Ius Novum
2/2019

BANKS' OBLIGATIONS RELATED TO PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE LIGHT OF AMENDED REGULATIONS

ANNA GOLONKA*

DOI: 10.26399/iusnovum.v13.2.2019.19/a.golonka

1. INTRODUCTION

On 13 July 2018, the Act of 1 March 2018 on preventing money laundering and terrorist financing (hereinafter APML)[1] entered into force. It repealed the former act under the same name, which was binding till 12 July 2018, and introduced new provisions. The repealed Act of 16 November 2000 was the first national regulation of a complex nature aimed at preventing the phenomenon of money laundering (originally, in accordance with its name, on preventing the introduction of financial assets originating from illegal or undisclosed sources to financial transactions)[2] and providing the core provisions regulating the issue. As a result of the amendment of 27 September 2002, it additionally covered preventing terrorist financing.[3] The Act of 1 March 2018 did not change anything within the regulation but laid down provisions concerning the prevention of the two above-mentioned phenomena. As

* PhD hab., UR Associate Professor, Criminal Law Department, Faculty of Law and Administration of the University of Rzeszów; e-mail: anna_golonka@o2.pl; ORCID: 0000-0002-0199-2203

1 Journal of Laws [Dz.U.] of 2018, item 723, as amended. The Minister of Development and Finance was the initiator of the Bill, which was filed on 5 May 2017 and given the number of 2233. The Sejm print No. 2233 is available at: http://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=2233 (accessed on 30/05/2018).

2 Originally: Act of 16 November 2000 on preventing the introduction of financial assets originating from illegal or undisclosed sources to financial transactions, Journal of Laws [Dz.U.] No. 116, item 1216.

3 Act of 27 September 2002 amending the Act on preventing the introduction of financial assets originating from illegal or undisclosed sources to financial transactions, Journal of Laws [Dz.U.] of 2002, No. 180, item 1500.

a result, fundamental questions are raised whether it was necessary to introduce the changes, about the main reason (*ratio legis*) for them and what obligations APML imposed on institutions.

Answering the first two of the above questions, having taken into consideration the legislative "tradition" of the successive amendments to the former Act of 16 November 2000, there are no doubts that in general the European Union norms were the only motives for the change of the status quo in this respect. Like all the other successive amendments to the "former" act, the "new" APML also resulted from the need to adjust the national regulation to the European requirements. Thus, the Act of 1 March 2018 constituted the implementation of 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 (referred to as 4th AML Directive), 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. However, it is worth mentioning that extensive work on legislative change is being carried out due to the successive, 5th AML Directive (see Procedure 2016/0208: COM (2016) 450: Proposal for a Directive of the European Parliament and of the Council, presented by the European Commission on 5 July 2016 and adopted by the Council on 14 May 2018) aimed, inter alia, at enhancing the process of exchanging information by financial analysis units, extending the regulation in the field of preventing risks of using modern technologies to commit the offence of money laundering or financing terrorism and taking into account the possibility of increased risks of involving representatives of legal professionals in active commission of such offences.[4]

On the other hand, in response to the question concerning the scope of changes introduced by APML, it is necessary to explicitly point out that the "new" statute introduces many far-reaching changes in the provisions laid down in the Act of 16 November 2000. Not only does it define obliged institutions but also imposes a series of new obligations on them, in particular those connected with the need to assess the risk of money laundering and terrorist financing as well as to use financial security measures. At the same time, this constitutes motivation to look at the regulations of 1 March 2018 and analyse them more thoroughly. However, coming to the point determined by the title of the article, it is worth focusing on those legal aspects that result from the imposition of new obligations connected with combating money laundering and terrorist financing on obliged institutions, especially banks, at least within the scope in which differences in comparison with the former regulations (i.e. the Act of 16 November 2000) are significant enough to discuss them below.

[4] The document is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15849_2017_INIT&from=PL (accessed on 19/07/2018).

2. BANKS AS ENTITIES OBLIGED TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

In the same way as in accordance with the Act of 16 November 2000, under APML banks are also classified as entities obliged to prevent the discussed activities. The issue of applying the regulations concerning the prevention of money laundering and terrorist financing to banks should not raise any doubts, at least from the historical point of view.

Banks were the first entities (potentially most vulnerable to negative consequences of money laundering) that introduced regulations dealing with the problem, e.g.:

– Ordinance No. 16/92 of the President of NBP (the National Bank of Poland) of 1 October 1992 (Dz.Urz. NBP No. 9, item 20), issued based on the statutory delegation under Article 100 paras. 5(2) and (3) of the Act of 31 January 1989: Banking Law,
– Ordinance No. C/2/I/94 of the President of NBP of 17 January 1994, which substituted for the above legal act, and
– Resolution No. 4/98 of the Commission for Banking Supervision of 30 June 1998, issued based on the statutory delegation under Article 106 para. 1 of the Act of 29 August 1997: Banking Law[5].

Thus, it is not surprising that banks are entities, as it is confirmed by the findings of the analysis of the Department of Financial Information, which prevent most diligently money laundering and terrorist financing. According to the Report of the General Inspector of Financial Information (GIIF) on the implementation of the Act of 16 November 2000 in 2017, the General Inspector received 3,272 notifications from the obliged entities (of the total of 4,115 notifications of suspicious activities and transactions, called SARs: Suspicious Activity Reports, which were included in the conducted analytical proceedings).[6] Like in the past years, most notifications came from banks/foreign bank branches, in fact 3,104 notifications in 2017, which constitutes 94.87% of the total number registered in the information system as those originating from obliged entities.[7]

In this context, one cannot be surprised that banks represent the financial services market that is most vulnerable to the potential use for the purpose of money laundering or terrorist financing, regardless of what their position is from the point of view of strategy or the role of their involvement in carrying out a given activity. Banks may indeed take a passive position (however, the assumption of their complete "exclusion" from participation in such an activity, at least from the practical point of view, as it is emphasised, is in general impossible in the present economic conditions). They may also take an active position and act as entities "involved in legitimisation of income from illegal activities unwittingly and in the way that is impossible to detect by those entities", which may result, inter alia, from non-adjustment to or

---

[5] Consolidated text, Journal of Laws [Dz.U.] of 2017, item 1876 as amended.

[6] GIIF's Report on the implementation of the Act of 16 November 2000 in 2017, Warsaw, March 2018, available at: https://www.mf.gov.pl/documents/764034/1223641/Sprawozdanie+2017 (accessed on 23/07/2018).

[7] *Ibid.*

non-compliance with obligations or procedures laid down in the binding provisions, and sometimes from their excessively "free" interpretation (e.g. in relation to the scope of transactions subject to obligatory registration, in particular, recognition that a transaction is the suspicious one).[8] Moreover, financial institutions may be wittingly involved in such activities, in particular, if they carry out legal and illegal transactions (e.g. credit institutions, which our legislator has taken into account at present by including also these institutions in the catalogue of obliged entities),[9] or banks may also found them exclusively in order to perform some of the discussed activities.[10] In the latter case, we deal with shadow banking, i.e. financial institutions that, unlike banks, are not subject to any restrictions resulting mainly from Banking Law such as financial supervision, capital obligations, organisational and legal limitations or deposit insurance requirements. Due to that, they are classified as non-banking financial companies. The above was decisive for emphasising the role of banks in the system of preventing money laundering and terrorist financing, and making them, in a way, "model" obliged institutions for the need of the present article.[11]

3. BANKS' OBLIGATIONS RESULTING FROM AMENDMENTS TO THE PROVISIONS ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

The amended Act on money laundering, following the example of the European Union regulation being implemented, i.e. the 4th AML Directive, is also mainly based on the assessment of risks of money laundering (risk-based approach – RBA). It should be interpreted as "a process serving the presentation of information on the nature and scale of money laundering/terrorist financing and basic offences connected with them as well as weaknesses in the AML/CFT system and other elements of the legal system that make it attractive for money launderers and

---

[8] Compare P. Chodnicka, *Zarządzanie ryzykiem prania pieniędzy w systemie bankowym*, Problemy Zarządzania Vol. 10, No. 4(39), 2012, pp. 206–207.

[9] In accordance with Article 2 para. 1(25) APML, making reference to the Act of 12 May 2011 on consumer loans (Journal of Laws [Dz.U.] of 2016, item 1528 and of 2017, item 819), the term "credit institution" should be interpreted as a lender other than: (a) a national or foreign bank, a foreign bank branch, a credit institution or a credit institution branch within the meaning of the Act of 29 August 1997: Banking Law; (b) a credit union and Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa (SKOK credit union); (c) an entity whose operations consist in providing consumer loans in the form of postponement of the payment of a price or remuneration for the purchase of goods and services it offers (Article 5(2a)).

[10] P. Chodnicka, *Zarządzanie ryzykiem…*, pp. 206–207.

[11] A bank is recognised as an obliged entity in accordance with Article 2 para. 1 APML. The catalogue of those entities laid down in Article 2 para. 1 APML is very abundant and includes entities such as, inter alia, investment funds, insurance firms, insurance intermediaries, legal profession representatives to certain extent (solicitors, legal advisors, notaries), entrepreneurs involved in currency exchange, entities providing accounting and book-keeping services, real estate agents, postal services operators, foundations, and entrepreneurs within the meaning of the Act of 2 July 2004 on the freedom of business operations within the scope of settlement of cash payment for goods worth or exceeding the worth of 10,000 euros, regardless of whether the transaction is a single operation or concerns a few operations that seem to be linked, etc.

terrorism backers".[12] Thus, the obligations laid down by the new provisions concerning obliged entities, *ad meritum,* consist in the need to take into consideration risk factors concerning customers, states or geographical areas, products, services, transactions or their delivery channels. More precisely, they include identification and assessment of risk connected with money laundering and terrorist financing as well as the use of financial security measures in case of establishing "business relationships" or carrying out "an occasional transaction" worth 15,000 euros or more, regardless of whether the transaction is conducted as a single operation or a few operations that seem to be linked with each other (in case of cash transactions worth 10,000 euros or more), and in case of money transfer when the value of an occasional transaction exceeds 1,000 euros (Article 35 APML). Due to the above, the statute discussed laid down legal definitions of the formerly unknown concepts as "business relationships" or "occasional transaction".

The term of business relationship means "the relationship between an obliged entity and a client that is connected with the professional activities of the obliged entity, which have an element of duration at the time when the contract is established" (Article 2 para. 1(20) APML). On the other hand, an occasional transaction is any transaction outside of a business relationship (Article 2 para. 1(22) APML**).** It should be added that within the meaning of APML, a transaction should be interpreted as "a legal or actual activity based on which property or financial assets are transferred or a legal or actual activity carried out in order to transfer property or possess financial assets" (Article 2 para. 1(21) APML).

However, attention is drawn to the fact that only those transactions that have an element of duration "at the time when" they are carried out (or more precisely "when the contract is established") should be recognised as "business relationships", which is not only imprecise but can cause real problems with the assessment when a given entity is involved in a business relationship. As the feature of "duration" may and should include the scope of activities undertaken so far, thus, the issue of a business relationship duration should be concluded from the entire activities carried out for a client by a given obliged entity or possibly, which seems to be less adequate, a certain "forecast" of a business relationship duration should be made based on a transaction carried out in a given period (not at the time). In other words, in the latter case, it is assumed that based on the nature of a transaction, it is possible to draw a conclusion that it leads to entering into durable business relationships with a client (e.g. opening of an account). The sense of "the time" absolutely does not constitute an indicator of duration that is essential for distinguishing between a "business relationship" and "occasional transaction". However, there should be no doubts that the assessment of the risk of money laundering or terrorist financing looks different in a situation when a transaction is carried out by a bank in accordance with the relationship established with a client and it would look different if it concerned an "occasional transaction" commissioned by an entity unknown to the given institution.

---

[12] 4th AML Directive – 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, OJ L 141, 5.6.2015, pp. 73–117.

What is interesting, in the light of the provisions of APML, apart from "typical" relationships with a client, there is an additional category called correspondent relationships. As far as this is concerned, the obligation to introduce appropriate regulations also results from the implementation of the 4th AML Directive. In accordance with Article 2 para. 2(18) of the Act of 1 March 2018, the relationships should include:

a) correspondent banking performed by a service-providing bank on behalf of a user bank,
b) relationship between credit institutions and financial institutions, including relationships within which similar services are offered by a service-providing institution on behalf of a user institution, and relationships established for the needs of transactions concerning securities or for the needs of transferring funds.

A correspondent bank is a credit institution providing payment and other services on behalf of another credit institution. Payments are made with the use of mutual accounts (called *nostro* and *loro* accounts), which can be linked with permanent lines of credit.[13] A bank, in order to settle payments within international transactions with another bank, must possess its own account in another foreign bank for holding currencies (the best one is that to be used for the settlement). A bank's (its own) account opened in a foreign bank is called a *nostro* account. On the other hand, following the rule of a "mirror image", a *loro* account (their account) is a foreign bank's account for a bank in which it is opened.[14]

Including crypto currencies within the scope of the regulation is another novelty, which is laid down in APML and is extraordinarily significant from the practical point of view.[15] As it was rightly emphasised, the development of crypto currencies, including the best known bitcoin (BTC), as a relatively new phenomenon without our full knowledge of its possibilities or threats to the economic transactions connected with its use, needs continuous monitoring and analysing as a criminogenic risk factor.[16] Due to that, many organisations and financial analysis units comparable to the GIIF in other countries (not only the EU member states) and international organisations founded to prevent money laundering and terrorist financing are now involved in a series of activities aimed at full recognition of threats posed by the development of crypto currencies.[17] Such currencies "are based on a complex system

---

[13] Compare: Guidelines of the European Central Bank of 20 September 2011, 2011/817/EU on monetary policy instruments and procedures of the Eurosystem (ECB/2011/14); available at: http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32011O0014 (accessed on 30/04/2018).

[14] Compare T.T. Kaczmarek, J. Królak-Werwińska, *Handel międzynarodowy. Zarządzanie ryzykiem. Rozliczenia finansowe*, Wolters Kluwer, Warsaw 2008, p. 115.

[15] Also compare *Komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego w sprawie "walut" wirtualnych of 7 July 2018*, available at: http://www.nbp.pl/home.aspx?f=/aktualnosci/wiadomosci_2017/ww-pl.html (accessed on 12/07/2018).

[16] Compare a document of 28 May 2015: Undersecretary of State in the Ministry of Finance [FN7.054.9.2015], *Regulacje dotyczące wirtualnej waluty bitcoin*. The document presents the explanation of the Ministry of Finance concerning the functioning of crypto currencies, Monitor Prawa Bankowego No. 6, 2016, pp. 13–17.

[17] Compare the GIIF's report on hazards connected with crypto currencies, available at: http://www.mf.gov.pl/ministerstwo-finansow/dzialalnosc/giif/komunikaty/-/asset_publisher/8KnM/

of cryptographic protocols. The creation of bitcoin consists in generating a code (a cipher) with the use of the so-called excavator, which is a particular programme and computer hardware with big calculation power in the peer-to-peer network".[18]

On the other hand, in accordance with APML, the crypto currency should be interpreted as "digital reflection of value that is not:

a) the legal tender issued by NBP, foreign banks or other public administration bodies,
b) an international unit of settlement established by an international organisation and recognised by its member states or countries cooperating with it,
c) electronic money in the meaning of the Act of 19 August 2011 on financial services,
d) a financial instrument in the meaning of the Act 29 July 2005 on financial instruments turnover,
e) a bill of exchange or a cheque,

– and is subject to exchange in economic transactions into legal tenders or recognised as a means of exchange, and may be retained or transferred electronically or may be an object of sales conducted electronically" (Article 2 para. 2(26) APML). In addition, Article 2 para. 2(27) APML lays down that financial assets in the meaning of APML include not only, as so far, property rights or other movable or immovable property, legal tenders, financial instruments in the meaning of the Act of 29 July 2005 on financial instruments turnover, other securities and foreign currencies but, at present, also crypto currencies. It seems that crypto currencies, *de lege lata*, are of secondary importance for banks. However, if we take into consideration the development of the financial services sector and, first of all, the mutual "penetration" of the risk areas (profits generated from transactions in "dirty" financial assets originating in bitcoin transactions may be legitimised with the use of banking services after a transaction with its use),[19] it is not possible to omit the issue in this article. It is also worth mentioning that in the light of the Bill on the Central Database of Accounts, which is envisaged in the 4th AML Directive and, as a result, also by the Polish legislator, there is also a definition of crypto currency laid down.[20] In accordance with Article 2(6)

---

content/komunikat-generalnego-inspektora-informacji-finansowej-w-sprawie-niebezpieczenstw-zwiazanych-z-walutami-wirtualnymi?redirect=http%3A%2F%2Fwww.mf.gov.pl%2Fministerstwo-finansow%2Fdzialalnosc%2Fgiif%2Fkomunikaty%3Fp_p_id%3D101_INSTANCE_8KnM%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-2%26p_p_col_count%3D1%26_101_INSTANCE_8KnM_advancedSearch%3Dfalse%26_101_INSTANCE_8KnM_keywords%3D%26_101_INSTANCE_8KnM_delta%3D5%26_101_INSTANCE_8KnM_cur%3D1%26_101_INSTANCE_8KnM_andOperator%3Dtrue%23p_p_id_101_INSTANCE_8KnM_ (accessed on 1/01/2018).

[18] J. Dąbrowska, *Charakter prawny bitcoin*, Studia i Artykuły, Człowiek w Cyberprzestrzeni No. 1, 2017, p. 55.

[19] This concerns the system with two-directional monetary flow in which a crypto currency may be exchanged into other currencies without reservations, as exemplified by bitcoin, which is convertible in online money exchange firms and on the stock exchange – compare P. Mackiewicz, M. Musiał, *Rozwój wirtualnych systemów monetarnych*, Nauki o Finansach (Financial Sciences) No. 1(18), 2014, pp. 136–139.

[20] For more on the issue, see J. Czarnecki, *Wirtualne waluty w projekcie ustawy o Centralnej Bazie Rachunków*, Biuletyn Nowych Technologii No. 2, 2017. The Article is available at: http://www.wardynski.com.pl/biuletyn_nowych_technologii/2017-02/Wirtualne_waluty_w_projekcie_ustawy_o_CBR.pdf (accessed on 10/07/2018).

Bill on the Central Database of Accounts (Centralna Baza Rachunków, CBR) dated 22 December 2016, a "crypto currency" means "a transferable property right which represents value in a digital form, has its equivalent in a legal tender, is treated as a means of exchange and a unit of settlement, has no status of a legal tender and is not electronic money within the meaning of the Act of 19 August 2011 on financial services, which may be transferred, retained or sold as legal tenders electronically".[21]

Although the Act on CBR has not entered into force yet, banks (in the same way as SKOK credit unions) introduced their own Central Information on Accounts, i.e. Centralna Informacja o Rachunkach (CIR).[22] This makes it possible to obtain access to information on accounts in every bank and SKOK. Before the introduction of CIR, a query about an account looked for had to be addressed to every bank and SKOK credit union separately. Thanks to CIR, it is possible to obtain information in one place, i.e. in the office where a client files a request. At present, thanks to CIR, an account owner who is a natural person and a member of SKOK, has an opportunity to, inter alia, get access to his own accounts and find a deceased person's (testator's) account. CIR also makes it possible to fulfil the obligations resulting from APML, in particular those relating to the necessity of constant monitoring of economic transactions, especially as banks and SKOK credit unions are obliged to use this database.[23] On the other hand, the Central Register of Beneficial Owners (Centralny Rejestr Beneficjentów Rzeczywistych, CRBR) is a novelty introduced by APML. The CRBR is an IT communications system used to process information about beneficial owners of companies referred to in Article 58 APML.[24]

Due to APML's *ratio legis* as well as the issues raised here, it seems that the amendments to provisions preventing money laundering are the most important as they result in obligations to "assess risk" imposed on banks as obliged entities. Thus, it is worth devoting more attention to those regulations.

The basic obligation concerning this issue that was imposed on all obliged entities results from Article 27 para. 1 APML and includes identification and assessment of risk connected with money laundering and terrorist financing involving a given institution;[25] however, in accordance with Article 27 para. 2, when assessing risk,

---

[21] The Bill is available on the website of Rządowe Centrum Legislacji: https://legislacja.rcl.gov.pl/projekt/12293403/katalog/12400913.

[22] CIR is available at: https://www.centralnainformacja.pl/ (accessed on 1/05/2018).

[23] *Ibid*.

[24] In accordance with Article 55 APML, entities that are subject to the obligation to report information on beneficial owners include general partnerships, limited partnerships, limited stock companies, limited liability companies and joint-stock companies with the exception of public companies in the meaning of the Act of 29 July 2005 on public offer and conditions for the introduction of financial instruments to the organised system of transactions and on public companies (Journal of Laws [Dz.U.] of 2016, item 1639 and of 2017 items 452, 724, 791 and 1089). It is worth indicating that in accordance with the legal definition (Article 2 para. 2(1) APML), a natural person who has not been recognised as one that is subject to control by another entity shall be, at the same time, assumed to be a beneficial owner.

[25] In accordance with Article 27 para. 1 APML, obliged entities shall identify and assess risk connected with money laundering and terrorist financing in relation to their operations "with consideration of risk factors concerning their clients, states or geographical areas, products, services, transactions or their delivery channels", and the activities should be "proportionate to the nature and size of the obliged entity".

obliged entities may (sic!) take into account the binding national risk assessment as well as the European Commission report referred to in Article 6 paras. 1–3 Directive 2015/849 (Article 27 para. 2). An obliged entity must develop its own risk assessment as a paper and electronic document and update it "if necessary", at least every second year, in particular in connection with the change in risk factors concerning clients, countries or geographical regions, products, services, transactions or channels of their delivery (Article 27 para. 3 APML).

Such wording makes one raise a few fundamental questions: What does "risk" mean? What criteria should be used to determine risk factors (taking into account that an obliged entity's activities aimed at preventing discussed processes should be "proportionate to the nature and size of the obliged entity")? And finally, what does "the national risk assessment" mean and why is it not significant enough to require that the obliged entity must base on it when developing its own document? The last issue raises another doubt connected with the criteria for the assessment of the risk level that should be taken into account and which of them, in case the national risk assessment is not taken into account, may be deemed to be typical "alternative" criteria on which an obliged entity should base its assessment of money laundering or terrorist financing risk.

In accordance with the EU regulations, one can assume that the concept of "risk" refers to the likelihood of money laundering or terrorist financing occurrence, or its potential consequences. "Risk" interpreted this way refers to inherent risk, i.e. one existing before its mitigation, and does not refer to residual risk, i.e. one that exists after its mitigation or elimination. On the other hand, "risk factors" should be recognised as variables that on their own or in combination with others may increase or decrease the risk of money laundering or terrorist financing and result from a given business relationship or an occasional transaction. Finally, we can speak about the "risk-based approach" when "competent authorities and firms identify, assess and understand the ML/TF risk to which firms are exposed and take AML/CFT measures that are proportionate to those risks".[26]

We can speak about such an approach in the context of the obligation imposed on obliged entities in accordance with Article 27 APML (identification and assessment of risk connected with money laundering and terrorist financing). Based on that provision, obliged entities should also consider such (generally determined) criminogenic factors as those concerning customers (behavioural factors), the country (of a customer and a beneficial owner[27] – geographical factors), including "delivery channels" as well as

[26] For definitions, compare Joint Guidelines of 4 January 2018 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (JC 2017 37), available at: https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_PL_04-01-2018.pdf (accessed on 25/07/2018).

[27] In accordance with Article 2 para. 2(1) APML, a beneficial owner is (in general) a natural person or natural persons having direct or indirect control over a client through the rights resulting from legal or factual circumstances making it possible to exert decisive influence on activities or actions undertaken by the client or natural person or natural persons on whose behalf business relationships are established or an occasional transaction is carried out.

products and services (economic factors).[28] Assessing risk, obliged entities may base on the national risk assessment (NRA). The Act of 1 March 2018 devotes Chapter 4 to such assessment. It does not determine, however, what this assessment is. One cannot find there a definition of NRA or detailed criteria for the assessment of the level of risk. It seems that there can be no mention of them *in abstracto*.[29] In the "new" Act on preventing money laundering and terrorist financing, however, one can find information on what the document is to contain, namely:

1) a description of the methodology of the national risk assessment;
2) a description of the phenomena connected with money laundering and terrorist financing;
3) a description of the binding regulations concerning money laundering and terrorist financing;
4) an indication of the level of risk of money laundering and terrorist financing in the Republic of Poland with its justification;
5) conclusions drawn from the assessment of money laundering and terrorist financing risk;
6) identification of the issues concerning the protection of personal data connected with the prevention of money laundering and terrorist financing.

Apart from recommendations concerning the document structure, the GIIF (as a body responsible for the development of NRA "in cooperation with the Committee, cooperating units and obliged entities" – Article 25 para. 1 APML) is obliged to consider the European Commission report.[30] It identifies, assesses and estimates the risk of money laundering and terrorist financing at the Union level and covers at least the issues concerning: areas of internal market that are recognised as the most exposed to the threat of being used in those processes, a risk connected with every sector concerned and most common methods used by criminals to launder money from illegal profits. It seems that one can interpret those indications as certain regular threats or tendencies on which, with regard to various industries or in more general terms to the type of business activity or the nature of provided services, obliged entities may base when developing their own matrices of assessment of the risk of committing the offence referred to in Article 299 or Article 165a of the Criminal Code (henceforth CC).[31] They contain a certain "model

---

[28] In accordance with Article 33 para. 3 APML, obliged entities shall document a recognised risk of money laundering or terrorist financing associated with business relationships or an occasional transaction and its assessment considering in particular factors concerning: the type of client, geographical area, account appropriation, type of products, services and methods of their distribution, value level of financial assets deposited by a client or the value of transactions carried out as well as the aim, regularity and period of business relationship existence.

[29] For other than those generally specified factors the consideration of which is required when obliged entities assess risk, compare in particular Article 27 and Article 33 para. 3 APML.

[30] Report from the Commission to the European Parliament and the Council, Brussels, 26.6.2017, COM 92017, 340 final available at: http://ec.europa.eu/transparency/regdoc/rep/1/2017/PL/COM-2017-340-F1-PL-MAIN-PART-1.PDF (accessed on 12/07/2018).

[31] An example of a standard client assessment (matrix) developed for investment funds, available at: https://www.izfa.pl/download/file/id/15/n/standard-oceny-klientow-funduszy-inwestycyjnych-w-celu-okreslenia-poziomu-ryzyka-zwiazanego-z-praniem-pieniedzy-oraz-finansowaniem-terroryzmu (accessed on 25/07/2018).

pattern" of identifying main types of internal risk with its division into sectors of provided services, specification of threats existing in particular sectors (horizontal exposure) and indication of financial security measures adjusted to those threats.[32]

On the other hand, discussing the issue of factors that should be considered in the context of the provisions laid down in APML in a relatively general way, theoretically, one should make use of such documents as Joint Guidelines developed based on Articles 17 and 18(4) of Directive (EU) 2015/849, of 4 January 2018, on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions.[33] However, the risk management introduced based on it will not, in fact, meet the expectations resulting from the new provisions' entry into force. It is due to the fact that, on the one hand, Joint Guidelines in a very detailed way list recommendations for each of the three (main) groups of factors that, according to that document, may be conducive to participation in the performance of one of the discussed processes,[34] and on the other hand, some statements in this document are quite often imprecise and not clearly determined, not to say that they may sometimes lead to irrational results of the risk assessment. An example that can be presented here is the factor of the level of risk concerning a customer's "reputation" and an indication that it should be also considered whether there are any "adverse media reports or other relevant sources of information about the customer, for example (…) any allegations of criminality or terrorism against the customer or the beneficial owner". It is worth mentioning here that in accordance with Joint Guidelines, "other relevant sources" should include, inter alia, "the firm's own knowledge" (however, it is not clear whether it refers to what an employee or the institution knows and what constitutes this extremely arbitrary source of information), professional expertise, including e.g. the tenure in the financial services market, information from industry bodies such as typologies and information on emerging risks and, what is interesting, also "information from civil society". Joint Guidelines also recommend recognition of other sources of information, e.g. "credible and reliable open sources" such as reports in reputable newspapers, information from credible private entities like risk assessment reports and analyses, and information from statistical organisations and academia. However, the decision on "credibility" or the "value" and reliability of information about money laundering and terrorist financing risks is absolutely arbitrary in nature.

It is also worth reminding that activities concerning the assessment of the level of risk undertaken by particular obliged entities should be proportionate to the nature and size of a given obliged entity. Therefore, in fact, the assessment of

---

[32] Act of 1 March 2018 maintains the former obligation to develop internal procedures (Article 50 APML), however, it introduces a requirement concerning the approval of such procedures by senior level management before their implementation and application.

[33] The Guidelines are available in Polish at: https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_PL_04-01-2018.pdf (accessed on 25/07/2018).

[34] It concerns factors associated with a client, geographical area (jurisdiction) as well as a product, service or transaction (including delivery channels); *ibid.*

the level of ML/TF risk will be different when conducted by a bank and when conducted by an entrepreneur who operates in accordance with the Act of 2 July 2004 on the freedom of business activity within the scope in which he carries out an occasional transaction paying in cash for goods that are worth 10,000 euros or more. The above indication, although fully understandable and justified, results in an obvious conclusion that referring to such criteria as the type of an institution, the scope of its operations and the likelihood that it may be involved in money laundering or terrorist financing, the territorial range, the size of business, etc. when assessing the level of risk may turn out to be a typical "legal justification" of a given institution's avoidance of undertaking steps ensuring diligent fulfilment of the APML provisions and, as a result, really contributing to the prevention of money laundering and terrorist financing.

Apart from the above, the discussed Act continues to maintain the obliged entities' fundamental obligations connected with the prevention of the discussed phenomena, which result from (negative) risk assessment. They are mainly stipulated in Article 74 APML (the obligation to notify the General Inspector of Financial Information without delay, however not later than in two working days from the confirmation of the suspicion by the obliged entity, about the circumstances that can raise suspicion of the commission of an offence under Article 299 CC [money laundering] or Article 165a CC [terrorist financing], with an indication of the scope of data taken into account in this notification – Article 74 para. 3), Article 86 APML (obligation to notify the GIIF without delay by means of electronic communication about raising justified suspicion that a given transaction or specified financial assets may be connected with money laundering or terrorist financing) and Article 90 APML (the so-called resultant submission of this notification in case its submission without delay has not been possible).

On the other hand, national banks, foreign banks' branches, credit institutions' branches or credit unions/cooperatives are exempt from the application of Article 89 APML stipulating the obligation to notify a prosecutor without delay about raising justified suspicion that financial assets subject to transactions or deposited in an account originate from an offence other than money laundering or terrorist financing, or fiscal crime, or are connected with an offence other than money laundering or terrorist financing, or fiscal crime.[35] The reason is obvious and is connected with *leges speciales* laid down in the provisions of Banking Law, which, within the discussed scope, what is worth mentioning here, were also subject to change.[36]

---

[35] The provision is aimed at detecting the source of "dirty income", called the source act (in other words: the base act) from which laundered financial assets originate.

[36] Compare Article 106a of the Act of 29 August 1997: Banking Law (Journal of Laws [Dz.U.] of 2017, item 1876, as amended), and also the amendment to Article 106a para. 3a of the Act that entered into force based on Article 166 APML, which resulted in the following wording of Article 106a para. 3a: "In case of a justified suspicion that an offence referred to in Article 165a or Article 299 CC was committed, or bank operations were used in order to conceal criminal activities or for the purpose associated with an offence or a fiscal offence, a prosecutor may, by means of a decision, freeze a particular transaction or resources in a bank account for a specified period not exceeding six months, also regardless of the lack of notification referred to in para. 1

Due to the extensive nature of amendments introduced by the Act of 1 March 2018, their exhaustive discussion in a scientific article like this does not seem possible. Moreover, this is not its aim. Its essential objective is to indicate those new provisions that determine obligations of banks as obliged entities in the way that is different from the one binding so far (i.e. laid down in the Act of 16 November 2000). Therefore, reference to the provisions that determined measures of financial security as well as identification or verification of a client's identity, or what kind of transactions are subject to mandatory registration (what has been mentioned in the introduction) will be ignored here as they are less significant for the discussed subject matter.[37] With regard to many of those issues, the provisions of the Act of 1 March 2018 are not much different from those laid down in the former Act. It can be only indicated here that financial security measures should be applied "within the scope and with the intensity taking into account the recognised risk of money laundering or terrorist financing connected with business relationships or an occasional transaction and its assessment" (Article 33 para. 4). Moreover, assessing business relationships, "in the way adequate for the situation", an obliged entity should also obtain information about the aim and intended nature of those relationships, and carry out their ongoing monitoring. This "monitoring" should cover, inter alia, the analysis of transactions conducted with a client "within business relationships" in order to ensure that the transactions are in compliance with the obliged entity's knowledge of the client, the type and scope of its operations, the "examination of the source of financial assets" in the client's disposal and, in cases justified by circumstances, ensuring that the documents, data or information in possession concerning business relationships are continually updated (Article 34 para. 1(1) and (4) APML). Apart from "traditional" financial security measures, obliged entities should ensure, in cases referred to in Articles 43–46 APML, the application of "increased financial security measures", in particular in case of the establishment of business relationships in untypical circumstances or with clients from a high risk third country or having a head office registered there.

Finally, it is worth adding that APML imposes a new obligation on obliged entities, which is not a novelty in case of banks. It is a duty to appoint "higher level management staff" responsible for the fulfilment of the obligations stipulated in statute. This should be interpreted as "a board member, a director or an employee of the obliged entity having the knowledge of the risk of money laundering and terrorist financing connected with an obliged entity's operations and taking decisions that can influence this risk" (Article 2 para. 2(9) APML).[38] Moreover, there is still a binding obligation to appoint an employee holding a senior managerial position responsible for ensuring that the operations of an obliged entity and its employees and other persons performing activities for the benefit of an obliged entity are in compliance with the provisions of the Act on preventing money laundering and terrorist financing (Article 8 APML).

[providing a prosecutor with information that is subject to bank secrecy – A.G.]. The decision shall include the scope, method and time for freezing a transaction or resources in the account".

[37] With regard to this, compare Article 35 APML.

[38] In accordance with Article APML, in case of an obliged entity, in which there is a board or another management body, a person responsible for the implementation of the statutory obligations should be appointed from among those body members.

4. CONCLUSIONS

Summing up, the entry into force of new provisions on preventing money laundering and terrorist financing results from the adjustment of Polish regulations to the EU norms, namely to the 4th AML Directive, which is binding at present. What indicates the fulfilment of the proposals resulting from the implementation of the provisions of the above-mentioned Directive to the national legal system is not just a "cosmetic" change in the provisions that were in force for over 17 years but the introduction of a completely new legal act.[39] The Act of 1 March 2018, adopting the solutions of the 4th Directive, imposes totally new (as far as their essence and wording are concerned) obligations on entities that are subject to its norms. Their catalogue was extended by new categories of institutions, such as e.g. entrepreneurs, in the meaning of the Act of 2 July 2004 on the freedom of business operations, within the scope of the provision of bank deposit safes, and foreign entrepreneurs' branches conducting such operations in the territory of the Republic of Poland or credit institutions in the meaning of the Act of 12 May 2011 on consumer loans. The change in this area was caused by the need for adjusting domestic legal solutions to the "patterns" determined by the EU regulations. The change should be approved of. Undoubtedly, it should also be recognised as right to notice hazards that crypto currencies may pose to business transactions (from the point of view of the possibility of using them to legitimise "dirty" profits). However, as far as this is concerned, the practice will show whether the regulation alone is sufficient enough to prevent financial assets laundering within bitcoin transactions or with the use of other crypto currencies. On the other hand, serious doubts should be raised in connection with new duties imposed on obliged entities, which in fact constitute the essence of the Act of March 2018 and also *ratio legis* for its enacting. This concerns obligations connected with risk assessment. In default of clear and precise criteria for the assessment of the level of risk, taking them into account may be difficult in practice. Much will depend on the procedures used so far, which obliged entities worked out in the years when the Act on preventing money laundering (i.e. the Act of 16 November 2000) was in force and to which they are likely to first of all refer in order to estimate the level of risk of money laundering or terrorist financing. Therefore, it can be expected that banks will continue to be leaders in sending SARs to the GIIF because they have been working out the methods of preventing making use of the financial system to launder money for over twenty years. As a result, banks may be treated as obliged entities that can be expected to diligently implement the provisions of the Act of 1 March 2018. The reasons for that are in general good because of the well-prepared and, first of all, applied in practice procedures of preventing the phenomena referred to in the discussed regulations, the compliance with which constitutes the best guarantee of proper (and efficient) communication between the obliged entities and the GIIF. On the other hand, the imposition of the unclearly defined risk-based approach on obliged entities or the imposition of obligations that are practically impossible for them to fulfil does not

[39] This concerns the Act of 16 November 2000, which entered into force on 23 June 2001.

constitute it. It is enough to indicate such an obligation as ongoing "monitoring of business relationships" with the whole load of imprecise phrases, including the term itself. Thus, it seems that efficient counteracting money laundering or terrorist financing will be possible, first of all, thanks to maintaining in the "new" APML the provisions concerning the mode of proceeding and competences of the entities participating in its implementation, i.e. apart from obliged entities, also the GIIF (performing its statutory duties through the Department of Financial Information), cooperating bodies and entities supervising the implementation of APML within the framework of supervision and control over obliged entities as well as emphasising their efficient cooperation in the field of detecting cases of suspicion that an offence of money laundering or terrorist financing has been committed. At the same time, it is necessary to express a conviction that, following the model of the provisions being in force so far, the efficiency of preventing the discussed phenomena will result from diligent identification of a client by obliged entities, which in case of banks cannot be overestimated, or the application of financial security measures adequate for the situation, which, in close cooperation with the GIIF, may result in freezing accounts, transactions or financial assets, and at the stage of preparatory proceedings in securing incriminating financial assets.

BIBLIOGRAPHY

Chodnicka P., *Zarządzanie ryzykiem prania pieniędzy w systemie bankowym*, Problemy Zarządzania Vol. 10, No. 4(39), 2012.

Czarnecki J., *Wirtualne waluty w projekcie ustawy o Centralnej Bazie Rachunków,* Biuletyn Nowych Technologii No. 2, 2017.

Dąbrowska J., *Charakter prawny bitcoin*, Studia i Artykuły, Człowiek w Cyberprzestrzeni No. 1, 2017.

Kaczmarek T.T., Królak-Werwińska J., *Handel międzynarodowy. Zarządzanie ryzykiem. Rozliczenia finansowe,* Wolters Kluwer, Warsaw 2008.

Mackiewicz P., Musiał M., *Rozwój wirtualnych systemów monetarnych*, Nauki o Finansach (Financial Sciences) No. 1(18), 2014.

Legal regulations

Act of 29 August 1997: Banking Law, consolidated text, Journal of Laws [Dz.U.] of 2017, item 1876, as amended.

Act of 16 November 2000 on preventing the introduction of financial assets originating from illegal or undisclosed sources to financial transactions, Journal of Laws [Dz.U.] No. 116, item 1216.

Act of 27 September 2002 amending the Act on preventing the introduction of financial assets originating from illegal or undisclosed sources to financial transactions, Journal of Laws [Dz.U.] of 2002, No. 180, item 1500.

Act of 2 July 2004 on the freedom of business operations, Journal of Laws [Dz.U.] of 2004, No. 173, item 1807.

Act of 29 July 2005 on public offer and conditions for the introduction of financial instruments to the organised system of transactions and on public companies, Journal of Laws [Dz.U.] of 2016, item 1639 and of 2017 items 452, 724, 791 and 1089.

Act of 12 May 2011 on consumer loans, Journal of Laws [Dz.U.] of 2016, item 1528 and of 2017, item 819.

Act of 19 August 2011 on financial services, Journal of Laws [Dz.U.] of 2011, No. 199, item 1175.

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 (4th AML Directive), OJ L 141, 5.6.2015, pp. 73–117.

5th AML Directive, Procedure 2016/0208: COM (2016) 450: Proposal for a Directive of the European Parliament and of the Council, amending Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, presented by the European Commission on 5 July 2016, adopted by the Council on 14 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15849_2017_INIT&from=PL (accessed on 19/07/2018).

Bill on the Central Database of Accounts (CBR) of 22 December 2016, https://legislacja.rcl.gov.pl/projekt/12293403/katalog/12400913.

Act of 1 March 2018 on preventing money laundering and terrorist financing, Journal of Laws [Dz.U.] of 2018, item 723, as amended.

Other documents and sources

Ordinance No. 16/92 of the President of NBP, the National Bank of Poland, of 1 October 1992 (Dz.Urz. NBP No. 9, item 20), substituted by Ordinance No. C/2/I/94 of the President of NBP of 17 January 1994.

Resolution No. 4/98 of the Commission for Banking Supervision of 30 June 1998.

Guidelines of the European Central Bank of 20 September 2011, 2011/817/EU on monetary policy instruments and procedures of the Eurosystem (ECB/2011/14), http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32011O0014 (accessed on 30/04/2018).

Document of 28 May 2015: Undersecretary of State in the Ministry of Finance [FN7.054.9.2015], *Regulacje dotyczące wirtualnej waluty bitcoin*, Monitor Prawa Bankowego No. 6, 2016.

Report from the Commission to the European Parliament and the Council, Brussels, 26.6.2017, COM 92017, 340 final, http://ec.europa.eu/transparency/regdoc/rep/1/2017/PL/COM-2017-340-F1-PL-MAIN-PART-1.PDF (accessed on 12/07/2018).

GIIF's report on hazards connected with crypto currencies, http://www.mf.gov.pl/ministerstwo-finansow/dzialalnosc/giif/komunikaty/-/asset_publisher/8KnM/content/komunikat-generalnego-inspektora-informacji-finansowej-w-sprawie-niebezpieczenstw-zwiazanych-z-walutami-wirtualnymi?redirect=http%3A%2F%2Fwww.mf.gov.pl%2Fministerstwo-finansow%2Fdzialalnosc%2Fgiif%2Fkomunikaty%3Fp_p_id%3D101_INSTANCE_8KnM%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-2%26p_p_col_count%3D1%26_101_INSTANCE_8KnM_advancedSearch%3Dfalse%26_101_INSTANCE_8KnM_keywords%3D%26_101_INSTANCE_8KnM_delta%3D5%26_101_INSTANCE_8KnM_cur%3D1%26_101_INSTANCE_8KnM_andOperator%3Dtrue%23p_p_id_101_INSTANCE_8KnM_ (accessed on 1/01/2018).

Joint Guidelines of 4 January 2018 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (JC 2017 37), available in Polish at: https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_PL_04-01-2018.pdf (accessed on 25/07/2018) and in English: https://eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf.

GIIF's Report on the implementation of the Act of 16 November 2000 in 2017, Warsaw, March 2018, https://www.mf.gov.pl/documents/764034/1223641/Sprawozdanie+2017 (accessed on 23/07/2018).

Komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego w sprawie "walut" wirtualnych of 7 July 2018, http://www.nbp.pl/home.aspx?f=/aktualnosci/wiadomosci_2017/ww-pl.html (accessed on 12/07/2018).

BANKS' OBLIGATIONS RELATED TO PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE LIGHT OF AMENDED REGULATIONS

Summary

The Act of 1 March 2018 on preventing money laundering and terrorist financing entered into force on 13 July 2018 and repealed the Act of 16 November 2000, substituting for it and introducing a series of changes in the system of preventing those negative phenomena. They consist in the need for obliged entities to assess the level of risk of money laundering or terrorist financing and, as a result, to take adequate financial security measures. A deeper analysis of the Act results in a conclusion that many of the newly enacted regulations, in fact, refer to terminology that is quite often not clear and unambiguous enough. Such a state may cause difficulties with the application of its provisions, which in particular concerns obliged entities, i.e. entities on which the Act imposes obligations connected with the protection of the financial system against the use of those entities to launder money or finance terrorism. On the other hand, banks hold a leading position in this system both in the sphere of regulations and actual, active involvement in preventing those phenomena. It results, inter alia, from prevention mechanisms that have been worked out for many years as well as internal regulations that can really contribute to the elimination of those financial institutions' participation in money laundering or terrorist financing. Therefore, it can be assumed that they constitute a kind of "model" obliged institutions for which the Act of 1 March 2018 is of fundamental importance. It seems to be especially significant that the presented expectations are not always supported by adequate norms, which concerns not just the idea of preventing money laundering but the requirements and methods of determining them in the Act of 1 March 2018. The present article is devoted to those issues.

Keywords: money laundering, terrorist financing, banks, obliged entities

OBOWIĄZKI BANKÓW ZWIĄZANE Z PRZECIWDZIAŁANIEM PRANIU PIENIĘDZY ORAZ FINANSOWANIEM TERRORYZMU W ŚWIETLE ZNOWELIZOWANYCH PRZEPISÓW

Streszczenie

W dniu 13 lipca 2018 r. weszła w życie ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, która uchyliła obowiązującą do tej daty ustawę z dnia 16 listopada 2000 r., zastępując ją i wprowadzając szereg zmian w systemie

prewencji przed tymi negatywnymi zjawiskami. Sprowadzają się one do potrzeby przeprowadzania przez instytucje obowiązane oceny poziomu ryzyka prania pieniędzy oraz finansowania terroryzmu, a w ślad za tym podejmowania stosownych środków bezpieczeństwa finansowego. Bardziej dogłębna analiza przedmiotowej ustawy nasuwa jednak spostrzeżenie, że wiele z nowowprowadzonych regulacji odwołuje się w istocie do terminologii, która nierzadko jest niewystarczająco klarowna i jednoznaczna. Taki stan rzeczy może powodować trudności w stosowaniu jej postanowień, co odnosi się w szczególności do instytucji obowiązanych, czyli podmiotów, na które przedmiotowy akt prawny nakłada obowiązki związane z ochroną systemu finansowego przed wykorzystaniem tych instytucji w celu prania pieniędzy lub finansowania terroryzmu. W systemie tym zaś banki od lat zajmują pozycję lidera zarówno w sferze regulacji, jak i faktycznego, aktywnego zaangażowania w zapobieganie tym procederom. Wynika to m.in. z wypracowanych mechanizmów prewencyjnych, a także wewnętrznych regulacji, które realnie mogą przyczynić się do wyeliminowania przypadków udziału tych instytucji finansowych w praniu pieniędzy lub finansowaniu terroryzmu. Można więc uznać, że stanowią one rodzaj „modelowych" instytucji obowiązanych, dla których zarazem ustawa z 1 marca 2018 r. ma kardynalne znaczenie. Wydaje się ono tym bardziej istotne, że tak nakreślone oczekiwania nie w każdym przypadku znajdują poparcie w stosownych unormowaniach, co dotyczy nie tyle samej idei zapobiegania praniu pieniędzy, ale raczej wymagań i sposobu ich określenia w ustawie z dnia 1 marca 2018 r. Tym zagadnieniom poświęcone jest niniejsze opracowanie.

Słowa kluczowe: pranie pieniędzy, finansowanie terroryzmu, banki, podmioty obowiązane

OBLIGACIÓN DE BANCOS EN RELACIÓN CON LA LUCHA CONTRA EL BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO A LA LUZ DE LOS PRECEPTOS REFORMADOS

Resumen

El 13 de julio de 2018 entró en vigor la ley de 1 de marzo de 2018 sobre lucha contra el blanqueo de capitales y financiación del terrorismo que derogó la ley de 16 de noviembre de 2000 vigente hasta dicha fecha y la sustituyó, introduciendo numerosas modificaciones en el sistema de prevención ante estos fenómenos negativos. Dichas modificaciones consisten en la necesidad de realizar juicio de nivel de riesgo de blanqueo de capitales y de financiación del terrorismo por parte de las instituciones obligadas y adoptar medidas adecuadas de seguridad financiera. El análisis más profundo de dicha ley lleva a la conclusión que muchas de las regulaciones nuevas hacen referencia a la terminología que es equívoca o no es clara. Tal estado de las cosas puede ocasionar dificultades en aplicación de sus disposiciones, lo que se refiere en particular a las instituciones obligadas, o sea sujetos a los que esta ley impone obligaciones relacionadas con la protección del sistema financiero ante utilización de estas instituciones para fines de blanqueo de capitales o financiación del terrorismo. En este sistema, los bancos desde hace años son líderes en la regulación y participan activamente en prevenir tales procesos. Esto viene, entre otros, de mecanismos de prevención puestos en práctica desde hace muchos años, así como de regulación interna que realmente puede ayudar a eliminar casos de participación de estas instituciones financieras en el blanqueo de capitales o financiación de terrorismo. Por lo tanto, pueden ser consideradas como instituciones obligadas "ejemplares", para las cuales la ley de 1 de marzo de 2018 tiene importancia fundamental. Tal expectativa no en cada caso

es fundada en la normativa adecuada, lo que se refiere no sólo a la idea en sí en prevenir el blanqueo de capitales, sino también a los requisitos y forma de su determinación por la ley de 1 de marzo de 2018. El artículo versa sobre todas estas cuestiones.

Palabras claves: blanqueo de capitales, financiación del terrorismo, bancos, instituciones obligadas

ОБЯЗАННОСТИ БАНКОВ, СВЯЗАННЫЕ С ПРОТИВОДЕЙСТВИЕМ ОТМЫВАНИЮ ДЕНЕГ И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА В СВЕТЕ НОВЕЛИЗИРОВАННЫХ ПОЛОЖЕНИЙ

Резюме

13 июля 2018 года вступил в силу Закон от 1 марта 2018 года о противодействии отмыванию денег и финансированию терроризма. Упомянутый Закон отменил и заменил действующий до этого времени Закон от 16 ноября 2000 года, что привело к введению ряда изменений в системе превенции этих негативных явлений. Они сводятся к необходимости проведения институтами обязательного анализа уровня риска отмывания денег и финансирования терроризма, с последующим принятием соответствующих мер финансовой безопасности. Тем не менее, более глубокий анализ упомянутого закона приводит к размышлениям о том, что многие из нововведённых норм фактически опираются на терминологию, которая нередко является недостаточно точной и однозначной. Такое положение вещей может усложнить соблюдение его положений, что касается в первую очередь специализированных учреждений, то есть субъектов, на которые этот правовой акт накладывает обязательства, связанные с защитой финансовой системы от использования этих учреждений в целях отмывания денег или финансирования терроризма. В данной системе в течение многих лет банки занимают лидирующие позиции как в сфере регулирования, так и в фактическом активном участии в деле по предотвращению этой практики. Это основано на разработанных в течение многих лет превентивных механизмах, а также внутренних нормах, которые могут на деле способствовать предотвращению участия финансовых учреждений в отмывании денег или финансировании терроризма. В связи с этим можно утверждать, что они выступают в качестве своего рода «образцовых» специализированных учреждений, для которых Закон от 1 марта 2018 года является ключевым. Представляется это тем более существенным, поскольку так чётко обозначенные потребности не всегда находят поддержку в соответствующих нормативных актах, что касается не столько самой идеи предотвращения практики отмывания денег, сколько предписаний и способа её определения в Законе от 1 марта 2018 года. Данной проблематике посвящено настоящее исследование.

Ключевые слова: отмывание денег, финасирование терроризма, банки, специализированные учреждения

VERPFLICHTUNGEN DER BANKEN VERBUNDEN MIT DER GEGENWIRKUNG VON GELDWÄSCHEREI UND TERRORISMUSFINANZIERUNG IN ANSEHUNG VON NOVELLIERTEN VORSCHRIFTEN

Zusammenfassung

Am 13. Juli 2018 trat in Kraft das Gesetz vom 01. März 2018 über die Gegenwirkung von Geldwäscherei und Terrorismusfinanzierung, welches das bis zu diesem Datum geltende Gesetz vom 16. November 2000 aufhob, dieses damit ersetzend und einige Änderungen im Präventionssystem vor diesen negativen Vorgängen einführend. Diese Änderungen führen zur Notwendigkeitsdurchführung eines Risikoniveaus Geldwäscherei und Terrorismusfinanzierung seitens dazu verpflichteter Institutionen, darauffolgend auf entsprechende finanzielle Sicherheitsmaßnahmen, einzugehen. Eine tiefere Analyse des gegebenen Gesetzes bietet jedoch eine Anmerkung, dass zahlreiche von neu eingeführten Regulierungen sich allerdings auf die Terminologie berufen, welche des Öfteren unzureichend klar und eindeutig ist. So ein Sachverhalt kann es erschweren, die Gesetzbestimmungen anzuwenden, besonders in Bezug auf dazu verpflichtete Institutionen, also Subjekte, auf welche der gegebene Rechtsakt Verpflichtungen auferlegt, die mit dem Finanzsystemschutz vor der Ausnutzung dieser Institutionen zum Zweck von Geldwäscherei und Terrorismusfinanzierung verbunden sind. In diesem System rangieren wiederum die Banken seit Jahren auf führenden Positionen nicht nur in dem Regulierungsbereich, sondern auch im tatsächlichen, aktiven Einsatz in Vorbeugung solcher Aktivitäten, was u.a. aus seit Jahren ausgearbeiteten Präventionsmechanismen resultiert, darüber hinaus auch aus internen Bestimmungen, welche durchaus zur Eliminierung von Teilnahmefällen solcher Institutionen in der Geldwäscherei beziehungsweise Terrorismusfinanzierung beitragen können. Es kann demnach angenommen werden, dass diese Institutionen etwa „Modellinstitutionen" darstellen, für welche zugleich das Gesetz vom 01. März 2018 eine Grundbedeutung hat. Es scheint umso wichtiger, dass auf diese Weise vorgezeichnete Erwartungen nicht in jedem einzelnen Fall Unterstützung in dementsprechenden Normalisierungen finden, dies betrifft nicht die Idee als solche gegen die Geldwäscherei entgegenzuwirken, aber eher die Erwartungen von deren Bestimmungsweisen im Einklang mit dem Gesetz vom 01. März 2018. Die vorliegende Bearbeitung dient diesem Zweck.

Schlüsselwörter: Geldwäscherei, Terrorismusfinanzierung, Banken, verpflichtete Institutionen

LES OBLIGATIONS DES BANQUES VISAIENT À LUTTER CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME À LA LUMIÈRE DES RÈGLEMENTS MODIFIÉS

Résumé

Le 13 juillet 2018, la loi du 1er mars 2018 sur la lutte contre le blanchiment de capitaux et le financement du terrorisme est entrée en vigueur. Elle a abrogé la loi du 16 novembre 2000, applicable jusqu'à cette date, en la remplaçant et en introduisant un certain nombre de modifications du système de prévention contre ces phénomènes négatifs. Ces modifications concernent la nécessité pour les institutions engagées d'évaluer le niveau de risque de

blanchiment de capitaux et de financement du terrorisme et, en conséquence, de prendre les mesures de sécurité financière appropriées. Cependant, une analyse plus approfondie de cette loi suggère que nombre des réglementations nouvellement introduites font essentiellement référence à une terminologie souvent insuffisamment claire et sans ambiguïté. Cet état de fait peut entraîner des difficultés dans l'application de ses dispositions, ce qui s'applique notamment aux institutions soumises à obligations, c'est-à-dire les entités auxquelles cet acte juridique impose des obligations relatives à la protection du système financier contre l'utilisation de ces institutions à des fins de blanchiment de capitaux ou de financement du terrorisme. Dans ce système, les banques occupent depuis de nombreuses années la position de leader en matière de réglementation et de participation active à la prévention de ces pratiques. Ceci est dû à des mécanismes de prévention mis au point depuis de nombreuses années, ainsi que des réglementations internes pouvant effectivement contribuer à éliminer les cas de participation des institutions financières au blanchiment de capitaux ou au financement du terrorisme. On peut donc considérer qu'il s'agit d'un type d'institutions «modèles» soumises à des obligations, pour lesquelles l'acte du 1er mars 2018 revêt une importance capitale. Il semble d'autant plus important que de telles attentes ne trouvent pas toujours leur soutien dans des réglementations appropriées, qui concernent non pas tant l'idée de prévenir le blanchiment de capitaux, mais plutôt les exigences et la manière de les définir dans la loi du 1 er mars 2018. Ce sens semble d'autant plus important que des attentes décrites de cette façon ne sont pas toujours étayées par les réglementations pertinentes, ce qui concerne non pas tant l'idée de prévenir le blanchiment de capitaux, mais plutôt les exigences et la manière de les définir dans la loi du 1 er mars 2018. Cette étude est consacrée à ces questions.

Mots-clés: blanchiment de capitaux, financement du terrorisme, banques, institutions soumises à obligations

OBBLIGHI DELLE BANCHE IN MATERIA DI PREVENZIONE DEL RICICLAGGIO DI DENARO E DEL FINANZIAMENTO DEL TERRORISMO ALLA LUCE DELLE NORME MODIFICATE

Sintesi

Il 13 luglio 2018 è entrata in vigore la legge del 1° marzo 2018 sulla lotta al riciclaggio di denaro e al finanziamento del terrorismo, che ha abrogato la legge del 16 novembre 2000, in vigore fino a tale data, sostituendola e introducendo una serie di modifiche al sistema di prevenzione contro questi fenomeni negativi. Si riducono alla necessità che gli enti obbligati valutino il livello di rischio di riciclaggio e di finanziamento del terrorismo e, di conseguenza, adottino adeguate misure di sicurezza finanziaria. Tuttavia, un'analisi più approfondita della legge in questione suggerisce che molte delle nuove norme introdotte fanno riferimento a una terminologia spesso non sufficientemente chiara e priva di ambiguità. Tale circostanza può causare difficoltà nell'applicazione delle sue disposizioni, che si riferisce in particolare agli enti obbligati, vale a dire entità alle quali l'atto giuridico in questione impone obblighi relativi alla protezione del sistema finanziario contro l'uso di tali enti a scopo di riciclaggio o di finanziamento del terrorismo. In questo sistema, le banche sono da anni all'avanguardia sia in termini di regolamentazione che di effettivo e attivo coinvolgimento nella prevenzione di tali pratiche. Il che è il risultato, tra l'altro, dei meccanismi di prevenzione sviluppati nel corso degli anni, nonché della regolamentazione interna, che può dare un reale contributo all'eliminazione dei casi di partecipazione di queste istituzioni finanziarie al riciclaggio di

denaro o al finanziamento del terrorismo. Si può quindi concludere che essi costituiscono una specie di "modello" di istituzioni obbligatorie, per le quali la legge del 1° marzo 2018 è di importanza fondamentale. Sembra tanto più importante in quanto tali aspettative non sempre sono sostenute da norme pertinenti, il che riguarda non solo l'idea stessa di pervenire il riciclaggio di denaro, ma piuttosto i requisiti e il modo di definirle nella legge del 1° marzo 2018. Tali questioni sono oggetto del presente studio.

Parole chiave: riciclaggio di denaro, finanziamento del terrorismo, banche, istituzioni obbligatorie

Cytuj jako:

Golonka A., *Banks' obligations related to prevention of money laundering and terrorist financing in the light of amended regulations [Obowiązki banków związane z przeciwdziałaniem praniu pieniędzy oraz finansowaniem terroryzmu w świetle znowelizowanych przepisów]*, „Ius Novum" 2019 (Vol. 13) nr 2, s. 124–145. DOI: 10.26399/iusnovum.v13.2.2019.19/a.golonka

Cite as:

Golonka, A. (2019) 'Banks' obligations related to prevention of money laundering and terrorist financing in the light of amended regulations', *Ius Novum* (Vol. 13) 2, 124–145. DOI: 10.26399/iusnovum.v13.2.2019.19/a.golonka