism financing. The request submitted must contain several pieces of information, such as background information, an adequate statement of reasons for the request, and the purpose for which the information requested will be used.[9] In this case, the question arises as to what constitutes a sufficient statement of reasons for the request? Will a suspicion of money laundering and terrorist financing be considered sufficient, or is it also necessary to produce an analysis of the reasons for such suspicion by the requesting EU FIU? The current regulation also does not address the issue of further action by the disclosing/requesting EU FIU if the statement of reasons is not sufficient on the part of the requesting EU FIU. These are issues that are still topical and have not yet received sufficient attention, which may ultimately be counterproductive and thus discourage EU FIUs from cooperating at the international level.

Another application issue relates to the duty to provide a timely response to a request for information by an FIU from another EU Member State. The AML IV Directive does not specify the maximum length of time for responding to a request for information from another EU FIU, thus it is at the sole discretion of the disclosing EU FIU. In our view, this has served as an impetus for the EU FIU to follow the recommendations of the Egmont Group of FIUs,[10] which recommends that the EU FIU respond to the request within one month (Egmont Group, 2014, 5). In order to ensure a timely exchange of information, the Egmont Group of FIUs has also created a request form containing a number of mandatory details to be provided by the requesting FIU (e.g. name of the FIU, urgency of the request, identification of the relevant entity for the disclosure of information) (Egmont Group, 2017, Annex A).

Despite the absence of a regulation on the maximum time limit for responding to a request from another EU FIU in the AML IV Directive, the European Commission has criticized EU FIUs, stressing that, despite the approval by the Egmont Group of FIUs of the recommendation by the EU FIUs, the given time limit appears to be much longer than the average time limits for exchanging information with other EU authorities, which are calculated in days or up to a maximum of one week. An example is Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, which provides for a time limit of up to three days (European Commission, 2019a, 8). In this context, it is impossible to disagree with the European Commission, that the one-month time limit set is disproportionately long, especially when an urgent request is served by the EU FIU, which may further delay subsequent legal actions taken by it. On the other hand, we also see possible misconduct by the competent EU authorities, which – by their inaction – gave the EU FIU a free hand to decide how long they shall take to respond.

Another application problem lies in the area of ensuring timely access to the requested information by the receiving EU FIU. Under Section 32 (4) of the AML IV Directive, Member

[9] Article 53 (1) of AML IV Directive.

[10] The Egmont Group of Financial Intelligence Units is an international organisation whose aim is to facilitate cooperation and intelligence sharing between FIUs in order to investigate and prevent money laundering and terrorist financing. The Egmont Group was founded in 1995 as an informal network of 24 national FIUs.

States shall ensure that their FIUs have timely access – direct or indirect – to the financial, administrative, and law enforcement information that they require to perform their duties and powers accordingly. Nevertheless, it is clear that, in practice, not all EU FIUs are able to access the data they need. In our view, the fundamental problem is the inconsistent regulation of the organizational status of the EU FIUs. Despite the fact that the AML IV Directive removed the original obstacle, of imposing a duty on the EU Member States to ensure mutual cooperation between EU FIUs irrespective of their organizational status,[11] the unification of the EU FIUs' direct access to all the information they need has not been enforced. As a result, we currently see significant differences between the EU Member States in the ability of EU FIUs to secure direct access to the data they require. For instance, EU FIUs may have limited access to certain databases due to the different organizational positions of EU FIUs (e.g., if organizational position of an EU FIU within the hierarchy of its state institutions (such as law enforcement authorities) is too low, it may not be granted unrestricted access to all relevant databases).

The exchange of information must respect the principle of purpose limitation. EU FIUs may use the information obtained only for the purposes specified in the request for information or the purposes specified by the disclosing EU FIU. When exchanging information and documents, the disclosing EU FIU may specify the conditions and limitations under which the receiving EU FIU may use the information.[12] In this case, the question arises as to what else may be subject to such a restriction. As of now, no uniform standards for information exchange exist at the EU level. In this case, the only recourse seems to be to ask the disclosing FIU for consent to use the information for other purposes as well.

3 Use of FIU.net/ESW, and personal data protection

The European Commission places emphasis on ensuring enhanced protection of data provided to another EU FIU. Data is protected at two levels: the method of data transmission (IT system) and the legal framework for ensuring the protection of personal data.

In order to protect personal data, EU FIUs are obliged to use secure communication channels. In this context, the AML IV Directive encourages FIUs to use FIU.net. This is a decentralized network used for exchanging information between EU FIUs. The decentralization of the network means that there is no common database where all the required data are stored, but all the participating EU FIUs have their own database of data that must be connected to FIU.net. This structure ensures that individual EU FIUs have control over their data as well as a certain level of flexibility in terms of data management (Mouzakiti, 2020, 359). The exchange of information is thus carried out on the basis of a request from the EU FIU for specific information. Requests for information may relate to specific suspicious entities as well as to more specific areas of activity by entities. Using the Ma3tch technology, EU FIUs can gain an overview of entities of interest in the other EU Member States and identify their revenues and funds. Using filters (FIU.net currently has about 126 filters); EU FIUs can compare data without requesting any personal data disclosure. If there is a positive hit, an EU FIU may then request the relevant EU FIUs to provide specific personal data of the individuals making a suspicious transaction. In this case, the FIU.net system guides EU FIUs to exchange only those data that are absolutely necessary for them, thus respecting the principle of data protection (Balboni & Macenaite, 2013, 334).

[11] Article 52 of AML IV Directive.

[12] Article 54 of AML Directive.

Although FIU.net creates a unified system for the exchange of information between EU FIUs, we also find a number of application problems. The first problem is one of optionality, i.e. the right of EU FIUs to join the FIU.net system. The AML IV Directive does not explicitly require every EU FIU to participate in FIU.net, but only asks the EU Member States to encourage their FIUs to use the system. It follows that it is up to each FIU to decide whether to use the FIU.net system or to choose a completely different approach. In this context, some EU FIUs – citing the complexity and opacity of the FIU.net system – currently continue to use the Egmont Secure Web (ESW). This was developed by the Egmont Group of FIUs and, like FIU.net, is intended to ensure a seamless exchange of information between FIUs. From this perspective, EU FIUs are divided into three types: the first group uses only FIU.net; the second uses ESW as an equivalent alternative to FIU.net; and the third group uses FIU.net as a primary tool, while ESW is used only if the primary system fails or is interrupted (European Commission, 2019a, 10). This inconsistency in the use of information exchange systems between EU FIUs may have a significant impact on the speed of information provided due to compatibility issues between the systems used by EU FIUs.

However, the fundamental question remains the appropriateness of choosing FIU.net as the sole system for information exchange between EU FIUs. It is clear that FIU.net, which was developed by the EU, is a more powerful tool for EU FIUs, especially when it comes to potential network technical issues (e.g. data leakage). On the other hand, we still consider the questionable institutional subordination of FIU.net to be the hindrance here. Since 2016, FIU.net has been integrated under Europol, which has created further opportunities for information sharing between EU FIUs and Europol but, already in 2019, the question was raised of whether Europol' was adequately competent for cooperation in the area of personal data processing in order to perform the role of FIU.net technical administrator. The content of the European Data Protection Supervisor's annual report showed that FIU.net contains personal data that goes beyond the list of data that can be processed by Europol (EDPS, 2019). In fact, Europol processes personal data only for the purpose of crisis control of a person suspected of committing or participating in a criminal offense,[13] whereas EU FIUs have a wider range of competencies and focus, among other things, on suspicious commercial operations in a financial-legal context. On the basis of the decision above, the European Parliament has proposed a temporary transfer of the competencies of the FIU.net administrator to the European Commission and to extend those of Europol to include the possibility of establishing cooperation with the EU FIUs (European Parliament, 2021).

It follows from the above that it is clear that the question of the suitability of the use of FIU.net is directly linked to the duty to ensure sufficient protection of personal data. We believe that the current application problem is the simultaneous application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR) and Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the

[13] Article 18 of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (the "Directive 2016/680"), in relation to EU Member States' FIU law-enforcement models. Under Recital 42 of the AML IV Directive, the GDPR applies to the processing of personal data for the purposes of preventing money laundering and terrorist financing, while Directive 2016/680 provides protection for personal data processed in the framework of police and judicial cooperation in criminal matters.[14] This raises the question of the suitability of applying the GDPR to the FIU police model, which has broader competencies toward law enforcement agencies.

Despite the fact that Art 41 of the AML IV Directive obliges all EU FIUs to apply the relevant provisions of the GDPR, some EU Member States continue to apply Directive 2016/680. The reason for taking a different approach is supposedly – in line with the arguments of EU Member States – to fulfil the core task of the EU FIU of detecting crime and the related use of law enforcement data, which ultimately results in EU FIUs effectively acting as law enforcement authorities (Mouzakiti, 2020, 365). Neither the European Commission nor the European Data Protection Supervisor disagreed with the reasoning put forward, pointing out that, despite performing similar tasks, EU FIUs may not be considered law enforcement or judicial authorities (EDPS, 2013). However, it remains debatable whether the competent EU authorities have sufficient competence to determine which data protection framework is appropriate for all FIUs in light of the range of existing FIU models chosen by the EU Member States.

Some EU Member States have gone even further and, instead of opting for one of the two data protection rules (GDPR and Directive 2016/680), they have applied dual (simultaneous) application of the two laws. However, the current application of the two regulations is associated with an application problem, consisting of the different levels of protection of personal data provided by the GDPR and Directive 2016/680. Examples include the prohibition of further processing of personal data regulated by the GDPR and the absence of a similar provision in Directive 2016/680, which regulates only the initial processing of personal data.[15]

Finally, it should be added that, when choosing a specific data protection legislation, or in the case of simultaneous application of two regulations, it remains questionable whether an EU FIU applying the GDPR – when it regards the exchange of information with an EU FIU applying Directive 2016/680 – can consider the protection of personal data provided at all as sufficient.

4 Exchange of information between EU and third country FIUs

While a significant part of the AML IV Directive further regulates the cooperation of EU FIUs, regulation of the area of cooperation with FIUs of third countries is completely absent. For this reason, EU FIUs exchange information according to the Egmont Group of FIUs' Charter (Egmont Group, 2018) or implement bilateral agreements or even Memoranda of Understanding.

[14] Recital 42 modifies the references to the ineffective Regulation and Directive, which have been replaced by the GDPR and Directive 2016/680. Under Article 94 of GDPR: "1. Directive 95/46/EC is repealed with effect from 25 May 2018. 2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation".

[15] Compare Article 5 of GDPR with Article 4 of Directive 2016/680.

The exchange of information between EU FIUs and third-country FIUs is thus carried out on a reciprocal basis. It follows that the scope of information provided to third country FIUs may vary, depending on both the type of information requested and on how the protection of personal data is ensured.

The lack of uniform regulation across the EU causes significant problems in how EU FIUs exchange information in accordance with the relevant EU legislation in force. We see application problems at two levels: the power of the EU FIU to conclude bilateral agreements and Memoranda of Understanding and ensuring the protection of personal data.

The European Commission has stressed that cooperation with FIUs of third countries falls under the exclusive external competence of the EU. It added that the current way of ensuring cooperation between EU and third-country FIUs is a manifestation of the arbitrariness of EU Member States acting without the involvement of EU bodies (European Commission, 2019a, 10). In our view, this is an absurd claim, which has no legal basis. At present, no relevant EU legislation further regulates even the principles of exchange of information between EU FIUs and third-country FIUs, let alone the procedural and legal process for ensuring cooperation (e.g. designation of the network for communication, FIU responsibilities, etc.). In this respect, it also seems inappropriate to argue that international agreements and Memoranda of Understanding could only be compatible with the EU's exclusive competence if they covered operational issues exclusively. However, the question arises as to how cooperation in other "non-operational" areas is to be enforced. This problem needs to be seen at a global level; it is not only a problem of the EU FIU providing information to a third country FIU but also the opposite problem, of not being able to obtain the necessary information requested by the EU FIU from third-country FIUs. If we are talking about the fact that money laundering and terrorist financing have no borders and the perpetrators may be located in third countries, it is obvious that EU FIUs will also suffer from a lack of necessary information, which may ultimately contribute to the transfer of perpetrators' illegal activities to third countries.

In the area of personal data protection, similar to the cooperation between EU FIUs, application problems remain due to inconsistent application of the GDPR and Directive 2016/680. EU FIUs, depending on their model, use the appropriate data protection safeguards for them when cooperating with third-country FIUs. The GDPR and Directive 2016/680 both regulate the principles for personal data transfers to third countries, but they differ. The GDPR presents stricter data protection regulations, since Directive 2016/680 does not cover specific areas of data protection. For instance, compared to the GDPR, Directive 2016/680 does not contain provisions on binding corporate rules, nor on data transfers and disclosures that are not allowed by Union law.[16]

The lack of an adequate level of data protection based on suspicious business transactions the GDPR and Directive 2016/680 by third-country FIUs also remains an issue. Not every third country FIU necessarily has a similar data protection regulation in place and thus may be subject to completely different requirements and conditions for ensuring the protection of personal data.[17] The problem has also been highlighted by the European Commission, which has identified a number of issues related to the reluctance of FIUs to exchange information with each other, mainly due to the lack of mutual trust and the fear that such transfers of personal data will not comply with the GDPR (European Commission, 2019b, 16).

[16] Compare Article 47 and Article 48 of GDPR.

[17] For more details see: Adetunji (2019).

Finally, EU FIUs are forced to comply with their international obligations and global standards in the fight against money laundering and terrorist financing, which stem, among other things, from the AML IV Directive as well as the FATF Recommendations and Egmont Group of FIU Recommendations. However, in this case, it is essential that EU FIUs comply with the relevant EU legislation when exchanging information with third-country FIUs.

5 Conclusion

FIUs are key players in the current fight against money laundering and terrorist financing. They are the only centres for collecting information on suspicious transactions and activity, making them an intermediate link between financial institutions and law enforcement authorities. Given that criminals laundering the proceeds of crime are not constrained by EU borders, it is of the utmost importance to ensure that international cooperation between FIUs functions properly. However, the current legal situation raises a number of issues related to the inadequacy of the legislation and the need for supplementation. Application problems are experienced at all levels of information exchange between FIUs. We consider the biggest problem to be the absence of legal definitions of basic terms and the regulation of the maximum length of time for responding to a request for information from an EU FIU, without which, in our opinion, it is not possible to talk about the overall effectiveness of the exchange of information between EU FIUs. In this context, it is necessary to add the mission definitions of terms, as well as to set the maximum response time to a request from an EU FIU to the AML IV Directive.

The inconsistency of the legislator can also be seen in the communication channels (FIU.net and ESW), the choice of which is left to the individual EU FIUs, which may cause significant problems in the area of data transfer, making it difficult to establish comprehensive international cooperation between EU FIUs. Furthermore, due to the existence of multiple EU FIU models, data exchange between EU FIUs has reached an "impasse", in that there is currently still a lack of consistency between the EU Member States in the application of the GDPR and Directive 2016/680. In our view, despite the existing direct obligation to apply the GDPR to all EU FIUs (also stemming from the AML IV Directive), it is not possible for EU Member States to arbitrarily decide, depending on the type of EU FIU model they use, which legislation they are "willing" to apply. It follows that we can also speak of an incorrect application of the provisions of the AML IV Directive.

The biggest grey area is currently that of cooperation between EU and third-country FIUs. The need to ensure this kind of cooperation is indisputable and cannot be left to the discretion of individual EU Member States. It is therefore questionable why there is not yet a uniform regulation of the basic processes of information exchange between EU and third-country FIUs. In an attempt to eliminate the grey area, EU Member States have attempted to establish cooperation with third-country FIUs by concluding cooperation agreements or Memoranda of Understanding, but this has not been accepted by the European Commission. In this case, we consider it particularly relevant to reflect on the future functioning of these relationships. As a result of the grey area, we believe that, by entering into special agreements and Memoranda of Understanding, the actions of EU FIUs are correct and beneficial for the further development of international cooperation in the field of information exchange.

References

Adetunji, J. A. (2019). Rethinking the Internal Mechanism of the EGMONT Group in Financial Crime Control. *Journal of Money Laundering Control*, 22(2), 327–338. https://doi.org/10.1108/JMLC-04-2018-0029

Balboni, P., & Macenaite, M. (2013). Privacy by Design and Anonymization Techniques in Action: Case Study of Ma3tch Technology. *Computer Law and Security Review*, 29(4), 330–340. https://doi.org/10.1016/j.clsr.2013.05.005

Brewczyńska, M. (2021). Financial Intelligence Units: Reflections on the Applicable Data Protection Legal Framework. *Computer Law & Security Review*, 43. https://doi.org/10.1016/j.clsr.2021.105612

Dražková, M. (2021). *Opatření v dohledu nad kapitálovým trhem.* C. H. Beck.

Egmont Group of Financial Intelligence Units. (2014). *Operational Guidance for FIU Activities and the Exchange of Information. Approved by the Egmont Group Heads of Financial Intelligence Units, July 2013, revised June 2014.* Online: https://bit.ly/3hbejmX

Egmont Group of Financial Intelligence Units. (2017). *Operational Guidance for FIU Activities and the Exchange of Information. Approved by the Egmont Group Heads of Financial Intelligence Units, July 2013, revised February 2017.* Online: https://bit.ly/3uDDKRk

Egmont Group of Financial Intelligence Units. (2018). *Egmont Group of Financial Intelligence Units Charter. Approved by the Egmont Group Heads of Financial Intelligence Units. Australia: Sydney, July 2013, revised in September 2018.* Online: https://bit.ly/3uzQk3Y

European Banking Authority. (2021, December 16). *Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU* (EBA/GL/2021/15). Online: https://bit.ly/3BnAcq8

European Commission. (2019a). Report from the Commission to the European Parliament and the Council assessing the framework for cooperation between Financial Intelligence Units (COM/2019/371 final).

European Commission. (2019b). Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions (COM/2019/373 final).

European Data Protection Supervisor. (2013, July 4). *Opinion on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds.* Online: https://bit.ly/3VL8Zpy

European Data Protection Supervisor. (2019). *Annual report 2019. Publication Office of the European Union.* Online: https://bit.ly/3W36Bdp

European Parliament. (2021, August 2). *Answer given by Ms Johansson on behalf of the European Commission. Parliamentary question – E-005327/20208(ASW).* Online: https://bit.ly/3uE9sxW

FATF. (2012-2022). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.* Online: https://www.fatf-gafi.org/recommendations.html

International Monetary Fund. (2004). *Financial Intelligence Units: An Overview.* https://doi.org/10.5089/9781589063495.069

Mouzakiti, F. (2020). Cooperation Between Financial Intelligence Units in the European Union: Stuck in the Middle Between the General Data Protection Regulation and the Police Data Protection Directive. *New Journal of European Criminal Law*, 11(3), 351–374. https://doi.org/10.1177/2032284420943303

Nanyun, N. M., & Nasiri, A. (2021). Role of FATF on Financial Systems of Countries: Successes and Challenges. *Journal of Money Laundering Control*, 24(2), 234–245. https://doi.org/10.1108/JMLC-06-2020-0070

Panevski, D., Peráček, T., & Rentková, K. (2021). Analysis of the Practices of Financial Intelligence Units (FIUs) and Other Anti-money Laundering Agencies within EU. In N. Kryvinska, & A. Poniszewska-Marańda (Eds.), *Developments in Information & Knowledge Management for Business Applications. Studies in Systems, Decision and Control, vol. 376* (pp. 241–269). Springer, Cham. https://doi.org/10.1007/978-3-030-76632-0_8

Legal sources

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

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

Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 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 Directives 2009/138/EC and 2013/36/EU.

Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA).