Hatály: 2018.I.3. -

Act LIII of 2017

on the Prevention and Combating of Money Laundering and Terrorist Financing[1]

The objective of this Act is to effectively enforce the provisions on combating money laundering and terrorist financing with a view to preventing the laundering of money and other financial means obtained from criminal activities through activities which are considered exposed to potential money laundering operations, as well as to help prevent the flow of funds and other financial means used in financing terrorism. In order to achieve the aforementioned objectives Parliament has adopted the following Act:

1. Scope

Section 1

(1) Subject to the exceptions set out in Subsections (3) and (4), this Act shall apply to the following entities having a registered office, branch or business establishment in Hungary:

a) credit institutions;

b) financial services institutions;

c) institutions for occupational retirement provision;

d) voluntary mutual insurance funds;

e) operators accepting and delivering international postal money orders;

f) providers of real estate agency or brokering and any related services;

g) providers of auditing services;

h) providers of accountancy (bookkeeping), tax expert, certified tax expert services, tax advisory activities under agency or service contract;

i) operators of casinos, card rooms, or providers of gambling services - other than distance gambling -, distance gambling services, online casino games;

j) traders in precious metals or articles made of precious metals;

k) traders in goods, involving a cash payment in the amount of two million five hundred thousand forints or more;

l) attorneys, notaries public; and

m) fiduciary managers;

(hereinafter referred to collectively as “service providers”).

(2) This Act shall apply to:

a) customers of service providers, including their authorized representatives, agents, proxies;

b) directors, employees of service providers and their contributing family members.

(3) This Act covers the supervisory body provided for in Section 5.

(4) This Act shall not apply to:

a) the activities of service providers relating to the provision of support to their employees tax

[1] Adopted by Parliament on 16 May 2017.

free or under preferential tax treatment under the Personal Income Tax Act, provided that the funds received in support can be used solely for certain specific goods or services specified in the Personal Income Tax Act;

b) the activities of financial services institutions concerning the provision of credit reference services and the operation of payment systems under Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (hereinafter referred to as "CIFE").

(5) This Act shall apply to the Magyar Nemzeti Bank (*National Bank of Hungary*) (hereinafter referred to as "MNB") only to the extent pertaining to its supervisory activities, and in connection with the regulations where this Act makes an express reference to the MNB.

(6) The provisions of this Act on establishing business relationships shall also apply to notaries public, if involved in the pursuit of activities under Subsection (2) of Section 73.

Section 2

Section 26 shall apply to the service providers referred to in Paragraphs *a), b)* and *e)* of Subsection (1) of Section 1 and to the MNB, if such service providers and the MNB is engaged in the provision of transfer of funds services under Point 9 of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No. 1781/2006 (hereinafter referred to as "Regulation").

2. Definitions

Section 3

For the purpose of this Act:

1. 'tax consultant, tax expert, certified tax expert' shall mean a person who has the professional qualification acquired in compliance with the professional and examination requirements adopted by the minister in charge of taxation, and is authorized to engage in the activities of tax consultants, tax experts and certified tax experts, and who is listed in the register of tax experts, tax consultants and certified tax experts provided for in the Act on the Rules of Taxation;
2. 'parent company' shall mean any company which effectively exercises a controlling influence over another company;
3. 'identification' shall mean a process where the data specified in Subsection (2) of Section 7, Subsections (2) and (3) of Section 8 and Subsections (1) and (2) of Section 9 are recorded in a documented traceable manner;
4. 'trader in goods' shall mean a person who, in the course of his economic activity, supplies products to consumers, traders and processing operators;
5. 'commodity dealer' shall mean the commodity dealer defined in Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities (hereinafter referred to as "IRA");
6. 'group' shall mean a group of companies which consists of a parent company, its subsidiaries, branches and the entities in which the parent company or its subsidiaries exercise controlling influence or hold a participating interest;
7. 'electronic money' shall mean the electronic money defined in the CIFE;
8. 'electronic money institution' shall mean the electronic money institution defined in Act

CCXXXV of 2013 on Payment Service Providers (hereinafter referred to as "PSP");

9. 'controlling influence' shall mean the dominant influence referred to under the definition of parent company in Act C of 2000 on Accounting (hereinafter referred to as "Accounting Act"), or a relationship between a person and a company:

a) under which the person with control has the capacity to decide on the distribution of the company's profits, the diversification of profit or loss to another company or the company's strategy, business or marketing policies,

b) that permits coordination of the management of the company with that of another company for the purposes of a mutual objective, regardless of whether the agreement is fixed in the articles of association (charter document) of the company or in another written contract,

c) under which common management is exercised through the management bodies, supervisory boards of the companies comprised of all or some of the same persons (who provide the necessary decision-making majority), or

d) under which the person with control is able to exercise substantial influence in the operation of another company without any capital involvement;

10. 'life insurance activities' shall mean activities in classes of life insurance listed under Annex 2 to Act LXXXVIII of 2014 on the Business of Insurance (hereinafter referred to as "Insurance Act");

11. 'European Union' shall mean the European Union and the European Economic Area;

12. 'shell bank' shall mean a credit institution, financial services institution or credit institution, an institution engaged in equivalent activities, established in a state in which it has no head office, and which is unaffiliated with a regulated financial group;

13. 'negotiable credit token' shall mean the negotiable credit token defined in the CIFE;

14. 'head office' shall mean the place where the service provider conducts its principal activity and where ultimate decision-making takes place;

15. 'third country' shall mean any state that is not a member of the European Union;

16. 'credit institution' shall mean the credit institution defined in the CIFE, excluding the MNB;

17. 'real estate agency or brokering' shall mean the business of mediation of the transfer or lease of real estate properties, and the sale of own real estate property commercially;

18. 'unincorporated organization' shall mean any legal entity other than legal persons and natural persons:

19. 'risk sensitivity approach' shall mean a procedure fixed in the internal policy referred to in Section 65 relying on the outcome of internal risk assessment, based on the nature of the business relationship or on the type and value of the transaction order and on the customer's circumstances, for the purpose of prevention and combating money laundering and terrorist financing;

20. 'accountancy' shall mean the accounting services defined in the Accounting Act;

21. 'foreign financial intelligence unit' shall mean the authority of any Member State of the European Union or any third country with similar or identical functions as the national financial intelligence unit with particular regard to the requirements of the Financial Action Task Force (FATF) and the Egmont Group;

22. 'subsidiary' shall mean any company over which another company effectively exercises a controlling influence, on the understanding that all subsidiaries of subsidiary companies shall also be considered subsidiaries of the parent company;

23. 'correspondent relationship' shall mean:

a) the provision of financial or investment services by one credit institution to another credit

institution, including providing a payment account, cash management, international funds transfers, check clearing and foreign exchange services;

b) the relationships between and among credit institutions and financial services institutions including, in particular, relationships established for securities transactions and payment transactions;

24. 'national risk assessment' shall mean an assessment at national level intended to identify, evaluate and interpret the risk of money laundering and terrorist financing, including the ongoing review thereof, and to define national risk management procedures;

25. 'payment institution' shall mean the payment institution defined in the PSP, and the institution operating the Posta Elszámoló Központ (*Postal Clearing Center*);

26. 'money laundering' shall mean either of the conducts defined in Sections 303-303/A of Act IV of 1978 on the Criminal Code in force until 30 June 2013 (hereinafter referred to as "Act IV/1978"), and in Sections 399-400 of Act C of 2012 on the Criminal Code (hereinafter referred to as "Criminal Code");

27. 'national financial intelligence unit' shall mean a department of the Nemzeti Adó- és Vámhivatal (*National Tax and Customs Authority*) delegated by the relevant legislation;

28. 'financial services institution' shall cover the following:

a) financial enterprises,

b) entities engaged in money processing activities, other than financial enterprises, in respect of their money processing operations,

c) payment institutions, in respect of their activities falling within the framework of payment services,

d) electronic money institutions, in respect of their activities falling within the framework of issuance of electronic money and payment services,

e) issuers of credit tokens;

f) currency exchange offices,

g) insurance companies, if authorized to pursue life insurance activities, in respect thereof,

h) multiple agents and brokers provided for in the Insurance Act as regards their activities relating to contracts within the life insurance branch;

i) multiple special services intermediaries and brokers defined in the CIFE,

j) investment firms,

k) commodity dealers, in respect of their activities falling within the framework of commodity exchange services,

l) investment fund managers, in respect of the marketing of investment units,

m) 'market operators' in respect of their activities defined in Act CXX of 2001 on the Capital Market (hereinafter referred to as "CMA") and the IRA;

29. 'financial enterprise' shall mean the financial enterprise defined in the CIFE;

30. 'currency exchange office' shall mean a special services intermediary pursuing currency exchange activities under contract with a credit institution;

31. 'high-risk third countries with strategic deficiencies' shall mean the countries provided for in Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies;

32. 'official document suitable for identification purposes' shall mean a personal identification document (identity card), passport, and driver's license card;

33. 'verification of identity' shall mean the procedure to verify the identity of the customer, agent, proxy or other authorized representative in accordance with Subsections (3)-(9) of Section

7, and to verify the identity of the beneficial owner in accordance with Subsection (5) of Section 8 and Subsection (4) of Section 9;

34. 'director of service provider' shall mean a natural person acting for the benefit of the legal person or unincorporated organization based on a power of representation, an authority to take decisions on behalf of or an authority to exercise control within that service provider;

35. 'director appointed under the service provider's internal policy provided for in Section 65' shall mean a natural person appointed by the director of service provider under the internal policy provided for in Section 65 according to the following criteria:

a) must have sufficient knowledge of the service provider's money laundering and terrorist financing risk exposure, and

b) must have sufficient seniority to initiate or take decisions affecting risk exposure;

36. 'terrorist financing' shall mean the provision or collection of funds with the intention that they should be used in order to carry out any of the offences within the meaning of Subsections (1) and (2) of Section 261 of Act IV/1978, or either of the conduct defined in Section 318 of the Criminal Code;

37. 'series of related transactions' shall mean:

a) the transactions for which the same customer places an order within a period of one year under the same title for the same subject matter;

b) in connection with currency exchange offices, the transactions conducted on the same customer's behalf within a period of one week;

c) as regards the service providers provided for in Paragraph *k)* of Subsection (1) of Section 1, installment payments and payment orders based on deferred payment facilities;

38. 'beneficial owner' shall mean:

a) any natural person who owns or controls at least twenty-five per cent of the shares or voting rights in a legal person or an unincorporated organization directly or - by way of the means defined in Subsection (4) of Section 8:2 of Act V of 2013 on the Civil Code (hereinafter referred to as "Civil Code") - indirectly, or who is able to exercise effective control over the legal person or unincorporated organization via other means, if that legal person or unincorporated organization is not listed on a regulated market and is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards,

b) any natural person who has a dominant influence in a legal person or unincorporated business association as defined in Subsection (2) of Section 8:2 of the Civil Code,

c) any natural person on whose behalf a transaction is being conducted, or who is able to exercise effective control over the activity of a customer via other means in the case of natural persons,

d) in the case of foundations:

da) where the future beneficiaries have already been determined, the natural person who is the beneficiary of twenty-five per cent or more of the property of the foundation,

db) where the individuals that benefit from the foundation have yet to be determined, the natural person in whose main interest the foundation is set up or operates, or

dc) the natural person who exercises control in the management of the foundation or exercises control over at least twenty-five per cent of the property of a foundation, and/or who is authorized to represent the foundation,

e) in the case of fiduciary asset management contracts:

ea) the principal, and the beneficial owner referred to in Paragraph *a)* or *b)* thereof,

eb) the fiduciary, and the beneficial owner referred to in Paragraph *a)* or *b)* thereof,

ec) the beneficiaries or class of beneficiaries, and the beneficial owner referred to in Paragraph

a) or *b)* thereof, furthermore

ed) any natural person exercising effective control over the trust fund via other means, furthermore

f) in the absence of the natural person referred to in Paragraphs *a)* and *b)*, the executive officer of the legal person or unincorporated business association;

39. 'issuer of credit tokens' shall mean a service provider authorized to issue negotiable credit tokens;

40. 'guidelines' shall mean instructions issued by the supervisory body provided for in Section 5 within the framework of its supervisory functions delegated under this Act, addressed to service providers in the following documents:

a) regulation issued to service providers provided for in Paragraphs *a)-f), h)-k)* and *m)* of Subsection (1) of Section 1,

b) guidance of a binding nature issued to the service provider defined in Paragraph *g)* of Subsection (1) of Section 1, and

c) instructions and rules of a binding nature issued to the service provider defined in Paragraph *l)* of Subsection (1) of Section 1,

(hereinafter referred to collectively as "guidelines");

41. 'customer' shall mean:

a) any person entering into a business relationship with the service provider, or who places an order with the service provider to carry out a transaction, and

b) as regards the service provider provided for in Paragraph *f)* of Subsection (1) of Section 1, any person requesting an offer for the purchase or sale, or the rental or lease of a real estate property;

42. 'customer due diligence' shall mean:

a) the implementation of the customer due diligence measures specified under Sections 7-11 in the case under Section 6,

b) customer due diligence measures carried out by operators of casinos, card rooms, distance gambling, online casino games in connection with the registration of players;

43. 'transaction' shall mean:

a) an operation comprising a part of a service provided under business relationship by the service provider within its professional activities, or

b) transaction order;

44. 'transaction order' shall mean a temporary relationship established by contract between a customer and a service provider pertaining to the services of the service provider falling within its professional activities;

45. 'business relationship' shall mean:

a) a long-term legal relationship established by contract between a customer and a service provider pertaining to the services of the service provider within the meaning of the activities described in Paragraphs *a)-e), g), h)* and *j)-m)* of Subsection (1) of Section 1,

b) as regards the operators of casinos or card rooms, a long-term legal relationship established when first entering the casino or card room, or as regards distance gambling operators and operators of online casino games, the registration of a player,

c) as regards the service provider provided for in Paragraph *f)* of Subsection (1) of Section 1, a legal relationship between a customer and a service provider pertaining to the services of the service provider falling within its professional activities.

Section 4

(1) For the purposes of this Act, 'politically exposed person' shall mean a natural person who is entrusted with prominent public functions, or who has been entrusted with prominent public functions within one year before the implementation of customer due diligence measures.

(2) For the purposes of Subsection (1), 'natural person who has been entrusted with prominent public functions' shall include:

a) heads of State, heads of government, ministers and deputy ministers, state secretaries, in Hungary the head of State, the Prime Minister, ministers and state secretaries;

b) members of parliament or of similar legislative bodies, in Hungary members of parliament and spokesmen for the nationality;

c) members of the governing bodies of political parties, in Hungary members and officers of the governing bodies of political parties;

d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, in Hungary members of the Alkotmánybíróság (*Constitutional Court*), of the courts of appeal and the Kúria (*Curia*);

e) members of courts of auditors or of the boards of central banks, in Hungary the President and Vice-President of the Állami Számvevőszék (*State Audit Office*), members of the Monetáris Tanács (*Monetary Council*) and the Pénzügyi Stabilitási Tanács (*Financial Stability Board*);

f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces, in Hungary the head of the central body of law enforcement bodies and organizations and his deputy, Chief of Staff of the Hungarian Army and Deputy Chiefs of Staff of the Hungarian Army;

g) members of the administrative, management or supervisory bodies of enterprises with majority state ownership, in Hungary the managing directors of enterprises with majority state ownership, including members of the management body exercising control or supervisory rights of such enterprises;

h) directors, deputy directors and members of the board or equivalent function of an international organization.

(3) For the purposes of this Act 'family members of politically exposed person' shall include the spouse or domestic partner of a politically exposed person; the biological and adopted children, stepchildren and foster children and their spouses or domestic partners, of a politically exposed person; the biological, adoptive, step- and foster parents of a politically exposed person.

(4) For the purposes of this Act, persons known to be close associates of politically exposed persons shall include:

a) any natural person who is known to have joint beneficial ownership of legal entities or unincorporated organizations, or any other close business relations, with a person referred to in Subsection (2);

b) any natural person who has sole beneficial ownership of a legal entity or unincorporated organization which is known to have been set up for the benefit of a person referred to in Subsection (2).

(5) The provisions of this Act relating to politically exposed persons shall also apply to family members or persons known to be close associates of politically exposed persons.

Section 5

For the purposes of this Act, 'supervisory body' shall mean:

a) the Magyar Nemzeti Bank (*National Bank of Hungary*) (hereinafter referred to as "Authority"), acting within its function as supervisory authority of the financial intermediary system with respect to the service providers referred to in Paragraphs *a)-e)* of Subsection (1) of

Section 1;

b)[2] the gaming supervisory authority with respect to the service providers referred to in Paragraph *i)* of Subsection (1) of Section 1;

c) the Magyar Könyvvizsgálói Kamara (*Chamber of Hungarian Auditors*) with respect to the service providers referred to in Paragraph *g)* of Subsection (1) of Section 1;

d) with respect to the service providers referred to in Paragraph *l)* of Subsection (1) of Section 1, in accordance with the derogating provisions set out in this Act pertaining to independent lawyers and law offices (hereinafter referred to collectively as "lawyers") and notaries public:

da) the bar association in which the lawyer in question is registered (hereinafter referred to as "regional bar association"),

db) the association in which the notary public in question is registered (hereinafter referred to as "regional association of notaries);

e) with respect to the service providers referred to in Paragraphs *j)* and *k)* of Subsection (1) of Section 1, the authority for trade and commerce;

f) with respect to the service providers referred to in Paragraphs *f)* and *h)* of Subsection (1) of Section 1, the authority functioning as the national financial intelligence unit (hereinafter referred to as "financial intelligence unit");

g) the office provided for in the Act on Fiduciaries and on the Regulations Governing Their Activities (hereinafter referred to as "Office") with respect to the service providers referred to in Paragraph *m)* of Subsection (1) of Section 1.

3. Customer due diligence obligation

Section 6

(1) Service providers shall apply customer due diligence measures in the following cases:

a) when establishing a business relationship;

b) when carrying out an occasional transaction that amounts to three million six hundred thousand forints or more;

c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to two million five hundred thousand forints or more;

d) when carrying out an occasional transaction that constitutes a transfer of funds, as defined in Point 9 of Article 3 of the Regulation, exceeding three hundred thousand forints;

e) for providers of gambling services, other than distance gambling, upon the payment of winnings amounting to six hundred thousand forints or more in the case of gambling services, other than distance gambling, provided through means other than communications equipment and networks, or upon the payment from player account amounting to six hundred thousand forints or more in the case of gambling services, other than distance gambling, provided through communications equipment and networks;

f) when there is any information, fact or circumstance giving rise to a suspicion of money laundering or terrorist financing, where the due diligence measures referred to in Paragraphs *a)-e)* have not been carried out yet;

g) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

---

[2] Amended by Section 101 of Act LXXII of 2017.

(2) The due diligence obligation provided for in Paragraphs *b)* and *c)* of Subsection (1) shall also apply to any series of related transactions with a combined value in the amount specified in Paragraphs *b)* and *c)* of Subsection (1). In this case, due diligence measures shall be carried out in connection with the transaction that brings the total value of the transactions to the amount specified in Paragraphs *b)* and *c)* of Subsection (1).

4. Customer due diligence measures

Section 7

(1) In the cases under Subsection (1) of Section 6 and Subsection (1) of Section 21, service providers shall carry out customer identification and verification procedures, including the customer's agent, proxy or other authorized representative.

(2) In the identification procedure, service providers are required to record the following particulars:

a) in the case of natural persons:

aa) surname and forename,

ab) surname and forename by birth,

ac) nationality,

ad) date and place of birth,

ae) mother's birth name,

af) home address, or habitual residence in the absence thereof,

ag) number and type of identification document;

b) in the case of legal persons or unincorporated organizations:

ba) name, abbreviated name,

bb) registered office, or the address of the Hungarian branch of foreign companies, if applicable,

bc) main activities,

bd) name and position of authorized representatives,

be) identification data of agent for service of process,

bf) the registered number of legal persons listed in the companies register, or the number of the resolution adopted on the foundation (registration, admission into the register) of other legal persons, or their register number,

bg) tax number.

(3) For the purposes of identification and verification procedures, service providers must require the following documents to be presented:

a) in the case of natural persons:

aa) official document suitable for identification purposes and official address card for Hungarian citizens,

ab) passport or personal identification document for foreign nationals, if it embodies an authorization to reside in Hungary, document evidencing the right of residence or a valid residence permit;

b) in the case of legal persons and unincorporated organizations, in addition to the documents of the persons described in Paragraph *a)* who are authorized to act in its name or on its behalf, a document issued within thirty days to date, to verify:

ba) if a domestic economic operator, that it has been registered by the court of registry, or that

the application for registration has been submitted; if a private entrepreneur, that the private entrepreneur's license or the certificate of registration has been issued,

bb) for other domestic legal persons whose existence is subject to registration by an authority or court, the document of registration,

bc) for foreign legal persons and unincorporated organizations, the document proving that it has been entered or registered under the law of the country in which it is established;

c) the instrument of constitution of legal persons and unincorporated organizations that have not yet been submitted to the court of registry, court or appropriate authority.

(4) In the case provided for in Paragraph *c)* of Subsection (3), the legal person or unincorporated organization shall produce documentary evidence of having been registered by the court of registry, the competent authority or court, within thirty days after the fact, and the service provider must enter the registered number or other register number into its records.

(5) For the purpose of verification of identity, service providers must check the validity of the identification documents mentioned under Subsection (3).

(6) In the process of verification of identity, in the case of agents service providers must check the validity of the power of attorney, and in the case of other authorized representatives the legal title of representation and the representative's entitlement.

(7) Where this is deemed necessary for the identification of the customer, the business relationship and the transaction order relying on the risk sensitivity approach, in the interest of the identification procedure and for the purpose of verification of identity, service providers shall be entitled - in addition to taking the measures defined in Subsections (2)-(6) - to verify personal identification information from publicly-accessible records or on the basis of registers the operator of which is required by law to supply information.

(8) In the interest of prevention and combating money laundering and terrorist financing, for the purpose of appropriate compliance with the obligations set out in this Act, for the full execution of due diligence obligations and for the effective implementation of supervisory activities, service providers shall make copies of documents presented in accordance with Subsection (3), containing the data referred to in Subsection (2) for the purpose of verification of identity.

(9) In order to ensure that data obtained in carrying out customer due diligence measures taken for the prevention and combating of money laundering and terrorist financing can be linked to player transactions, and for the effective implementation of supervisory activities, operators of casinos, card rooms shall be empowered to record the photographic images of natural person customers and to make video recordings of activities carried out in the casino or card room, and to keep such photographic images in storage in their electronic registers. Operators of casinos, card rooms shall keep such video recordings for forty-five days from the time of recording. The service provider affected shall extend that time limit when so requested by the supervisory body provided for in Section 5, until the conclusion of the supervisory body's proceeding.

(10) Service providers may implement the measures referred to in Subsections (2)-(6) hereof by way of the means specified by the supervisory body provided for in Section 5, via the service provider's safe, secure and previously audited electronic means of communication.

(11) The supervisory body provided for in Section 5 shall issue guidelines for the implementation of Subsection (10).

Section 8

(1) In the case provided for in Subsection (1) of Section 6, the customer - if a natural person - is

required to provide a written statement - subject to the formal requirements set out by the service provider - by way of physical presence, or via the service provider's safe, secure and previously audited electronic means of communication by way of the means specified by the supervisory body provided for in Section 5, as to whether he is acting in the name or on behalf of the beneficial owner.

(2) In the statement provided for in Subsection (1) service providers must obtain to request the following particulars of the beneficial owner:

a) surname and forename;

b) surname and forename by birth;

c) nationality;

d) date and place of birth;

e) home address, or habitual residence in the absence thereof.

(3) In addition to the data specified in Subsection (2), service providers must obtain to request the customer to provide a statement declaring whether the beneficial owner is a politically exposed person. If the beneficial owner is a politically exposed person, the aforesaid statement must also indicate the specific Paragraph of Subsection (2) of Section 4 under which the beneficial owner is considered politically exposed.

(4) Where there is any doubt concerning the identity of the beneficial owner, the service provider shall request the customer to reconfirm the identity of the beneficial owner by means of another statement.

(5) The service provider shall take measures to verify the beneficial owner's identification data on the basis of documents presented, publicly-accessible records and registers or other similar registers the operators of which are required by law to supply information to the service provider.

Section 9

(1) In the case provided for in Subsection (1) of Section 6, the customer's authorized representative - if a legal person or an unincorporated organization - is required to provide a written statement - relying on the customer's accurate and up-to-date records - by way of physical presence, or via the service provider's safe, secure and previously audited electronic means of communication by way of the means specified by the supervisory body provided for in Section 5, identifying the legal person or unincorporated organization customer's beneficial owner. In the statement the service provider must obtain to request the following particulars of the beneficial owner:

a) surname and forename;

b) surname and forename by birth;

c) nationality;

d) date and place of birth;

e) home address, or habitual residence in the absence thereof;

f) the nature and extent of ownership interest.

(2) In addition to the data specified in Subsection (1), service providers must obtain to request the customer to provide a statement declaring whether the beneficial owner is a politically exposed person. If the beneficial owner is a politically exposed person, the aforesaid statement must also indicate the specific Paragraph of Subsection (2) of Section 4 under which the beneficial owner is considered politically exposed.

(3) Where there is any doubt concerning the identity of the beneficial owner, the service provider shall request the customer to reconfirm the identity of the beneficial owner by means of

another statement.

(4) The service provider shall take measures to verify the beneficial owner's identification data on the basis of documents presented, publicly-accessible records and registers, or other similar registers the operators of which are required by law to supply information to the service provider.

(5) The customer's statement referred to in Subsection (1) may be omitted under the risk sensitivity approach, if the service provider recorded the data specified in Subsections (1) and (2) based on the documents presented and on publicly-accessible records and registers, or other similar registers the operators of which are required by law to supply information to the service provider.

(6) In the case provided for in Subsection (5) the service provider shall indicate that the data specified in Subsections (1) and (2) had been recorded in the absence of the customer's statement provided for in Subsection (1).

Section 10

(1) In the case provided for in Subsection (1) of Section 6, the service provider shall record the following information pertaining to the business relationship and the transaction:

a) regarding business relationships, the type, subject matter and the term of the contract;

b) regarding transactions, the subject matter and the value of the transaction;

c) the particulars of the execution (place, time, mode).

(2) Apart from the data provided for in Subsection (1), the service provider may also request - under the risk sensitivity approach - information about the source of funds, as well as documentary evidence for the purpose of verification of information disclosed relating to the source of funds.

(3) Under the risk sensitivity approach, the service provider may render the establishment of business relationships, the execution of transactions conditional upon the approval of its director specified in the internal policy provided for in Section 65.

(4) Service providers may implement the measures referred to in Subsections (1)-(2) also by way of the means specified by the supervisory body provided for in Section 5, via the service provider's safe, secure and previously audited electronic means of communication.

Section 11

(1) In accordance with the applicable legislation, service providers shall conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information the service provider has in its possession on the customer in accordance with the relevant regulations.

(2) Under the risk sensitivity approach, service providers may conduct ongoing monitoring of the business relationship under Subsection (1) hereof in the strengthened procedure provided for in the internal policy referred to in Section 65.

(3) Under the risk sensitivity approach, service providers shall pay special attention to all complex and unusual patterns of transactions and financial operations.

(4) Under the risk sensitivity approach, the service provider provided for in Paragraph *i)* of Subsection (1) of Section 1 shall monitor the activity of a customer executing a financial transaction amounting to two million forints or more within one calendar or game day in the strengthened procedure.

Section 12

(1) Service providers shall ensure that data and documents held in accordance with Sections 7-10 in connection with a customer and the business relationships are kept up-to-date.

(2) In order to meet the obligation provided for in Subsection (1), under the risk sensitivity approach, but at least every five years, service providers shall review the data and information available on a customer. If based on the findings of the review the service provider has concerns regarding the up-to-dateness of the data and statements, the customer due diligence measures shall be repeated.

(3) During the life of the business relationship, the customer is required to notify the service provider concerning any change in the data and information supplied for the purposes of due diligence or those concerning the beneficial owner within five working days of the day when such information is received.

(4) In order to meet the obligation set out in Subsection (3), the service provider shall advise its customers in writing concerning their obligation to report any and all changes in their particulars.

(5) Where there is no movement of any kind in an account maintained by a service provider provided for in Paragraphs *a)-d)* of Subsection (1) of Section 1 over a period of two calendar years, apart from arrangements that take several years to mature, the service provider shall request the customer in writing or by way of the means fixed in the contract - within thirty days - to report the changes in his particulars, advising that no transactions will be executed on the account before the identification data is disclosed.

Section 13

(1) Save as provided in Subsections (2)-(6), service providers are required to ensure that verification of the identity of the customer and the beneficial owner takes place before the establishment of a business relationship or the carrying out of the transaction.

(2) Service providers may be allowed to carry out the verification of the identity of the customer and the beneficial owner during the establishment of a business relationship if necessary so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing. In such situations those procedures for the verification of the identity of the customer shall be completed before the first transaction is carried out.

(3) In the case of insurance policies within the field of life insurance under Annex 2 to the Insurance Act, in addition to the customer due diligence measures required for the customer and the beneficial owner, insurance companies shall, before establishing the business relationship:

a) in the case of beneficiaries that are identified in the contract as specifically named persons, or any person entitled to receive benefits from the insurance company under insurance contract, take the name of the person; and

b) in the case of beneficiaries that are not identified in the contract as specifically named persons, or any person entitled to receive benefits from the insurance company under insurance contract, obtain sufficient information for subsequent identification.

(4) In the case of beneficiaries of insurance policies within the field of life insurance under Annex 2 to the Insurance Act, or any person entitled to receive benefits from the insurance company under insurance contract that are not identified in the contract as specifically named persons, the verification of the identity of the beneficiaries or person entitled to receive benefits from the insurance company under insurance contract shall take place at the time of the payout at the latest or at the time of the exercise by the beneficiary of its rights stemming from the contract

(policy).

(5) The service providers entitled to provide payment account services, and those authorized to open client accounts, securities accounts and safe custody accounts may open such accounts if the conditions set out by law are satisfied, provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer, the customer's agent, proxy and other authorized representative until the completion of the verification of the identity of the customer and the beneficial owner.

(6) Voluntary mutual insurance funds may open an individual account governed under Act XCVI of 1993 on Voluntary Mutual Insurance Funds (hereinafter referred to as "VMIFA") if the conditions set out by law are satisfied, provided that there are adequate safeguards in place to ensure that no services are provided to the customer and the service beneficiary until the completion of the verification of the identity of the customer and the beneficial owner. In the event of the member's death, the service provider shall identify the death beneficiary, or the heir, to whom payment is made before executing the transaction. Institutions for occupational retirement provision may open a membership account governed under Act CXVII of 2007 on Occupational Retirement Pension and Institutions for Occupational Retirement Provision (hereinafter referred to as "OPA") if the conditions set out by law are satisfied, provided that there are adequate safeguards in place to ensure that no services are provided to the member, annuitant and the beneficiary until the completion of the verification of the identity of the member and/or the beneficial owner.

(7) Fiduciary managers shall obtain sufficient information for subsequent identification and verification of identity in the case of beneficiaries that are not identified in the contract as specifically named persons. In that case, verification of identity shall take place at or before the time of payout or at or before the time the beneficiary intends to exercise rights stemming from the contract.

(8) Where the service provider is unable to comply with the customer due diligence measures specified in Sections 7-10, it may not carry out an operation through a payment account, establish a business relationship or carry out the transaction order, or shall terminate the business relationship with the customer in question.

(9) If the customer is a legal person or unincorporated organization, following completion of the customer due diligence procedures concerning a person acting in its name or on its behalf, due diligence procedures shall also be carried out concerning the legal person or unincorporated organization in question.

(10) The customer due diligence measures specified in Sections 7-10 need not be carried out again where:

a) the service provider has already completed the customer due diligence procedures specified in Sections 7-10 relating to the customer, the customer's agent, proxy or other authorized representative in connection with other business relationships or transaction orders;

b) the service provider has already carried out the verification of the identity of the customer, the customer's agent, proxy or other authorized representative in connection with prevailing business relationships or transactions in accordance with Subsections (2)-(6) of Section 7; and

c) no changes have taken place in the particulars listed under Subsection (2) of Section 7, Subsections (2) and (3) of Section 8 and Subsections (1) and (2) of Section 9.

Section 14

(1) The service providers specified in Paragraphs *a)-d)* of Subsection (1) of Section 1, with the

exception of credit institutions and currency exchange offices in the case of currency exchange services - for the purpose of prevention and combating money laundering and terrorist financing - shall record the data provided for in Subparagraphs *aa)* and *ad)* of Paragraph *a)* of Subsection (2) of Section 7 if the customer is a natural person, or in Subparagraphs *ba)* and *bb)* of Paragraph *b)* of Subsection (2) of Section 7 if the customer is a legal person or unincorporated organization, and also the data provided for in Paragraph *b)* of Subsection (1) of Section 10, and may request the documents referred to in Subsection (3) of Section 7 to be presented when carrying out an occasional transaction that amounts to less than three million six hundred thousand forints.

(2) By way of derogation from Subsection (1) hereof, service providers engaged in the activity referred to in Paragraph *g)* of Point 28 of Section 3 - for the purpose of prevention and combating money laundering and terrorist financing - shall record the data provided for in Subparagraphs *aa)* and *ad)* of Paragraph *a)* of Subsection (2) of Section 7 when making a cash deposit that amounts to less than three hundred thousand forints, above and beyond the premium due under the contract, or in Subparagraphs *ba)* and *bb)* of Paragraph *b)* of Subsection (2) of Section 7 if the customer is a legal person or unincorporated organization, and also the data provided for in Paragraph *b)* of Subsection (1) of Section 10, and may request the documents referred to in Subsection (3) of Section 7 to be presented.

(3) By way of derogation from Subsection (1) hereof, the institution operating the Posta Elszámoló Központ (*Postal Clearing Center*) referred to in Point 25 of Section 3 - for the purpose of prevention and combating money laundering and terrorist financing - shall record the data provided for in Subparagraphs *aa)* and *ad)* of Paragraph *a)* of Subsection (2) of Section 7 when carrying out an occasional transaction - with the exception of the supply of goods or services initiated and carried out in Hungary in an amount below three hundred thousand forints, or payment made to a payment account for the purpose of taxes, fines, duties, or in Subparagraphs *ba)* and *bb)* of Paragraph *b)* of Subsection (2) of Section 7 if the customer is a legal person or unincorporated organization, and also the data provided for in Paragraph *b)* of Subsection (1) of Section 10, and may request the documents referred to in Subsection (3) of Section 7 to be presented.

(4) The service providers specified in Paragraphs *e)-h)*, *j)-k)* and *m)* of Subsection (1) of Section 1, for the implementation of the obligations specified in Subsection (2) of Section 6, shall record the data provided for in Subparagraphs *aa)* and *ad)* of Paragraph *a)* of Subsection (2) of Section 7 if the customer is a natural person, or in Subparagraphs *ba)* and *bb)* of Paragraph *b)* of Subsection (2) of Section 7 if the customer is a legal person or unincorporated organization, and also the data provided for in Paragraph *b)* of Subsection (1) of Section 10, and may request the documents referred to in Subsection (3) of Section 7 to be presented when carrying out an occasional transaction that amounts to three hundred thousand forints or more.

5. Simplified customer due diligence

Section 15

(1) In the cases provided for in the internal policy referred to in Section 65, service providers are required to carry out the customer due diligence measures specified in the internal policy and in Subsection (1) of Section 11, and - where this is deemed necessary for the identification of the customer, the business relationship and the transaction order with a view to the prevention and combating of money laundering and terrorist financing - shall record the data specified in

Subsection (2) of Section 7 and may request the documents specified in Subsection (3) of Section 7 to be presented for the purpose of verification of identity.

(2) Service providers may implement the measures referred to in Subsection (1) hereof also by way of the means specified by the supervisory body provided for in Section 5, via the service provider's safe, secure and previously audited electronic means of communication.

(3) Service providers are required to carry out the customer due diligence measures specified in Subsection (1) of Section 11, and - for the identification of the customer, the business relationship and the transaction order with a view to preventing and combating money laundering and terrorist financing - may record the data specified in Subsection (2) of Section 7 and may request the documents specified in Subsection (3) of Section 7 to be presented for the purpose of verification of identity with respect to the issue of electronic money, if:

a) the cash-substitute payment instrument on which electronic money is stored is not reloadable, or reloadable but it has a maximum monthly payment transactions limit of sixty-five thousand forints, which can be used only in the territory of Hungary;

b) the maximum amount of electronic money stored electronically does not exceed sixty-five thousand forints;

c) the electronic money can be used exclusively to purchase goods or services;

d) the payment instrument cannot be funded with anonymous electronic money, where the customer has not been identified; and

e) the electronic money issuer carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual transactions, or information, fact or circumstance giving rise to a suspicion of money laundering or terrorist financing.

(4) Service providers shall carry out all customer due diligence measures under Sections 7-10 in the case of redemption in cash or cash withdrawal by the electronic money holder of the monetary value of the electronic money where the amount redeemed exceeds twenty-five thousand forints.

6. Enhanced customer due diligence

Section 16

(1) Service providers shall apply enhanced customer due diligence measures:

a) in the cases referred to, or when taking the measures provided for, in Sections 17-21;

b) when dealing with customers established in third countries identified as having strategic deficiencies or as high-risk third countries;

c) in the cases provided for in the internal policy referred to in Section 65.

(2) In the cases provided for in Paragraph *a)* of Subsection (1) hereof, service providers shall apply the enhanced customer due diligence measures provided for in Sections 17-21 in addition to the customer due diligence measures specified in Sections 7-11.

(3) In the cases provided for in Paragraphs *b)* and *c)* of Subsection (1) hereof, service providers shall apply the enhanced customer due diligence measures provided for in the internal policy referred to in Section 65.

Section 17

(1) For the purposes of identification and verification of identity, service providers shall require

customers to submit to the service provider certified copies of the documents provided for in Subsection (3) of Section 7 containing the data specified in Subsections (2) of Section 7, if the customer, authorized representative, agent or proxy has not been physically present for identification purposes and for the verification of his identity.

(2) Certified copies of the documents referred to in Subsection (1) shall be accepted for the verification of the identity of the customer if:

a) it has been certified by a notary public or by a Hungarian foreign mission in accordance with the relevant provisions of Act XLI of 1991 on Notaries Public (hereinafter referred to as "NPA") on the attestation of certification of copies, or

b) the copy was prepared by an authority of the country where it was issued, if such authority is empowered to make certified copies and - unless otherwise provided for by an international agreement - the competent Hungarian foreign mission has provided a confirmatory certification of the signature and seal of the said authority.

(3) Requesting a certified copy of the document referred to in Subsection (1) hereof may be omitted, if the service provider applies the enhanced customer due diligence measures provided for in the internal policy referred to in Section 65.

(4) The enhanced customer due diligence measures provided for in Subsection (3) must also be suited beyond any doubt for the identification of the customer and the beneficial owner and for the verification of their identity, and for recording information pertaining to the business relationship and the transaction order in accordance with Sections 7-10, and with the guidelines issued by the supervisory body.

(5) Service providers may implement the measures referred to in Subsections (3)-(4) hereof also by way of the means specified by the supervisory body provided for in Section 5, via the service provider's safe, secure and previously audited electronic means of communication.

(6) For the opening of a client account and a securities account provided for in Point 130 and Point 46 of Subsection (1) of Section 5 of the CMA, respectively, and for the opening of a safe custody account, for the verification of identity the customer shall have the option to submit the documents specified in Subsection (3) of Section 7, as well as the statement provided for in Sections 8 and 9 by way of electronic means - such as in particular by way of email scanned in - or by way of fax, when there is no information, fact or circumstance giving rise to suspicion of money laundering or terrorist financing. In that case, for the purpose of opening the account the customer may likewise supply evidence by way of electronic means or by way of fax of having a payment account, from which or to which payments will be made to or from the client account (hereinafter referred to as "verified payment account"). A verified payment account shall be accepted only if maintained by a service provider specified in Subsection (1) of Section 22. Before the customer appears in person for the purpose of identification and for the verification of identity, or before the documents specified in Subsections (1) and (2) are submitted, with the exception of the settlement of transactions where the client account, securities account or safe custody account is involved only payments made by simple transfer and only in respect of client accounts opened in accordance with this Subsection may be carried out, where deposits shall be accepted only from the customer's verified payment account and payments shall be made only to the customer's same verified payment account.

(7) The service provider where the client account, securities account and safe custody account is opened shall request proof - by way of disclosing the data it has recorded according to Subsection (6) and customer's natural identification data for the purpose of verifying the customer's identification data - from the service provider where the verified payment account is opened that the procedure for identifying the customer has been completed in connection with the

verified payment account, and that the data and information supplied by the customer relating to the client account, securities account and safe custody account are true and correct. The requested service provider shall comply with the request within eight days. If the customer has no payment account at the requested service provider, the service provider in question shall delete the data received upon the data request from the service provider where the client account, securities account and safe custody account is maintained immediately upon compliance with the data request.

Section 18

(1) Service providers provided for in Paragraphs *a)* and *b)* of Subsection (1) of Section 1 are required, before establishing correspondent relationships with a foreign-registered service provider, to:

a) conduct an in-depth analysis for assessing and evaluating the foreign-registered service provider's anti-money laundering and anti-terrorist financing controls;

b) be satisfied that the foreign-registered service provider has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to monitor access to the said accounts of the correspondent on an ongoing basis; and

c) be satisfied that the foreign-registered service provider is able to provide relevant customer due diligence data to the correspondent institution, upon request.

(2) Establishing a correspondent relationships with a foreign-registered service provider must be approved in advance by the director of the service provider provided for in Paragraphs *a)* and *b)* of Subsection (1) of Section 1 specified in the internal policy provided for in Section 65.

(3) Service providers provided for in Paragraphs *a)* and *b)* of Subsection (1) of Section 1 are prohibited to engage in or continue a correspondent relationship with a shell bank or with a service provider that has a correspondent relationship with a shell bank.

(4) Service providers provided for in Paragraphs *a)* and *b)* of Subsection (1) of Section 1 shall determine under the risk sensitivity approach whether it will the enhanced customer due diligence measures provided for in Subsections (1)-(2) before establishing a new correspondent relationships with a service provider established in any Member State of the European Union.

Section 19

(1) The customer - if a natural person - is required to provide a written statement by way of physical presence, or via the service provider's safe, secure and previously audited electronic means of communication by way of the means specified by the supervisory body provided for in Section 5, as to whether he is considered politically exposed. If the natural person customer is a politically exposed person, the statement must also indicate the specific Paragraph of Subsection (2) of Section 4 under which the customer is considered politically exposed.

(2) If a natural person customer is considered politically exposed, the statement must also indicate - in addition to the data specified in Subsection (1) - information as to the source of funds.

(3) The service provider must take measures to check the statement submitted under Subsection (1) in records and registers which are available for such purpose under the relevant legislation or which are made publicly available.

(4) In respect of establishing business relationships or executing transaction orders in the case

of politically exposed persons, prior approval by the service provider's director specified in the internal policy provided for in Section 65 is required.

(5) Service providers shall conduct ongoing monitoring under Subsection (1) of Section 11 of the business relationship with a politically exposed person in the strengthened procedure provided for in the internal policy referred to in Section 65.

(6) The customer's statement referred to in Subsection (1) may be omitted if the service provider recorded the data specified in Subsections (1) and (2) based on the documents presented and on publicly-accessible records and registers, or other similar registers the operators of which are required by law to supply information to the service provider.

(7) In the case provided for in Subsection (6) the service provider shall indicate that the data specified in Subsections (1) and (2) had been recorded in the absence of the customer's statement provided for in Subsection (1).

Section 20

(1) In the case of insurance policies within the field of life insurance under Annex 2 to the Insurance Act, the customer is required to provide a written statement by way of physical presence, or via the service provider's safe, secure and previously audited electronic means of communication by way of the means specified by the supervisory body provided for in Section 5, as to whether the beneficiary, or any person entitled to receive benefits from the insurance company under insurance contract, and the beneficial owner thereof is considered politically exposed. If the beneficiary, or the person entitled to receive benefits from the insurance company under insurance contract is a politically exposed person, the statement must also indicate the specific Paragraph of Subsection (2) of Section 4 under which the customer is considered politically exposed.

(2) The customer shall have the option to make the statement referred to in Subsection (2) after establishing the business relationship. In that case, the statement shall be made at or before the time of payout or at or before the time of assignment of the insurance policy in part or in whole.

(3) Where there is any doubt concerning the veracity of the statement made under Subsection (1), the service provider must take measures to check the statement in records and registers which are available for such purpose under the relevant legislation or which are made publicly available.

(4) In respect of politically exposed persons, a business relationships may be established after the service provider's director specified in the internal policy provided for in Section 65 is duly informed.

(5) Service providers shall conduct ongoing monitoring under Subsection (1) of Section 11 of the business relationship with a politically exposed person in the strengthened procedure provided for in the internal policy referred to in Section 65.

(6) The customer's statement referred to in Subsection (1) may be omitted if the service provider recorded the data specified in Subsection (1) based on the documents presented and on publicly-accessible records and registers, or other similar registers the operators of which are required by law to supply information to the service provider.

(7) In the case provided for in Subsection (6) the service provider shall indicate that the data specified in Subsection (1) had been recorded in the absence of the customer's statement provided for in Subsection (1).

Section 21

(1) With regard to any transaction for the exchange of money involving a sum amounting to three hundred thousand forints or more, credit institutions and currency exchange offices shall be required to carry out the identification procedure with respect to all of the data listed under Subsection (2) of Section 7 and to verify the identity of the customer, authorized representative, agent or proxy, and to carry out the customer due diligence measures specified in Sections 8-10.

(2) The transaction document shall contain the data specified in Subparagraphs *aa)* and *ag)* of Paragraph *a)* and in Subparagraphs *ba)* and *bb)* of Paragraph *b)* of Subsection (2) of Section 7.

(3) The customer due diligence obligation provided for in Subsection (1) shall also apply to any series of related transactions if the total value thereof reaches three hundred thousand forints. In this case, due diligence measures shall be carried out in connection with the transaction order the acceptance of which brings the total value thereof to three hundred thousand forints.

7. Customer due diligence measures carried out by other service providers

Section 22

(1) Service providers shall be authorized to accept the outcome of customer due diligence procedures provided for in Sections 7-10 if carried out:

a) by a service provider established, or having a branch or business establishment in the territory of Hungary or any Member State of the European Union; or

b) by a service provider established, or having a branch or business establishment in the territory of a third country that meets the conditions laid down in Subsection (3).

(2) In the case under Subsection (1), as regards compliance with the requirements set out in Sections 7-10, the ultimate responsibility for the customer due diligence procedure remains with the service provider that has accepted the outcome of the customer due diligence procedure carried out by another service provider.

(3) If the customer due diligence procedure carried out by a service provider established, or having a branch or business establishment in the territory of a third country, the outcome thereof may be accepted under Subsection (1) if:

a) the service provider applies customer due diligence requirements and record keeping requirements as laid down or equivalent to those laid down in this Act, and compliance is supervised in accordance with provisions laid down or equivalent to those laid down in this Act, or

b) the service provider's registered office, branch or business establishment is situated in a third country which imposes equivalent requirements to those laid down in this Act.

(4) Service providers shall not be authorized to accept the outcome of customer due diligence procedures provided for in Sections 7-10 if carried out by a service provider established, or having a branch or business establishment in the territory of a third country identified as having strategic deficiencies or as a high-risk third country.

(5) The prohibition defined in Subsection (4) hereof shall not apply where the outcome of customer due diligence procedures provided for in Sections 7-10 carried out by a branch or subsidiary of a service provider established in the territory of Hungary or in any Member State of the European Union is accepted, if such branch or subsidiary is located in a third country identified as having strategic deficiencies or as a high-risk third country, if that branch or subsidiary comply with the group-wide policies and procedures in accordance with Section 62.

Section 23

(1) In the case under Subsection (1) of Section 22, the service provider shall be authorized to make available to other service providers data and information obtained for the purposes of due diligence measures provided for in Sections 7-10 subject to the prior consent of the customer affected.

(2) In the case under Subsection (1) of Section 22 and if the conditions set out in Subsection (3) of Section 22 are satisfied, if the service provider that has carried out the customer due diligence measures and the service provider accepting the outcome of customer due diligence procedures have agreed on sharing the outcome of customer due diligence measures, the service provider that has carried out the customer due diligence measures shall forthwith make available - at the written request of the service provider accepting the outcome of customer due diligence procedures - data obtained for the purposes of verification of the identity of the customer or the beneficial owner, and copies of other relevant documents on the identity of the customer or the beneficial owner to the service provider accepting the outcome of customer due diligence procedures subject to the prior consent of the customer affected.

Section 24

Sections 22 and 23 shall not apply to outsourcing and agency relationships entered into on the basis of a contractual arrangement. As regards the outcome of customer due diligence measures provided for in Sections 7-10, in terms of availability and acceptance, the outsourcing service provider and the agent is to be regarded as part of the service provider.

8. Central register of beneficial ownership information

Section 25

(1) Service providers shall forward data on the beneficial owners of legal persons and unincorporated organizations, and also of fiduciary managers immediately after it is recorded and verified in accordance with Section 9 to the central register established for the purpose of data storage under the relevant legislation, provided such data is not contained in that central register.

(2) The financial intelligence unit, investigating authorities, the anti-terrorist organization, national security services, public prosecutors and the courts shall have direct unrestricted access to request data from the central register referred to in Subsection (1), the supervisory body provided for in Section 5 in order to perform its tasks delegated under this Act, as well as for the purpose of carrying out the customer due diligence measures provided for in Sections 7-12.

(3) Third persons may request data from the central register referred to in Subsection (1) - excluding data specified in this Act on the beneficial owners of fiduciary managers - on a case-by-case basis to the extent strictly necessary in order to achieve the objective of use, if:

a) able to verify the objective for which the data will be used and if able to produce documentary evidence so as to demonstrate a legitimate interest with a view to combating money laundering and terrorist financing, and

b) it is necessary for the enforcement of their rights and legitimate interest, and

c) able to meet the conditions prescribed by the law on setting up the central register.

(4) Having access to such information may not bring unreasonable harm to the personality

rights or upon the privacy of the person affected by the data disclosure.

(5) By way of derogation from Subsections (2) and (3) hereof, the right of access of service providers - other than the ones provided for in Paragraphs *a)-e)* and *l)* of Subsection (1) of Section 1 - and third persons to the central register referred to in Subsection (1) hereof may be restricted fully or partially, on a case-by-case basis in exceptional circumstances, if:

a) allowing access to the beneficial owner's data would expose the beneficial owner to the risk of the commission of a criminal offence against his person or property,

b) the beneficial owner is a minor or otherwise incapable.

(6) Detailed provisions on holding the data and information specified in Section 9 on the beneficial ownership of legal persons or unincorporated organizations are contained in the legislation on the central register of beneficial ownership information.

9. Information accompanying transfers of funds

Section 26

(1) The Authority, and with respect to the MNB the financial intelligence unit shall function as the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions provided for in Articles 8 and 12 of the Regulation.

(2) At the Member State level, the Authority and the financial intelligence unit shall function as the competent authority responsible in the field of anti-money laundering and counter terrorist financing provided for in Article 14 of the Regulation.

(3) Service providers shall disclose to the authorities referred to in Subsection (2) acting in their vested official capacity concerning information on the payer and the payee provided for in Article 4 of the Regulation for the purposes specified in Article 14 of the Regulation.

(4) Service providers shall hold information on the payer and the payee provided for in Article 4 of the Regulation in accordance with Sections 57 and 58.

(5) The Authority, and with respect to the MNB the financial intelligence unit shall function as the competent authority provided for in Article 17(4) and (7) and Articles 19-22 of the Regulation.

(6)[3] The Authority shall carry out the supervisory procedure in due observation of the provisions of the Act on General Public Administration Proceedings, subject to the exceptions set out in Act CXXXIX of 2013 on the National Bank of Hungary (hereinafter referred to as "MNB Act"), furthermore, the financial intelligence unit shall act in accordance with the Act on General Public Administration Proceedings.

(7) In the event of any infringement of the provisions of the Regulation or inadequate compliance with the obligations set out in the Regulation, the Authority shall take the measures specified under Subsection (1) of Section 69, consistent with the gravity of the infringement, and shall prohibit the service provider from engaging in the provision of transfer of funds services before the infringement is terminated.

(8) The fine referred to in Paragraph *h)* of Subsection (1) of Section 69 may be imposed upon any service provider for non-compliance with the Regulation and with the provisions contained in resolutions adopted by the Authority, and for partial or late compliance with the said provisions.

(9) In the event of any infringement of the provisions of the Regulation or non-compliance with

[3] Amended by Subsection (1) of Section 94 of same Act.

the obligations set out in the Regulation, the financial intelligence unit shall take the measures specified under Paragraphs *a)* and *b)* of Subsection (1) of Section 69 consistent with the gravity of the infringement.

(10) In the event of any infringement of the provisions of the Regulation or non-compliance with the obligations set out in the Regulation, the Authority and the financial intelligence unit shall proceed in accordance with Subsections (6) and (7) of Section 69 with respect to legal persons and unincorporated organizations.

(11) In the event of any infringement of the provisions of the Regulation or non-compliance with the obligations set out in the Regulation service providers shall report to the Authority and the financial intelligence unit as provided for in Section 72.

(12) In the cases under Article 2(5), Article 5(2), Article 6(2) and Article 7(3) and (4) of the Regulation, the amount transferred shall be translated to euro based on the official exchange rate quoted by the MNB in effect on the day when the transfer order in question is received, or by the exchange rate published in the MNB Bulletin for the conversion of currencies that are not quoted by the MNB to euro in effect on the day when the transfer order in question is received.

(13) Service providers are not required to apply the provisions of the Regulation with respect to transfer of funds services carried out in Hungary that are in compliance with Article 2(5) of the Regulation.

10. Risk assessment

Section 27

(1) Service providers are required to conduct internal risk assessment relating to discharging their functions conferred in this Act based on the nature of the business relationship or on the type and value of the transaction order and on the customer's circumstances, including the products, services and the means employed. Those steps shall be proportionate to the nature and size of the service provider.

(2) In conducting the internal risk assessment referred to in Subsection (1), service providers shall take appropriate steps to identify and assess the risk factors relating to the nature of the business relationship or the type and value of the transaction, their customers, products, services, geographic areas and the means employed.

(3) The risk assessments conducted by the service providers as referred to in Subsection (1) shall be documented, kept up-to-date and made available to the competent authorities in exercising their licensing and regulatory activities.

(4) Conducting the internal risk assessments may not be required where this possibility is provided by the supervisory body provided for in Section 5 in the guidelines made available to service providers.

(5) Relying on the outcome of the internal risk assessment provided for in Subsection (1), service providers shall have in place internal procedures to mitigate and manage the risks, based on the nature of the business relationship or on the type and value of the transaction and on the customer's circumstances relating to their products, services and the means employed, provided for in the internal policy referred to in Section 65. Those steps shall be proportionate to the nature and size of the service provider.

(6) In conducting the internal risk assessment referred to in Subsection (1), and to mitigate and manage the risks, service providers shall make use of the findings of national risk assessment.

(7) The internal risk assessment provided for in Subsection (1) and the internal procedure referred to in Subsection (5) hereof may be used subject to prior approval by the service provider's director specified in the internal policy provided for in Section 65.

(8) Service providers obliged to prepare internal risk assessment shall monitor risks of money laundering and terrorist financing, review the internal procedures if deemed necessary and take steps to modify it subject to prior approval by the service provider's director specified in the internal policy provided for in Section 65.

Section 28

(1) In carrying out the supervisory activity provided for in Section 66, the supervisory body provided for in Section 5 shall conduct supervisory risk assessment based on the nature and size of the service provider or the sector, or on the service provider's or sector's circumstances, including the customers, the products, services and the means employed. Those steps shall be proportionate to the nature and size of the service provider.

(2) The supervisory body provided for in Section 5 shall identify the risks of money laundering and terrorist financing taking into account risk factors specific to service providers or sectors including those relating to their customers, products, services and the means employed, making use of all the information available pursuant to Section 27.

(3) In conducting the supervisory risk assessment referred to in Subsection (1) hereof the supervisory body provided for in Section 5 shall make use of the findings of national risk assessment.

(4) In carrying out the supervisory activity provided for in Section 66, the supervisory body provided for in Section 5 shall draw up a supervisory protocol - taking into account the findings of supervisory risk assessment - based on the nature and size of the service provider or the sector, and on the service provider's or sector's circumstances relating to their customers, products, services and the means employed. Those steps shall be proportionate to the nature and size of the service provider.

(5) The supervisory body provided for in Section 5 shall monitor changes in risks of money laundering or terrorist financing identified in the risk assessment of the sector it supervises, identify risks which has not yet been identified, and shall update its risk assessment accordingly.

Section 29

The minister in charge of the money, capital and insurance markets (hereinafter referred to as "Minister") shall inform the Commission and the Member States of the results of coordinated national risk assessment.

11. Reporting obligations

Section 30

(1) The directors, employees of service providers and their contributing family members shall report without delay any information, fact or circumstance giving rise to a suspicion:

a) of money laundering,

b) of terrorist financing, or

c) that specific property is derived from criminal activity,

that is to be reported (hereinafter referred to collectively as "information, fact or circumstance relevant for reporting") to the person designated under Subsection (1) of Section 31 (hereinafter referred to as "reporting").

(2) The report made in accordance with Subsection (1) shall contain:

a) the data and information the service provider has recorded pursuant to Sections 7-14;

b) detailed description of the information, fact or circumstance relevant for reporting; and

c) documents supporting the information, fact or circumstance relevant for reporting, if available.

(3) Directors and employees of service providers and their contributing family members shall examine the occurrence of information, fact or circumstance giving rise to suspicion of money laundering, terrorist financing or that specific property is derived from criminal activity in connection with transactions already carried out or pending, including transactions initiated by the customer but not yet executed, and also in the case provided for in Subsection (8) of Section 13.

Section 31

(1) Service providers shall, depending on the structure of the organization, in particular its size and the number of management level, appoint one or more persons (hereinafter referred to as "compliance officer") to forward without delay to the financial intelligence unit the reports received from the directors and employees of service providers and their contributing family members. The compliance officer must be a director or employee of the service provider, or their contributing family member.

(2) Service providers are required to notify the financial intelligence unit concerning the appointment of the compliance officer, including the name, position and contact information of such officer, and the date of starting such activity, as well as any subsequent changes therein, within five working days of the date of the effective date of the change.

(3) The person appointed under Subsection (3) shall dispatch the report in the service provider's name to the financial intelligence unit in the form of a secure electronic message, and the financial intelligence unit shall confirm receipt of the report in the form of an electronic message sent to the reporting service provider without delay.

Section 32

(1) Until the report referred to in Subsection (1) of Section 31 is dispatched as provided for in Subsection (3) of Section 31 the service provider shall refrain from carrying out the transaction.

(2) Where refraining from carrying out the transaction referred to in Subsection (1) is impossible, or filing the report before the transaction is executed is likely to frustrate efforts to pursue the beneficiary, the compliance officer shall dispatch the report in the service provider's name pursuant to Subsection (3) of Section 31 after carrying out the transaction.

Section 33

Disclosure of information in good faith by a director or employee of a service provider, including their contributing family members and the compliance officer (hereinafter referred to collectively as "reporting person") shall not constitute a breach of any restriction on disclosure of

information imposed by legislative provision or by contract, and shall not invoke civil or criminal liability even in circumstances where the report ultimately proves to be unfounded.

Section 34

(1) The service provider shall suspend the execution of a transaction if any information, fact or circumstance relevant for reporting arises, where in the service provider's opinion immediate action by the financial intelligence unit is considered appropriate for investigating such information, fact or circumstance. In that case, the service provider shall without delay report to the financial intelligence unit to investigate the cogency of the report.

(2) Suspending a transaction as under Subsection (1) may be executed by the suspension of all other transactions with respect to services provided to the customer involving transactions to the debit of the customer's assets. In that case the service provider shall bring it to the attention of the financial intelligence unit in the report dispatched pursuant to Subsection (1).

(3) When so requested by the authority provided for in Subsection (1) of Section 48, the financial intelligence unit shall be empowered to order service providers in writing to carry out certain suspended transactions specified by the financial intelligence unit - during the period of suspension - for reasons of prevention, detection or investigation of criminal activities.

(4) The service provider shall carry out a suspended transaction upon receipt of notice from the financial intelligence unit in accordance with Paragraph *b)* of Subsection (4) of Section 35, or after the suspension following the expiry of the time limits specified in Subsections (2) and (3) of Section 35 in the absence of a notice from the financial intelligence unit.

(5) As regards the suspension of transactions, service providers shall comply with the guidelines issued by the supervisory body provided for in Section 5.

Section 35

(1) Upon receipt of written notice from the financial intelligence unit, service providers shall suspend the execution of transactions as instructed by the financial intelligence unit concerning any information, fact or circumstance relevant for reporting connected to the transaction or related to the service provider's customer.

(2) The financial intelligence unit shall check the information, fact or circumstance relevant for reporting within four working days from the time when the report provided for in Subsection (1) of Section 34 was dispatched, or after the date of the notice referred to Subsection (1) hereof, or whether the transmission of information under Subsection (1) of Section 48 is appropriate.

(3) The financial intelligence unit shall have power to extend the period of the investigation referred to in Subsection (2) hereof by an additional three working days if deemed appropriate for the transmission of information under Subsection (1) of Section 48.

(4) The financial intelligence unit shall inform the service provider in writing within the time limit prescribed in Subsection (2):

a) concerning the extension of the investigation as under Subsection (3);

b) if the transaction can be carried out before the investigation of the financial intelligence unit is completed.

Section 36

The service provider and the financial intelligence unit - if acting in good faith - shall not be

subject to civil or criminal liability for the suspension of the execution of a transaction in accordance with Subsection (1) of Section 34 or Subsection (1) of Section 35 if it ultimately proves to be unsubstantiated, and the transaction can be carried out pursuant to Subsection (4) of Section 34.

Section 37

(1) If the supervisory body provided for in Section 5 obtains any information, fact or circumstance relevant for reporting during its regulatory proceedings, it shall notify the financial intelligence unit thereof without delay.

(2) If the customs authority obtains any information, fact or circumstance relevant for reporting in the process of inspection of goods and passengers passing through the customs border, it shall notify the financial intelligence unit thereof without delay.

12. Financial intelligence unit

Section 38

(1) The financial intelligence unit shall perform analysis and assessment with a view to combating money laundering and terrorist financing, and for the purpose of prevention, detection and investigation of criminal activities, including operational and strategic analyses.

(2) The financial intelligence unit shall function as a department of the Nemzeti Adó- és Vámhivatal (*National Tax and Customs Authority*) and shall operate independently within the scope of its duties delegated by this Act.

Section 39

The financial intelligence unit shall perform operational analysis for the purpose of transmission of information under Subsection (1) of Section 48 and Subsection (1) of Section 49 in connection with any information, fact or circumstance relevant for reporting. In the operational analysis the financial intelligence unit shall:

a) compare the information received in accordance with Section 40 taking into account the risks identified by the national risk assessment and the data processed for the purpose of analysis and assessment, and shall conduct risk analyses in the form of an automated procedure;

b) compare the information obtained under this Act, and under Act XLVIII of 2007 on the Implementation of Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community (hereinafter referred to as "Cash Control Act"), the databases for which it has direct access, public information and data made available to the general public, and the data made available pursuant to this Act, and shall identify and define any connection that may exist between them;

c) monitor financial transactions and processes connected to the data referred to in Paragraph *a)*, and shall examine business relationships and transaction orders;

d) decide on the need to execute the provisions set out in Subsection (3) of Section 34, Subsection (4) of Section 35, Sections 42-44 and in Section 46;

e) decide on the steps to be taken within the framework of international exchange of information and cooperation provided for in Section 49;

f) make statements and draw conclusions in the interest of transmission of information under Subsection (1) of Section 48.

Section 40

An operational analysis will be carried out:

a) upon receipt of a report from a service provider;

b) upon receipt of notice from a service provider regarding the suspension of a transaction referred to in Subsection (1) of Section 34;

c) upon receipt of information from the supervisory body provided for in Section 5, or from the customs authority under Subsection (2) of Section 37;

d) upon receipt of a request from the authorities referred to in Subsection (1) of Section 48 for the information provided for in Subsection (4) of Section 48;

e) based on the information transmitted by the customs authority in accordance with Subsection (3) of Section 4 of the Cash Control Act;

f) based on the data request by the body responsible for the implementation of the order for the freezing of assets provided for in the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests, and by the body responsible for the implementation of restrictive measures relating to the transfer of funds, or upon their disclosure of information, fact or circumstance relevant for reporting;

g) based on the various forms of international exchange of information and cooperation with a foreign financial intelligence unit provided for in Subsection (1) of Section 49.

Section 41

(1) The financial intelligence unit shall perform strategic analysis addressing money laundering and terrorist financing trends and patterns.

(2) The financial intelligence unit may decide to send information to the bodies listed in Subsection (1) of Section 48, and to the supervisory bodies provided for in Section 5 about the results of strategic analyses, provided that the body in question is entitled by law for processing such data, and it is required for exercising its powers or for carrying out its tasks.

Section 42

(1) In carrying out the operational analysis, the financial intelligence unit shall have access to, and shall have the right to process any and all data from the service providers' records to the extent required for the performance of its tasks, including payment, insurance, bank, securities and fund secrets, occupational retirement secrets and trade secrets.

(2) In carrying out the operational analysis, the financial intelligence unit may contact service providers requesting access to the data and secrets referred to in Subsection (1) to the extent necessary for the performance of its tasks. The requested service provider shall comply and disclose the data and secrets requested to the financial intelligence unit.

(3) Service providers shall respond fully and speedily to inquiries from the financial intelligence unit through secure channels.

Section 43

(1) To the extent required for the performance of its tasks in carrying out the operational analysis, the financial intelligence unit shall have access to, and shall have the right to process data from the central government agency, the courts and the supervisory body provided for in Section 5, including tax secrets and customs secrets.

(2) The requested central government agency, the court and the supervisory body provided for in Section 5 shall make available to the financial intelligence unit the data and secrets referred to Subsection (1) as requested by the financial intelligence unit in carrying out the operational analysis.

Section 44

(1) To the extent required for the performance of its tasks in carrying out the operational analysis, the financial intelligence unit shall have access to, and shall have the right to process data from investigating authorities, public prosecutor's offices, the national security service, and internal affairs division that investigates professional misconduct and criminal acts and the anti-terrorist organization defined by the Act on the Police.

(2) In carrying out the operational analysis, the financial intelligence unit may request data from the bodies referred to in Subsection (1). Except for the case under Subsection (4), the requested body may not refuse the disclosure of such data.

(3) Apart from the data requested under Subsection (2), the financial intelligence unit shall have direct access to the database of the investigating arm of the NAV for obtaining data to the extent required for carrying out the operational analysis. Direct access shall be provided by the investigating arm of the NAV.

(4) In exceptional cases, the head of the requested body may refuse to comply with the data request made under Subsection (2), or may refuse to provide direct access under Subsection (3) if:

a) such data disclosure or provision of direct access

aa) is likely to jeopardize the success of ongoing investigations or covert information gathering operations,

ab) is considered harmful to national security;

b) disclosure is against an international agreement;

c) with respect to any data received from a foreign secret service, the foreign secret service in question did not consent for the disclosure of such data; or

d) the Member State participating in the international joint investigation team or anti-crime unit did not consent for the disclosure of such data.

(5) As regards the sharing of data disclosed with any organization mentioned in Subsection (1) of Section 48 and in Subsection (1) of Section 49 of this Act, the head of the requested body referred to in Subsection (2) shall be entitled:

a) to prohibit it;

b) to restrict it;

c) to render it subject to prior consent.

Section 45

(1) The financial intelligence unit shall be entitled to set a time limit of minimum eight and maximum thirty days for compliance with the data requests made under Section 42, Section 43 and Subsection (2) of Section 44. The requested body shall comply with the data request or shall

communicate the reason for non-compliance within the prescribed time limit.

(2) During the period of suspension provided for in Subsection (1) of Section 34 and Subsection (1) of Section 35, the financial intelligence unit may - in justified cases - reduce the time limit referred to in Subsection (1) hereof for compliance with the data requests made under Section 42, Section 43 and Subsection (2) of Section 44.

(3) In the requests made under Section 42, Section 43 and Subsection (2) of Section 44, the financial intelligence unit shall specify the specific types of data and the reason for which they are requested.

(4) If the request made by the financial intelligence unit involves personal data, it shall be limited to such personal data which are deemed absolutely necessary for the purposes of the request in terms of quantity and type.

Section 46

(1) In carrying out the operational analysis, the financial intelligence unit shall have power to initiate proceedings falling within the competence of the central government agency, for which it shall supply the data and information deemed necessary for opening and conducting the proceedings, and which the body conducting the proceedings is authorized to process. The central government agency requested to open the proceedings shall send feedback to the financial intelligence unit regarding the use of information received, or - if the proposed proceedings were in fact opened - on the outcome of the proceedings immediately after the proceedings are concluded by final decision.

(2) In carrying out the operational analysis, the financial intelligence unit may decide to send information that may be necessary for proceedings falling within the competence of the supervisory body provided for in Section 5, or the court of registry, and shall disclose data which the body conducting the proceedings is authorized to process.

(3) The supervisory body provided for in Section 5, and the court of registry shall send feedback to the financial intelligence unit regarding the use of information received by 31 March of the year following the given year.

Section 47

The financial intelligence unit may use the data and secrets obtained under Sections 42-44 and 46 solely for the purposes defined in Subsection (1) of Section 48 and Subsection (1) of Section 49, and only within the framework of its operational analysis provided for in Section 39.

Section 48

(1) The financial intelligence unit may disclose the findings of its operational analysis exclusively for the purpose of combating money laundering and terrorist financing, and for the purpose of prevention, detection or investigation of criminal activities, to:

a) the investigating authorities;

b) the public prosecutor’s office;

c) the court;

d) the national security services;

e) the internal affairs division that investigates professional misconduct and criminal acts and the anti-terrorist organization defined by the Act on the Police.

(2) The financial intelligence unit may supply data to the body responsible for the implementation of the order for the freezing of assets for discharging its duties delegated by the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests.

(3) The financial intelligence unit shall keep the data contained in the data transfer records maintained under Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information for a period of twenty years from the time of transmission of data.

(4) The authorities listed in Subsection (1) may request data and information from the data processing systems of the financial intelligence unit to the extent required for discharging their respective duties delegated by law, with the reason indicated.

(5) The authorities provided for in Subsections (1) and (2) shall send feedback to the financial intelligence unit about the use made of the findings of the operational analysis, including the outcome of the investigations or inspections performed on the basis of that information, and - if available - the description of the basic penal offense.

(6) As regards the information the financial intelligence unit has received pursuant to Subsection (1) of Section 49, and forwarded under Subsection (1) hereof, it shall be entitled:

a) to prohibit;

b) to restrict;

c) to render subject to prior consent;the use of such information for the purpose of compliance with Subsection (1) of Section 53.

Section 49

(1) The financial intelligence unit may on its own accord participate in international exchange of information and cooperation with foreign financial intelligence units with a view to combating money laundering and terrorist financing and to facilitating the prevention, detection or investigation of criminal activities, and also with Europol in accordance with the Act on the International Cooperation of Law Enforcement Authorities.

(2) The international exchange of information and cooperation referred to in Subsection (1) shall apply even if the type of predicate offenses that may be involved is not identified at the time of the exchange of information.

(3) In accordance with Financial Action Task Force recommendations and the guidances of the Egmont Group, the financial intelligence unit shall conduct international exchange of information and cooperation through protected channels of communication.

(4) The financial intelligence unit shall conduct international exchange of information and cooperation in due observation of Financial Action Task Force recommendations and the directives of the Egmont Group.

(5) The financial intelligence unit shall have authority to enter into a cooperation agreement with a foreign financial intelligence unit where this is deemed necessary to facilitate the process of exchanging information and cooperation under Subsection (1).

Section 50

(1) In accordance with Section 49, in performing its analysis and assessment function, the financial intelligence unit may send requests to foreign financial intelligence units and to the Europol.

(2) The request covers all facts and information which are considered material for combating

money laundering or terrorist financing, including the related data of natural and legal persons and unincorporated organizations, to the extent strictly necessary for the activities of the foreign financial intelligence unit, or for providing an effective reply to the request. The request shall specify the grounds for the request and how the information sought will be used.

(3) If the financial intelligence unit plans to send a request pursuant to Section 42 to a service provider that provides services in Hungary, however, it is not established, and does not have a business establishment or branch in Hungary, the financial intelligence unit shall send the request to the financial intelligence unit of the Member State where the service provider is established, or has a business establishment or branch.

Section 51

(1) In accordance with Section 49, in performing its analysis and assessment function, the financial intelligence unit may send information to foreign financial intelligence units and to the Europol.

(2) The information shall contain the data provided for in Subsection (2) of Section 50 as appropriate. The information shall specify the reason for sending it and how the information sent should be used.

(3) If the financial intelligence unit receives a report or information in accordance with this Act or the Cash Control Act that concerns another Member State of the European Union, the financial intelligence unit shall notify the financial intelligence unit of that Member State without delay.

Section 52

(1) The financial intelligence unit shall have the option to forward information it has received within the framework of international exchange of information and cooperation in accordance with this Act or the Cash Control Act to the foreign financial intelligence unit and the Europol.

(2) The financial intelligence unit shall refuse to reply to a request made by a foreign financial intelligence unit for the exchange of information, including the related information, if:

a) to do so would harm Hungary's essential national security or law enforcement interests;

b) to do so is contrary to Hungarian law;

c) the information sought may be disclosed only if permitted by the holder of such information, and such consent is not available;

d) the information sought may be disclosed only if permitted by the foreign financial intelligence unit or the Europol, and such consent is not available.

(3) The financial intelligence unit shall not refuse international exchange of information and cooperation on the grounds that statutory provisions on tax crimes in the law of the other Member State of the European Union or of any third country differs from Hungarian law.

(4) The financial intelligence unit may impose restrictions or conditions relating to the use of information it has forwarded to a foreign financial intelligence unit.

(5) The financial intelligence unit shall grant consent for the foreign financial intelligence unit to disseminate the information transmitted to the competent foreign authorities promptly and to the largest extent possible. The financial intelligence unit may refuse to give consent only if:

a) it falls beyond the scope of application of this Act;

b) to do so would jeopardize the success of investigations;

c) it may be given only if permitted by the foreign financial intelligence unit, and such consent is not available;

d) it may be refused in accordance with Subsection (2), however, this was not known at the instant the information was transmitted;

e) there is a risk of serious harm to legitimate interests.

(6) The financial intelligence unit shall appropriately explain its refusal to grant consent.

Section 53

(1) The financial intelligence unit shall be allowed to use the information received within the framework of international exchange of information and cooperation only for the purpose for which it was sought or provided, or for which it was made available by the foreign financial intelligence unit in the information. Any use of the information for purposes beyond those originally approved, and any dissemination of that information shall be subject to the prior consent by the foreign financial intelligence unit providing the information.

(2) The financial intelligence unit shall be allowed to use the information received within the framework of international exchange of information and cooperation only for the purposes defined in this Act.

(3) The financial intelligence unit may use an information exchange mechanism that meets the requirement set out in Subsection (4) of Section 49, that, however, differs from the ones defined in Sections 50 and 51, with respect to the financial intelligence units of other Member States of the European Union, provided that the reason for using such mechanism is the acceleration or preparation of international exchange of information.

(4) A technology that has facilities for matching personal data with that of other financial intelligence units of other Member States of the European Union in an anonymous way by ensuring full protection and encryption of personal data shall also be considered applicable.

13. Prohibition of disclosure

Section 54

(1) The reporting person and the financial intelligence unit, and the service provider requested under Subsection (2) of Section 42 and Subsection (2) of Section 75, the authority requested pursuant to Subsection (2) of Section 43, the body responsible for the implementation of the order for the freezing of assets, and the requested body provided for in Sections 44 and 46 shall not disclose to the customer concerned or to other third persons, bodies the fact that a report has been filed, information has been transmitted, the contents of such information, on the analysis and assessment activity, the fact that the transaction has been suspended under Sections 34 and 35, the name of the reporting person, or whether any investigation is being carried out on the customer, and shall ensure that the filing of the report, the contents thereof, and the identity of the person filing the report remain confidential.

(2) The prohibition laid down in Subsection (1) shall not include disclosure to the supervisory body provided for in Section 5 by the reporting person, including the request made to the service provider under Subsection (2) of Section 42 and Subsection (2) of Section 75, to the body provided for in Subsection (2) of Section 43, Sections 44 and 46, or the disclosure of information under Subsection (2) of Section 41 and the dissemination of information mentioned in Sections 48 and 49.

(3) The prohibition laid down in Subsection (1) shall not apply to disclosure between the credit

institutions and financial institutions or between those institutions and their branches and majority-owned subsidiaries located in third countries, provided that those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures provided for in Section 62.

(4) The prohibition laid down in Subsection (1) hereof shall not prevent disclosure between service providers referred to in Paragraphs *g), h)* and *l)* of Subsection (1) of Section 1 from Member States, or from third countries which impose requirements equivalent to those laid down in this Act, who perform their professional activities within the same legal person or a network.

(5) The prohibition laid down in Subsection (1) hereof shall not prevent disclosure between service providers referred to in Paragraphs *a)-e), g), h)* and *l)* of Subsection (1) of Section 1 involving two or more service providers, provided:

a) that it is related to the same customer and the same transaction involving two or more obliged service providers;

b) that of the two or more service providers involved, at least one is engaged in activities governed by this Act, while the other service providers are situated in a Member State, or in a third country which imposes requirements equivalent to those laid down in this Act;

c) the service providers involved are engaged in the same activity listed under Subsection (1) of Section 1; and

d) the service providers involved are subject to obligations as regards professional secrecy and personal data protection equivalent to those laid down in Hungarian legislation.

Section 55

The restriction prescribed in Section 54 applies to access to the customers' data recorded in accordance with Sections 7-11, and to the data manager's compliance with customer requests for information concerning their personal data.

14. Data protection, records and statistical data

Section 56

(1) Directors, contributing family members and employees of service providers participating in the tasks delegated by this Act shall be able to access personal data in carrying out their obligations delegated under Sections 7-11 exclusively for the purposes of their activities performed with a view to combating and prevention of money laundering and terrorist financing, to the extent appropriate for such activities.

(2) Service providers shall be authorized to process personal data obtained in carrying out their obligations delegated under Sections 7-11 for a period of eight years after the end of the business relationship or after the date of carrying out the transaction order.

Section 57

(1) Service providers shall keep in their records and registers data, other than personal data, obtained in the process of discharging their obligations delegated under Sections 7-11, including data obtained during electronic identification and all other data and information related to business relationships for a period of eight years after the end of the business relationship or after

the date of carrying out the transaction order.

(2) Service providers are required to keep in their records and registers documents they have obtained in the process of discharging their obligations delegated under Sections 7-11, including copies of such documents, and data obtained during electronic identification, documents evidencing compliance with reporting and data disclosure requirements under Section 42 and the suspension of transactions according to Sections 34 and 35, including copies of such documents, and all other data and information related to business relationships, and their copies, for a period of eight years after the end of the business relationship or after the date of carrying out the transaction order.

(3) The service providers referred to in Paragraphs *a)-e)* and *l)* of Subsection (1) of Section 1 shall keep records of all cash transactions in the amount of three million six hundred thousand forints or more (whether in forints or any other currency) in the registers mentioned in Subsections (1) and (2) hereof for a period of eight years.

(4) Service providers shall delete or destroy the data and documents provided for in Section 56, and in Subsections (1)-(3) hereof, including their copies, immediately upon the expiry of the retention period.

Section 58

(1) By way of derogation from Subsection (2) of Section 56 and Subsections (1)-(3) of Section 57, service providers shall keep the data and documents therein provided for upon request by the supervisory body provided for in Section 5, the financial intelligence unit, the investigating authority, the public prosecutor's office or the court for the period specified in the request, not exceeding ten years from the end of the business relationship or after the date of carrying out the transaction order.

(2) The data retention period may be extended upon request made under Subsection (1) only if the data, document specified therein is necessary for an ongoing procedure or for a procedure to be launched in the future.

(3) After the final conclusion of the procedure referred to in Subsection (2), or if the procedure contemplated did not materialize, the service provider shall delete the data, document from its records. The authority mentioned in Subsection (1) shall forthwith inform the service provider affected on the final conclusion of the procedure referred to in Subsection (2), or if the procedure contemplated did not materialize.

(4) The financial intelligence unit and the supervisory body provided for in Section 5 shall keep any data, documents obtained in accordance with this Act for a period of ten years from the date when it was obtained.

Section 59

(1) The financial intelligence unit shall ensure - in cooperation with the supervisory bodies provided for in Section 5, investigating authorities, the Legfőbb Ügyészség (*Prosecutor General*) and the Országos Bírósági Hivatal (*National Office for the Judiciary*) - that it is able to review the effectiveness of its systems to combat money laundering or terrorist financing by maintaining comprehensive statistics on matters relevant to the effectiveness of such Hungarian systems.

(2) The statistics referred to in Subsection (1) shall include:

a) the number of reports received;

b) the number of transactions suspended pursuant to Sections 34 and 35, the number of cases

when the suspension was successful, showing also the sums thus secured broken down by currency type;

c) the number of cases for the freezing of assets in connection with terrorist financing under the Act on the Implementation of Restrictive Measures Imposed by the EU and the UN SC Relating to Liquid Assets and Other Financial Interests and the number of cases for the freezing of assets by court order, and the forint and euro value of the funds and economic resources frozen by court order;

d) the number of reports which the financial intelligence unit disseminated under Subsection (1) of Section 48 and Subsection (1) of Section 49, and the share of such reports among all reports received by the financial intelligence unit;

e) data regarding the number of requests and information the financial intelligence unit sent under Section 49 to foreign financial intelligence units for information, and the number of requests received from foreign financial intelligence units that were answered;

f) the number of criminal proceedings instituted based on suspicion of money laundering, acts of terrorism under Section 261 of Act IV/1978, or investigated for suspicion of acts of terrorism (Criminal Code, Sections 314-316), failure to report a terrorist act (Criminal Code, Section 317) and terrorist financing (Criminal Code, Section 318), showing separately the number of cases further investigated upon the transmission of information by the financial intelligence unit, as well as the number of cases that resulted in further investigation making use of the information transmitted by the financial intelligence unit, description of basic penal offenses and the method of the completion of the investigation;

g) in the criminal proceedings under Paragraph *f)*,

ga) the number of prosecutions and the number of persons prosecuted,

gb) the number of final judgments and the persons convicted;

h) the number of criminal cases provided for in Paragraph *f)* where any seizure of property took place, the value of the seized property, and the value of seized assets expressed in forints and euros, the number of cases where any property has been frozen and the value of the frozen assets expressed in forints and euros, the number of cases where any property has been seized or confiscated, the value of the property seized or confiscated, and the value of seized assets expressed in forints and euros, and the value of assets subject to confiscation of property expressed in forints and euros;

i) data measuring the size and importance of the different sectors which fall within the scope of this Act, recorded by the supervisory bodies provided for in Section 5.

(3) The investigating authorities and the Legfőbb Ügyészség shall supply information relating, respectively, to Paragraphs *f)* and *h)* of Subsection (2), Paragraph *f)*, Subparagraph *ga)* of Paragraph *g)* and Paragraph *h)* of Subsection (2), the Országos Bírósági Hivatal shall disclose information about the data concerning the freezing of assets under Paragraph *c)* of Subsection (2), the forint value of the funds and economic resources frozen by court order along with the information under Subparagraph *gb)* of Paragraph *g)* of Subsection (2), and the supervisory body provided for in Section 5 shall communicate the data referred to in Paragraph *i)* of Subsection (2) to the financial intelligence unit quarterly. The investigating authorities and the Legfőbb Ügyészség, the Országos Bírósági Hivatal and the supervisory body provided for in Section 5 may perform the disclosure of data by way of electronic means as well.

(4) Records of the data referred to in Paragraph *i)* of Subsection (2) shall be broken down according to profession.

(5) The financial intelligence unit shall publish comprehensive statistics collected in accordance with Subsection (2) on its website annually.

(6) The financial intelligence unit shall inform the European Commission at its request about the statistics provided for in Subsection (2) on a regular basis, via the Minister.

(7) The financial intelligence unit shall inform the service providers, the supervisory bodies provided for in Section 5 and the Minister concerning the success rate related to the reports and any proposals it may have to improve such success rate regularly, but at least annually.

15. Group-wide policies and procedures, actions in connection with branches and subsidiaries situated in other Member States of the European Union and in third countries

Section 60

(1) Service providers referred to in Subsection (1) of Section 1, that are part of the same group are required to implement policies and procedures at the group level (hereinafter referred to as "group-wide policies and procedures").

(2) Group-wide policies and procedures shall cover the protection of personal data obtained by the service providers in carrying out their obligations delegated under Sections 7-11, as well as compliance with reporting and data disclosure requirements under Section 42, including the contents thereof, the suspension of transactions according to Sections 34 and 35, the reporting person, including procedures for sharing information within the group relating to the reporting person and on any criminal proceedings which are pending or threatened against the customer.

Section 61

(1) Pursuant to Subsection (1) of Section 60, the service providers provided for in Subsection (1) of Section 1 shall ensure that the branches and subsidiaries they operate in another Member State of the European Union respect the national provisions of that other Member State against money laundering and terrorist financing.

(2) Service providers referred to in Paragraphs *a)* and *b)* of Subsection (1) of Section 1 that are established in other Member States of the European Union, who provide services in Hungary, however, they do not have a branch or subsidiary, are required to appoint a central contact point in Hungary to ensure compliance with anti-money laundering and anti-terrorist financing rules and to facilitate the implementation of supervisory measures prescribed in Section 68.

(3) Service providers shall implement measures in compliance with group-wide policies and procedures at the level of its branches and subsidiaries in other Member States of the European Union.

Section 62

(1) Where service providers have branches and subsidiaries located in third countries where the requirements are not equivalent to those set out in this Act, such service providers shall implement measures in accordance with this Act with respect to their branches and subsidiaries located in such third countries to the extent that the third country's law so allows.

(2) Service providers shall implement measures in compliance with group-wide policies and procedures at the level of its branches and subsidiaries located in third countries.

(3) Where a third country's law does not permit the implementation of the measures required

under Subsection (2), service providers shall forthwith inform the Minister thereof through the supervisory body.

(4) The Minister shall inform the Commission and the other Member States of cases where the legislation of the third country does not permit application of the measures equivalent to those required under Subsection (1).

(5) Where a third country's law does not permit the implementation of the measures equivalent to those required under Subsection (2), service providers shall ensure that branches and subsidiaries in that third country apply additional measures developed by European supervisory authorities in accordance with the guidelines approved by the European Commission, or in justified cases the supervisory body provided for in Section 5 may decide to apply such additional measures.

16. Internal control and information systems, training programs

Section 63

(1) Service providers - with respect to their employees participating in carrying out the activities provided for in this Act - shall have in place internal control procedures and information systems facilitating customer due diligence, reporting and record keeping for the purpose of preventing the establishment of business relationships and transactions which may be related to money laundering or terrorist financing.

(2) The system referred to in Subsection (1) shall have facilities to enable the service provider to respond fully and speedily to inquiries from the financial intelligence unit, the supervisory body provided for in Section 5 or from law enforcement agencies.

(3) Additionally, the internal control and information system provided for in Subsection (1) shall include appropriate internal procedures enabling the service providers' directors, employees and contributing family members to report any breaches of the provisions of this Act by the service provider through a specific, independent and anonymous channel, proportionate to the nature and size of the service provider concerned.

(4) The supervisory body provided for in Section 5 may issue guidelines for service providers under its supervision for the execution of the obligation prescribed in Subsection (1).

(5) Within five working days following the time of taking up the pursuit of their activities, service providers shall, depending on the structure of the organization, in particular its size and the number of management level, appoint one or more managers specified in the internal policy put in charge of monitoring the compliance of employees with the obligations stemming from this Act.

Section 64

(1) Service providers are required to take measures appropriate for their identified risks to ensure that their employees participating in carrying out the activities provided for in this Act are aware of the statutory provisions relating to the prevention and combating of money laundering and terrorist financing, that they are able to recognize operations, business relationships and transactions which may be related to money laundering or terrorist financing and to instruct them about the procedures to follow in accordance with this Act in cases when detecting information, facts or circumstances that may suggest money laundering or terrorist financing.

(2) Service providers are required to take appropriate measures to ensure that their employees participating in carrying out the activities provided for in this Act are aware of international and national provisions of law on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests, so that they are able to proceed in accordance with the provisions contained therein.

(3) In order to discharge the obligations set out in Subsections (1) and (2) hereof, service providers provided for in Subsection (1) of Section 1 are required to arrange training programs for their employees participating in carrying out the activities provided for in this Act.

(4) The supervisory body provided for in Section 5 may issue guidelines for service providers under its supervision for the execution of the obligation prescribed in Subsection (3).

17. Internal policies

Section 65

(1) Service providers shall have in place internal policies relating to discharging their functions falling within the scope of obligations provided for in this Act.

(2) The supervisory body provided for in Section 5 shall grant approval for the internal policy if found in compliance with the mandatory content requirements set out in this Act and in the decree implementing it, and if it is not contrary to any legislation and to the purpose of this Act.

(3) The supervisory body provided for in Section 5 shall provide guidelines for service providers under its supervision for drawing up the internal policy.

(4) Service providers shall review their internal policy after any amendment made in the relevant legislation, after changes in the guidelines issued by the supervisory body provided for in Section 5 or in its internal systems - including the internal risk assessment provided for in Section 27 - within thirty days, and shall make changes accordingly.

(5) The supervisory body provided for in Section 5 shall grant approval for the internal policy reviewed according to Subsection (4) hereof within the framework of supervisory procedures provided for in this Act for the first time after the review in accordance with the supervisory risk assessment, if found in compliance with the mandatory content requirements set out in this Act and in the decree implementing it, and if it is not contrary to any legislation and to the purpose of this Act.

(6) Traders in goods may undertake to discharge the obligations set out in this Act by submission of the internal policy to the authority of trade and commerce. The authority of trade and commerce shall grant approval for the internal policy and, at the same time, register the service provider in question. Only registered traders in goods shall be authorized to accept cash payments of two million five hundred thousand forints or more.

(7) In respect of discharging the responsibilities prescribed in this Act, the Office shall draw up uniform policies for fiduciary managers that shall be treated as the internal policies of providers of fiduciary asset management services in conformity with this Section. The Office shall review the uniform policies after any amendment adopted to this Act, or any changes in the risk assessment provided for in Section 27, and shall make amendments accordingly.

(8) The service providers listed under Paragraphs *a)-e)* and *i)* of Subsection (1) of Section 1 shall submit their internal policies for approval to the supervisory body provided for in Section 5 accompanied by the application for authorization in addition to satisfying the requirements set out by law.

(9) The service providers taking up the activities defined in Paragraphs *f)-h)* and *j)* of Subsection (1) of Section 1 shall be required to draw up their internal policies and submit it for approval to the supervisory body provided for in Section 5 within forty-five days following the commencement of operations.

(10) The service providers existing at the time of entry into force of this Act shall be required to draw up their internal policies in connection with their activities falling within the scope of this Act and submit it for approval to the supervisory body provided for in Section 5 within forty-five days following the entry into force of this Act for the purpose of approval.

18. Supervision, measures

Section 66

(1) The supervisory body provided for in Section 5 shall, in the process of exercising supervisory functions under this Act, monitor the compliance of service providers with the provisions of this Act in accordance with the law governing the activities of supervisory bodies, as provided for in Subsection (3).

(2) The supervisory activity provided for in Subsection (1) of the supervisory body provided for in Section 5 shall cover the service providers' compliance with international and national provisions of law on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests.

(3)[4] Subject to the exceptions set out in this Act, the supervisory bodies mentioned under Paragraphs *e)* and *f)* of Section 5 shall carry out their respective supervisory functions in accordance with the Act on General Public Administration Proceedings, the supervisory body mentioned under Paragraphs *a)* and *g)* of Section 5 shall carry out its supervisory functions in accordance with the Act on General Public Administration Proceedings and the MNB Act, the supervisory body mentioned under Paragraph *b)* of Section 5 shall carry out its supervisory functions in accordance with the Act on General Public Administration Proceedings and the Act on the Gambling Operations, and the supervisory body mentioned under Paragraph *c)* of Section 5 shall carry out its supervisory functions in accordance with the Act on the Chamber of Hungarian Auditors, the Activities of Auditors, and on the Public Oversight of Auditors and the Act on General Public Administration Proceedings. The supervisory bodies mentioned in Paragraphs *e)-g)* of Section 5 shall not apply the provisions of the Act on General Public Administration Proceedings on conditional decisions in administrative proceedings opened upon request in accordance with this Act.

(4) The supervisory body provided for in Subparagraph *da)* of Paragraph *d)* of Section 5 shall carry out its supervisory functions in accordance with Act XI of 1998 on Attorneys (hereinafter referred to as "Attorneys Act"), and the supervisory body provided for in Subparagraph *db)* of Paragraph *d)* of Section 5 shall proceed in accordance with the NPA.

Section 67

(1) In the process of exercising supervisory functions, the supervisory body provided for in Section 5 shall apply the findings of supervisory risk assessment performed under Section 28 and

[4] Amended by Subsection (1) of Section 94 of same Act.

shall adjust the frequency and extent of supervisory procedures provided for in this Act to the risks identified.

(2) The scope of supervisory activities provided for in Section 66 and in this Section carried out by the supervisory body provided for in Section 5 shall also cover the monitoring of internal risk assessment procedures and internal policies of service providers referred to in Section 27.

Section 68

(1) The supervisory body provided for in Section 5 shall, in the process of exercising supervisory functions under this Act, also monitor the compliance of Hungarian branches and subsidiaries of service providers established in other Member States of the European Union with the provisions of this Act.

(2) In carrying out its supervisory functions, the supervisory body provided for in Section 5 may apply the measures referred to in Section 69 for a transitional period as regards the central contact point provided for in Subsection (2) of Section 61, in exceptional circumstances such as in particular to address serious failings that require immediate remedies.

(3) In carrying out the supervisory measures referred to in Subsections (1) and (2) hereof, the supervisory body provided for in Section 5 shall cooperate with the supervisory body of the other Member State affected.

Section 69

(1) In the event of any infringement of the provisions of this Act or inadequate compliance with the obligations set out in this Act, the supervisory bodies mentioned in Paragraphs *a)*-*c)* and *e)*-*g)* of Section 5 shall have authority to take the following measures consistent with the gravity of the infringement:

a) issue a warning to the service provider;

b) order the service provider to cease the unlawful conduct within the prescribed time limit;

c) order the service provider to revise the internal policy within the time limit prescribed by the supervisory body according to specific criteria, and to present it to the supervisory body;

d) in the case of service providers referred to in Paragraphs *a)*-*e)*, *g)*, *i)* and *m)* of Subsection (1) of Section 1, the supervisory body shall - subject to certain legal restrictions - withdraw the activity or operating permits until the infringement is terminated, or shall suspend them;

e) in the case of service providers referred to in Paragraphs *j)* and *k)* of Subsection (1) of Section 1, the supervisory body shall delete the service provider from the register, in the case of service providers referred to in Paragraphs *f)* and *h)* of Subsection (1) of Section 1 it shall request the body operating the register to remove the service provider;

f) bring charges against the director of the service provider, or its employee or contributing family member for having their responsibility for the infringement established;

g) initiate that the director of the service provider be suspended from office or dismissed until the infringement is terminated;

h) in addition to or independent of the measures enumerated under Paragraphs *a)*-*i)*:

ha) impose a fine of not less than four hundred thousand forints upon the service providers referred to in Paragraphs *a)*-*c)* and *e)* of Subsection (1) of Section 1, and not more than 10 per cent of the annual net turnover shown in the annual account approved by the body entitled thereunto, or in the consolidated annual account, not exceeding two billion forints,

hb) impose a fine of not less than four hundred thousand forints upon the service providers

referred to in Paragraph *d)* of Subsection (1) of Section 1, and not more than 10 per cent of the revenue comprising the total of revenues from membership fees and aids received in the year preceding the given year, not exceeding two billion forints,

hc) impose a fine of not less than one hundred thousand forints upon the service providers referred to in Paragraphs *f)-k)* and *m)* of Subsection (1) of Section 1, and not more than four hundred million forints.

(2) If the amount of the proceeds from the infringement can be determined in the case under Subparagraph *hc)* of Paragraph *h)* of Subsection (1), and double of that amount exceeds four hundred million forints, the fine may be imposed up to double of such proceeds.

(3) If, in addition to any breach of the provisions of this Act, the supervisory body finds that international and national provisions of law on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests had also been breached, the amount of the fine shall be determined based on median of the fine. The median constitutes half of the sum of the lowest and highest fines to be imposed.

(4) If the supervisory body decided to impose a fine in the case under Subsection (3), the maximum amount of the fine shall be increased by the median, however it may not reach the combined total of the fines imposed for any breach of the provisions of this Act and the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests.

(5) In taking actions, the supervisory bodies mentioned in Paragraphs *a)-c)* and *e)-g)* of Section 5 shall take into consideration:

a) the gravity of the breach;

b) the intentional or negligent conduct by the persons responsible for the infringement;

c) the infringer's market share, where this is applicable with regard to the given service category;

d) the impact the infringement has on the service provider or on its customers;

e) the level of cooperation of the responsible parties with the supervisory body in question;

f) the duration, repeated occurrence or frequency of the infringement.

(6) The measures defined under Subsection (1) shall likewise be imposed upon a service provider where a director of the service provider - if a legal person or an unincorporated organization - has committed the infringement of the provisions of this Act for the benefit of the service provider.

(7) The measures defined under Subsection (1) shall likewise be imposed upon a service provider where an employee of the service provider or a contributing family member - if a legal person or an unincorporated organization - has committed the infringement of the provisions of this Act for the benefit of the service provider, and it could have been prevented by the appropriate supervision or control that is required of the director of the service provider.

(8)[5] The fine imposed under Paragraph *h)* of Subsection (1) shall be paid within thirty days from the date when it was communicated. At the service provider's request the supervisory body may authorize deferred payment or payment by installment for performance of the pecuniary claim (hereinafter referred to as "payment facilities"). The service provider ordered to pay the fine may submit an application for the authorization of payment facilities within five days from the date of communication of the resolution if compliance in due time proves impossible due to reasons beyond its control, or it would give rise to disproportionate difficulties for it. The service

[5] Enacted by Section 93 of same Act, effective as of 1 January 2018.

provider shall produce authentic proof for such circumstances, supported by documentary evidence.

Section 70

The supervisory bodies provided for in Section 5, in carrying out the supervisory activity, shall closely cooperate with each other, the financial intelligence unit, investigating authorities, the public prosecutor's office and the court, and also with supervisory bodies of other Member States and third countries.

Section 71

(1) The supervisory bodies provided for in Paragraphs *a)-c)* and *e)-g)* of Section 5 are required to publish a final and enforceable decision adopted in supervisory procedures provided for in this Act, including decisions enforceable irrespective of any appeal, on their website immediately after it was delivered to the service provider affected, containing inter alia data and information about the nature of the infringement or negligence, and also on the identity of the infringer.

(2) The supervisory bodies provided for in Paragraphs *a)-c)* and *e)-g)* of Section 5 shall be allowed to postpone compliance with the obligation of publication referred to in Subsection (1) hereof insofar as the underlying reason exists, if:

a) public disclosure of data and information on the infringer would cause disproportionate disadvantage to the person affected, having regard to the gravity of the infringement; or

b) it would jeopardize the sound and smooth functioning of the service sector referred to in Paragraphs *a)-e)* of Subsection (1) of Section 1; or

c) it would jeopardize the success of an ongoing procedure or a procedure to be launched in the future.

(3) The supervisory bodies provided for in Paragraphs *a)-c)* and *e)-g)* of Section 5 may be exempted from compliance with the obligation of publication referred to in Subsection (1) hereof if:

a) the postponement of publication is considered insufficient on the grounds specified in Subsection (2); or

b) it would be disproportionate based on the gravity of the infringement.

(4) Insofar as the reason under Paragraph *a)* of Subsection (2) thereof persists, by decision of the supervisory bodies provided for in Paragraphs *a)-c)* and *e)-g)* of Section 5 the obligation of publication may be satisfied without disclosing any data and information on the infringer, in a form granting anonymity.

(5) In the event of publication of the decisions declared enforceable irrespective of any appeal pursuant to Subsection (1) hereof, the information posted by the supervisory bodies provided for in Paragraphs *a)-c)* and *e)-g)* of Section 5 on their website at the time the decision became final shall include information about the outcome of the appeal process.

(6) The supervisory bodies provided for in Paragraphs *a)-c)* and *e)-g)* of Section 5 shall keep the information published in accordance with Subsection (1) hereof accessible for a period of five years from the date of publication.

Section 72

(1) The director, employee or contributing family member of a service provider, as well as the

customers (hereinafter referred to as “reporting person”), shall be entitled to notify the supervisory body provided for in Section 5 in writing - with name and address - where there is any suspicion of infringement of the provisions of this Act by a service provider (its director, employee or contributing family member) (hereinafter referred to as “report”).

(2) The supervisory body provided for in Section 5 shall investigate the report within thirty days from the date of receipt, and shall decide whether supervisory procedures provided for in this Act should be invoked ex officio, on the mode of investigation, or if supervisory procedures are considered unnecessary. If the reporting person sent the report to an entity other than the competent supervisory body, the supervisory body provided for in Section 5 shall transfer the report without delay to the body vested with competence and jurisdiction for carrying out the investigation.

(3) The supervisory body provided for in Section 5 shall notify the reporting person:

a) about its decision brought under Subsection (2) forthwith;

b) if the report has been transferred, at the time thereof.

(4) Examination of a report as to merits may be omitted if:

a) it was sent by the same person and it is identical to a report that was sent previously;

b) the reporting person sent the report to the supervisory body six months after gaining knowledge of the occurrence referred to in Subsection (1);

c) the reporting person failed to verify his credentials as required under Subsection (1);

d) the report is manifestly unfounded;

e) investigating the report is outside the scope of this Act;

f) the supervisory body has no competence and jurisdiction for investigating the report.

(5) The supervisory body provided for in Section 5 shall refrain from investigating a report received from a person who cannot be identified, except if - based on information available - the report reveals a serious infringement.

(6) The reporting person - if acting in good faith - shall not suffer any disadvantage in consequence of the report.

(7) The authority vested with competence for conducting the supervisory procedures provided for in this Act shall be exclusively permitted to process the personal data of the reporting person and the alleged infringer for the purpose of implementing obligations arising from this Section. The personal data of the person concerned may not be disclosed to unauthorized third parties, and may not be published without the prior written consent of the data subject.

(8) Data related to the report, the ensuing investigation and the measures taken in consequence shall be retained for a period of five years from the last investigative measure or from the conclusion of the measure.

19. Derogations relating to lawyers and notaries public

Section 73

(1) The obligations of customer due diligence and reporting prescribed in this Act shall apply to attorneys - with the exception set out in Subsection (3) hereof - if they hold any money or valuables in custody or if they provide legal services in connection with the preparation and execution of the following legal acts in accordance with Subsection (1) of Section 5 of the Attorneys Act:

a) buying or selling any participation (share) in a business association or other economic

operator;

b) transfer of ownership of real estate property;

c) founding, operating or dissolving a business association or other economic operator;

d) conclusion of a fiduciary asset management contract or unilateral acts for the purpose of fiduciary asset management;

e) transfer of any movable property, in particular funds, financial instruments, without consideration.

(2) The customer due diligence and reporting requirements prescribed in this Act shall apply to notaries public - with the exception set out in Subsection (4) - if he provides safe custody services or if he conducts non-contentious civil procedure under the NPA in connection with the preparation and execution of the following legal acts:

a) buying or selling any participation (share) in a business association or other economic operator;

b) transfer of ownership of real estate property;

c) founding, operating or dissolving a business association or other economic operator;

d) conclusion of a fiduciary asset management contract or unilateral acts for the purpose of fiduciary asset management.

(3) The reporting obligation prescribed in this Act, and the obligation to respond to inquiries made by the financial intelligence unit as provided for in Subsection (3) of Section 75 shall not apply to attorneys:

a) in the event of obtaining any information, fact or circumstance relevant for reporting in connection with providing the defense in criminal proceedings or legal representation before a court - other than the court of registry - during any stage of such defense or representation or at any time thereafter;

b) in the event of obtaining any information, fact or circumstance relevant for reporting in connection with the defense or legal representation referred to in Paragraph *a)* while providing legal advice relating to the opening of such proceedings.

(4) The reporting obligation prescribed in this Act, and the obligation to respond to inquiries made by the financial intelligence unit as provided for in Subsection (3) of Section 75 shall not apply to notaries public:

a) in the event of obtaining any information, fact or circumstance relevant for reporting in connection with tutoring the parties while providing legal advice relating to the opening of such proceedings;

b) in connection with non-contentious proceedings, other than non-contentious civil actions under the NPA.

Section 74

(1) Attorneys and notaries public shall file their report with the regional bar association or regional branch, respectively. The employees of attorneys and notaries public (including assistant attorneys) shall file the report with the attorney or notary public who exercises employer’s rights, who shall forward that report forthwith to the regional bar association. Employees of law firms shall report to the person designated by the members’ meeting, who shall forward the report forthwith to the bar association with which the law firm is registered.

(2) The presidents of the regional bar associations and regional branches shall appoint a person to be responsible for promptly forwarding the reports received from the persons referred to in Subsection (1) to the financial intelligence unit. The regional bar associations and regional

branches are required to promptly notify the financial intelligence unit concerning the appointment of the compliance officer and also when the appointed compliance officer is replaced.

(3) With regard to law firms, the members' meeting may decide whether the obligations prescribed in Subsection (1) of Section 30 and in Sections 63 and 64 are to be fulfilled by the law firm or by the members.

Section 75

(1) To the extent required for the performance of its tasks in carrying out the operational analysis, the financial intelligence unit shall have access to, and shall have the right to process data from attorneys and notaries public, including privileged information held by the attorney or notary public.

(2) For the purpose of carrying out the operational analysis, the financial intelligence unit may contact attorneys and notaries public requesting access to the data and privileged information referred to in Subsection (1). The financial intelligence unit shall send the request via the compliance officer provided for in Subsection (2) of Section 74, and the compliance officer shall forward it to the requested attorney or notary public without delay.

(3) If the requested attorney or notary public holds the data, privileged information indicated in the request in connection with carrying out the activities specified in Subsections (1) and (2) of Section 73, or in consequence thereof, the attorney or notary public shall send the data, privileged information indicated in the request to the compliance officer within the time limit prescribed in Section 45, and the compliance officer shall forward it to the financial intelligence unit without delay.

(4) If the attorney or notary public holds the data, privileged information indicated in the request for reasons other than the activities specified in Subsections (1)-(2) of Section 73, or in consequence thereof, or holds the data, privileged information in connection with carrying out such activities, however, the exemption under Subsections (3)-(5) of Section 73 applies, the attorney or notary public shall be entitled to refuse to respond to the request. If refused to respond, the attorney or notary public shall forthwith notify the financial intelligence unit thereof by way of the means provided for in Subsection (3).

(5) Fulfillment of the reporting obligation by attorneys and notaries public, including their compliance with requests made by the financial intelligence unit shall not constitute a violation of the confidentiality requirements prescribed by law.

(6) In the application of this Act, notaries public shall not be subject to the obligation laid down in Subsection (2) of Section 3 of the NPA.

Section 76

(1) In respect of discharging the responsibilities prescribed in this Act, the Magyar Ügyvédi Kamara (*Hungarian Bar Association*) shall draw up uniform policies for individual lawyers and single-member law firms that shall be treated as the internal policies of individual lawyers and single-member law firms in conformity with Section 65.

(2) The Magyar Ügyvédi Kamara shall draw up standard policies in order to meet the obligation provided for in Subsection (3) of Section 65, in which to determine the contents of guidelines to be issued by regional bar associations.

(3) In respect of discharging the responsibilities prescribed in this Act, the Magyar Országos

Közjegyzői Kamara (*Hungarian Association of Notaries Public*) shall draw up guidelines for notaries public that shall be treated as the internal policies of notaries public provided for in Section 65.

(4) The Magyar Ügyvédi Kamara shall review the policies referred to in Subsections (1) and (2), and the Magyar Országos Közjegyzői Kamara shall review the guidelines referred to in Subsection (3) after any amendment adopted to this Act, and also after any changes are made in the risk assessment procedure provided for in Section 27, and shall make amendments accordingly.

20. Closing provisions

Section 77

(1) The Minister is hereby authorized to decree the mandatory layout of internal policies.

(2) The Minister is hereby authorized to decree, with regard to the service providers referred to in Paragraphs *f)* and *h)-k)* of Subsection (1) of Section 1:

a) the sets of rules for the preparation of risk assessments;

b) the detailed rules for the operation of the internal control and information systems;

c) the cases where simplified and enhanced customer due diligence procedure apply, and the rules for approval by the supervisory authority;

d) the minimum requirements relating to audited electronic means of communication, including their operation, the method of auditing, and for the execution of customer due diligence by such means;

e) the cases where strengthened procedures apply, and the relevant conditions;

f) the cases where decisions by management are required for establishing a business relationship or for carrying out a transaction order under the risk sensitivity approach;

g) the detailed rules for training programs;

h) the detailed rules for the suspension of transactions.

(3) The Governor of the Magyar Nemzeti Bank (*National Bank of Hungary*) is hereby authorized to decree, with regard to the service providers referred to in Paragraphs *a)-e)* and *m)* of Subsection (1) of Section 1:

a) the sets of rules for the preparation of risk assessments;

b) the detailed rules for the operation of the internal control and information systems;

c) the cases where simplified and enhanced customer due diligence procedure apply, and the rules for approval by the supervisory authority;

d) the minimum requirements relating to audited electronic means of communication, including their operation, the method of auditing, and for the execution of customer due diligence by such means;

e) the cases where strengthened procedures apply, and the relevant conditions;

f) the cases where decisions by management are required for establishing a business relationship or for carrying out a transaction order under the risk sensitivity approach;

g) the detailed rules for training programs;

h) the detailed rules for the suspension of transactions.

Section 78

(1) This Act - with the exception set out in Subsection (2) - shall enter into force on 26 June 2017.

(2) Sections 93-94 shall enter into force on 1 January 2018.

(3) Paragraph *m)* of Point 28 of Section 3 shall enter into force on 3 January 2018.

Section 79

By way of derogation from Subsection (7) of Section 13, service providers must refuse to carry out transactions following 26 June 2019:

a) for customers with whom the business relationship was established before 26 June 2017;

b) for customers whose due diligence measures had not been carried out by 26 June 2019; and

c) if the outcome of the customer due diligence requirements specified under Sections 7-11 and Sections 19-20 is not fully available on 26 June 2019.

Section 80

(1) The service providers existing at the time of entry into force of this Act shall be required to revise their internal policies within ninety days after the date of issue of the supervisory guidelines provided for in this Act, at the latest by 30 September 2017 in accordance with this Act, and shall notify in writing the supervisory body provided for in Section 5 that the internal policy had in fact been revised. The institution operating the Postal Clearing Center provided for in Point 25 of Section 3 shall meet that obligation within one hundred eighty days after the date of issue of the supervisory guidelines provided for in this Act, at the latest by 1 January 2018.

(2) The Magyar Ügyvédi Kamara (*Hungarian Bar Association*) shall draw up internal policies under this Act for individual lawyers and single-member law firms, and the Magyar Országos Közjegyzői Kamara (*Hungarian Association of Notaries Public*) shall draw internal policies for notaries public within forty-five days following the time of this Act entering into force.

(3) The Magyar Ügyvédi Kamara shall draw up standard policies in order to determine the contents of guidelines to be issued by regional bar associations within twenty days following the time of this Act entering into force.

(4) Traders in goods, if not listed in the register referred to in Subsection (6) of Section 65, shall be authorized to accept cash payments of two million five hundred thousand forints or more until 31 October 2017.

(5) The Office shall draw up uniform policies in accordance with this Act for fiduciary managers within forty-five days following the time of this Act entering into force.

Section 81

If the service provider notified the national financial intelligence unit about the compliance officer appointed under Subsection (3) of Section 23 of Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter referred to as “Act CXXXVI/2007”) before the entry into force of this Act, the information under Subsection (2) of Section 31 shall be provided in the case of any change in the person of the compliance officer or in his particulars referred to in Subsection (2) of Section 31. In that case, the functions of the compliance officer shall be carried out by the compliance officer appointed according to Subsection (3) of Section 23 of Act CXXXVI/2007 until the effective date of change in the person of the compliance officer.

21. Compliance with the Acquis

Section 82

(1) This Act serves the purpose of compliance with 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.

(2) This Act contains provisions for the implementation of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No. 1781/2006.

22. Amendments

Sections 83-92[6]

Sections 93-94[7]

Section 95[8]

[6] Repealed under Section 12 of Act CXXX of 2010, effective as of 27 June 2017.
[7] Repealed under Section 12 of Act CXXX of 2010, effective as of 2 January 2018.
[8] Repealed under Section 12 of Act CXXX of 2010, effective as of 27 June 2017.