

Act CXXXVI of 2007

on the Prevention and Combating of Money Laundering and Terrorist Financing

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 derived from the commitment of criminal acts through the financial system, the capital markets and other areas exposed to potential money laundering operations, as well as to help combat the flow of funds and other financial means used in financing terrorism.

In order to achieve the above objectives the Parliament has adopted the following Act:

Scope of the Act

Section 1

(1) With the exceptions set out in Subsections (3)-(5) this Act shall apply to persons who, in the territory of Hungary are:

- a) engaged in providing financial services or in activities auxiliary to financial services;
- b) engaged in providing investment services or in activities auxiliary to investment services;
- c) engaged in providing insurance services, insurance intermediary services or employer pension services;
- d) engaged in providing commodity exchange services;
- e) engaged in accepting and delivering domestic and international postal money orders;
- f) engaged in providing real estate agency or brokering and any related services;
- g) engaged in providing auditing activities;
- h) engaged in providing accountancy (bookkeeping), tax consulting services whether or not certified, or tax advisory activities under agency or service contract;
- i) operating a casino, a card room or engaged in organising online gambling;
- j) engaged in trading with precious metals or articles made of precious metals;
- k) engaged in trading in goods involving the acceptance of cash payments in the amount of three million six hundred thousand forints or more;
- l) operating as a voluntary mutual insurance fund;
- m) acting as lawyers or notaries public.

(2) This Act shall apply to:

- a) customers of service providers;
- b) executive officers, employees of service providers and their contributing family members.

(3) Service providers engaged in trading in goods may not, within the scope of these activities, accept any cash payment in the amount of three million six hundred thousand forints or more, unless they undertake to discharge the obligations conferred upon service providers by this Act in accordance with Subsection (4) of Section 33.

(4) This Act shall not apply to:

a) the activities of agents described in Point 12.2 of Chapter I of Schedule No. 2 to Act CXII of 1996 on Credit Institutions and Financial Enterprises (hereinafter referred to as the 'HptAct');

b) the dependant insurance intermediaries described in Subsection (4) of Section 33 of Act LX of 2003 on Insurance Institutions and Insurance Business (hereinafter referred to as the 'Insurance Act');

c) the independent insurance intermediaries described in Subsection (4) of Section 33 of the Insurance Act as regards their activities relating to the field of non-life insurance under Part A of Schedule No. 1 to the Insurance Act;

d) the insurance companies, if authorized to pursue only the activities relating to the field of non-life insurance under Part A of Schedule No. 1 to The Insurance Act, and the insurance companies authorized to engage in activities in the field of non-life insurance under Part A of Schedule No. 1 to the Insurance Act and at the same time in activities in the field of life assurance under Schedule No. 2 to the Insurance Act, as regards their activities relating to the field of non-life insurance.

(5) This Act shall not apply to the activity defined in Paragraph a) of Subsection (1), if carried out by the Central Bank of Hungary (hereinafter referred to as 'MNB'), with the exception of providing money transmission services under the provisions of Sections 2 and 22.

Section 2

Section 22 shall apply to the service providers, who:

a) are engaged in the activities referred to in Paragraphs a)-b) and e) of Subsection (1) of Section 1 of this Act; and

b) provide money transmission services within the territory of Hungary under Point 7 of Article 2 of Regulation (EC) No. 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds (hereinafter referred to as the 'Regulation').

Interpretative provisions

Section 3

For the purposes of this Act:

a) '*tax adviser, tax consultant, certified tax consultant*' shall mean any person, who has the qualifications described under specific other legislation, is authorized to engage in such activities, and is registered in the registry of tax advisers, tax consultants and certified tax consultants described under specific other legislation;

b) '*identification*' shall mean the recording in writing of the data specified in Subsections (2)-(3) of Section 7, and in Subsections (2)-(3) of Section 8;

c) '*European Union*' shall mean the European Union and the European Economic Area;

d) '*Member State of the European Union*' shall mean any Member State of the European Union and other States who are parties to the Agreement on the European Economic Area;

e) '*shell bank*' shall mean a service provider engaged in the activity defined in Paragraph a) of Subsection (1) of Section 1, incorporated in a jurisdiction in which it has no physical presence, and to which supervision on a consolidated basis shall not apply;

f) *'network'* shall mean the larger structure to which the service providers engaged in the activity defined in Paragraphs g)-h) and m) of Subsection (1) of Section 1 belong and which shares common ownership, management and compliance control;

g) *'third country'* shall mean any state that is not member of the European Union;

h) *'real estate agency or brokering'* shall mean the business of mediation of the transfer or lease of real estate properties, including the preparation of transaction orders, real estate appraisal, real estate investment and real estate development;

i) *'trading in goods'* shall mean the sale of goods by way of business to buyers, traders or processors;

j) *'accounting services'* shall mean the activities defined in Subsections (1)-(2) of Section 150 of Act C of 2000 on Accounting;

k) *'correspondent banking services'* shall mean the keeping of an account by a credit institution for an other credit institution for the purpose of performing orders of financial transaction services or of performing financial or investment services;

l) *'authority operating as the financial intelligence unit'* shall mean the unit of the National Tax and Customs Administration as defined in a legal regulation;

m) *'official certificate suitable for the proof of identity'* shall mean the personal identity card, passport, or driver's license in a card format;

n) *'verification of identity (verification)'* shall mean the procedure to verify the identity of the customer, the proxy, the authorized signatory and the representative, in accordance with the provisions of Subsections (4)-(6) of Section 7, and to verify the identity of the beneficial owner in accordance with the provisions of Subsection (5) of Section 8;

o) *'service provider'* shall mean the person or organization engaged in the activity referred to in Subsection (1) of Section 1;

p) *'executive officer of a service provider'* shall mean any natural person, who is entitled to represent a service provider whether being a legal person or an organization not having a legal personality, to exercise the power of taking decisions on behalf of this service provider, and to exercise the controlling power within this service provider;

q) *'individual transaction orders linked in effect'* shall mean:

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

qb) in the case of service providers engaged in currency exchange activities, transactions for which the customer places an order within a period of one week;

qc) as regards the service providers engaged in the activity referred to Paragraph k) of Subsection (1) of Section 1, instalment payments and payment orders performed on the basis of instalment purchase;

r) *'beneficial owner'* shall mean:

ra) the natural person, who directly or – in a manner specified in Subsection (3) of Section 685/B of Act IV of 1959 on the Civil Code (hereinafter referred to as 'Civil Code') – indirectly owns or controls at least twenty-five per cent of the shares or voting rights in a legal person or in an organisation not having a legal personality, if that legal person or organisation not having a legal personality is not a registered company on the regulated market to which publication requirements consistent with Community legislation or equivalent international requirements apply;

rb) the natural person, who has a dominant influence in a legal person or an organisation not having a legal personality as determined in Subsection (2) of Section 685/B of the Civil Code;

rc) the natural person, on whose behalf a transaction order is executed;

rd) in the case of foundations, the natural person:

1. who is the beneficiary of at least twenty-five per cent of the property of the foundation, if the future beneficiaries have already been determined;

2. in whose main interest the foundation is established or operates, if the beneficiaries have yet to be determined; or
3. who is a member of the managing organisation of the foundation, or who has a dominant influence over at least twenty-five per cent of the property of the foundation, or who acts on behalf of the foundation; and
 - re*) in the absence of a natural person specified in Subparagraphs ra)–rb), the executive officer of the legal entity or the organisation not having a legal personality;
 - s*) ‘*customer*’ shall mean
 - sa*) any person entering into a business relationship with a service provider in order to use any of the services falling within the scope of the activities described in Subsection (1) of Section 1, or who places an order with the service provider to carry out a transaction order;
 - sb*) as regards the service providers engaged in the activity referred to in Paragraph f) of Subsection (1) of Section 1, any person requesting for a proposal for the sale or purchase of a real estate;
 - t*) ‘*customer due diligence procedures*’ shall mean
 - ta*) in the cases referred to in Section 6, the carrying out of the customer due diligence measures specified under sections 7-10;
 - tb*) the register of the gambler referred to in Subsection (1) and (2) of Section 29/H of Act XXXIV of 1991 on the organising of gambling
 - u*) ‘*transaction order*’ shall mean the occasional contractual relationship based on a written agreement between a customer and a service provider pertaining to the services of the service provider falling within its professional activities;
 - v*) ‘*business relationship*’ shall mean:
 - va*) a long-term contractual relationship based on an agreement 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) Subsection (1) of Section 1;
 - vb*) the activities of a notary public concerning the procedure specified under Subsection (2) of Section 36;
 - vc*) as regards the service provider engaged in the activity referred to in Paragraph *i*) of Subsection (1) of Section 1, the long-term contractual relationship created when first entering the casino or card room and the registration of the gambler by the organiser of online gambling.
 - vd*) as regards the service providers engaged in the activity referred to in Paragraph f) of Subsection (1) of Section 1, legal relationship between the customer and the service provider pertaining to the services of the service provider falling within its professional activities.
 - w*) ‘*money laundering*’ shall mean the crimes specified 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 of 1978’) or in Sections 399-400 of Act C of 2012 on the Criminal Code (hereinafter referred to as ‘Criminal Code’);
 - x*) ‘*terrorist financing*’ shall mean the provision or collection of financial instruments required to commit a criminal act under Subsections (1) and (2) of Section 261 of Act IV of 1978 or the crimes specified in Section 318 of the Criminal Code;
 - y*) *foreign national financial intelligence unit*: the authority of a foreign country having – with special respect to the requirements of the Financial Action Task Force (FATF) and Egmont Group – the same or similar responsibilities as the authority operating as the financial intelligence unit.

Section 4

(1) For the purposes of this Act, ‘politically exposed persons’ shall mean natural persons residing in another Member State or in a third country who are or have been entrusted with prominent public functions within one year before the carrying out of customer due diligence measures, and immediate family members, or persons known to be close associates, of such persons.

(2) For the purposes of Subsection (1), ‘natural persons entrusted with prominent public functions’ shall include the following:

- a)* heads of the State, heads of the government, ministers, secretaries of state;
- b)* members of parliaments;
- c)* members of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal;
- d)* heads of courts of auditors, members of courts auditors, or of the highest decision-making body of central banks;
- e)* ambassadors, *chargés d’affaires* and members of the armed forces with Senior Officer rank, General position and General rank;
- f)* members of the administrative, management or supervisory bodies of State-owned enterprises of majority control.

(3) For the purposes of Subsection (1), close relative shall have the meaning set out in Paragraph *b)* of Section 685 of the Civil Code, including domestic partners.

(4) For the purposes of Subsection (1), persons known to be close associates of politically exposed persons shall include the following:

- a)* any natural person who is known to have joint beneficial ownership of a legal person or an organization not having a legal personality, 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 person or an organization not having a legal personality which is known to have been established for the benefit of the person referred to in Subsection (2).

Section 5

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

- a)* with respect to the service providers engaged in the activities referred to in Paragraphs *a)-e)* and *l)* of Subsection (1) of Section 1, with the exception set out in Paragraph *b)*, the Hungarian Financial Supervisory Authority (hereinafter referred to as ‘the Authority’);
- b)* with respect to the service providers engaged in cash processing operations of activities auxiliary to financial services referred to in Paragraph *a)* of Subsection (1) of Section 1, the MNB;
- c)* with respect to the service providers engaged in the activities referred to in Paragraph *i)* of Subsection (1) of Section 1, the state tax authority;
- d)* with respect to the service providers engaged in the activity referred to in Paragraph *g)* of Subsection (1) of Section 1, the Chamber of Hungarian Auditors;
- e)* with respect to the service providers engaged in the activity referred to in Paragraph *m)* of Subsection (1) of Section 1, in accordance with the special provisions set out in this Act pertaining to independent lawyers and law offices (hereinafter referred to as ‘lawyers’) and notaries public:
 - ea)* the competent regional bar association in which the lawyer in question is registered (hereinafter referred to as ‘regional bar association’);

eb) the competent regional chamber in which the notary public in question is registered (hereinafter referred to as ‘regional chamber’);

f) with respect to the service providers engaged in the activities referred to in Paragraphs *j)* and *k)* of Subsection (1) of Section 1, the trade licensing authority;

g) with respect to the service providers engaged in the activities referred to in Paragraphs *f)* and *h)* of Subsection (1) of Section 1, the authority operating as the financial intelligence unit.

The obligation of carrying out customer due diligence procedures

Section 6

(1) Service providers are required to apply customer due diligence procedures:

a) when establishing a business relationship;

b) with the exception set out in Section 11/A and in Section 17, when executing transaction orders amounting to three million six hundred thousand forints or more;

c) when there is any information, fact or circumstance indicating money laundering or terrorist financing, where the due diligence measures referred to in Paragraphs *a)-b)* have not been carried out yet;

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

(2) The obligation of carrying out the due diligence procedures specified in Paragraph *b)* of Subsection (1) shall also apply to individual transaction orders linked in effect, if their combined value reaches three million six hundred thousand forints or more. In this case, due diligence procedures shall be carried out at the time of acceptance of the transaction order the execution of which brings the combined value of the linked transaction orders to the threshold of three million six hundred thousand forints.

Customer due diligence measures

Section 7

(1) In the cases referred to in Subsection (1) of Section 6, service providers are required to identify the customer, the proxy, the authorised signatory and the representative, and to verify their identity.

(2) In the course of identification, service providers are required to record at least the following particulars of customers:

a) in connection with natural persons:

aa) surname and forename (birth name);

ab) address;

ac) nationality;

ad) type and number of identification document;

ae) in respect of foreign nationals, the place of abode in Hungary;

b) in connection with legal persons or organizations not having a legal personality:

ba) full name and abbreviated name;

bb) address of registered office or, in case of foreign-registered enterprises, the address of their branch office in Hungary;

bc) in the case of legal persons registered by the court of registration, the company registration number; in the case of other legal persons, the number of the resolution of their foundation (registration, incorporation) or their registration number.

(3) In addition to what is contained in Subsection (2), in the course of identification, service providers may record the following particulars of customers where it is deemed necessary for the identification of the customer, the business relationship and the transaction order, on the basis of the results of the procedure specified in the internal rules referred to in Section 33, based on the nature of the business relationship or on the type and value of the transaction order and on the customer's circumstances in the interest of preventing and combating money laundering and terrorist financing:

a) in connection with natural persons:

aa) place and date of birth;

ab) mother's name;

b) in connection with legal persons or organizations not having a legal personality:

ba) principal activity;

bb) name and position of authorised representatives;

bc) identification data of agent for service of process.

(4) For the purposes of verification of identity, service providers are required to require the following documents to be presented:

a) in connection with natural persons:

aa) for Hungarian nationals, an official certificate suitable for the proof of identity and an official certificate for the proof of address;

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

ac) [*no longer in effect*]

b) for legal persons or organizations not having a legal personality, in addition to the documents of the persons described in Paragraph *a*) who are authorized to act in their names and on their 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 registration or that the application for registration has been submitted; if a private entrepreneur, that he has a private entrepreneur's license, or the certificate of registration has been issued;

bb) in case of domestic legal persons whose existence is subject to registration by an authority or the court, the fact that the registration has taken place;

bc) in case of foreign-registered legal persons or organizations not having a legal personality, the fact that the person or body has been registered under the law of the country in which it is established;

c) prior the submitting of an application for company registration to the court of registration, or an application for registration by an authority or the court to the competent authority or court, the articles of incorporation (articles of association, charter document) of legal persons and organizations not having a legal personality.

(5) In the application of Paragraph *c*) of Subsection (4), the legal person or organization not having a legal personality is required to produce documentary evidence of having been registered by the court of registration, or the competent authority or court, within thirty days after the fact, and the service provider is required to enter the company registration number or registration number into its records.

(6) For the purposes of verification of identity, service providers are required to check the validity of identification documents presented on the basis of Subsection (4).

(7) During the verification of identity the service provider shall verify the validity of the letter of authorisation in the case of an authorised representative or the legal title of disposition in the case of a person with right of disposal, as well as the right of representation of the representative.

(8) For the purpose of the identification and the verification of identity, in the case referred to in Subsection (1) of Section 6 the service provider may, in addition to the measures set out in Subsections (2)–(7), verify the identity-related information in a publicly available register or in a register from whose manager it has statutory right to request data, where it is deemed necessary for the identification of the customer, the business relationship and the transaction order, on the basis of the results of the procedure specified in the internal rules referred to in Section 33 and based on the nature of the business relationship or on the type and value of the transaction order and on the customer's circumstances, with a view to the prevention and combating of money laundering and terrorist financing.

Section 8

(1) In the cases referred to in Subsection (1) of Section 6, the natural person customer is required to provide a written statement in the manner determined by the service provider as to whether he is acting in his own name or in the name or on behalf of the beneficial owner.

(2) If the natural person customer's written statement indicates that he is acting in the name or on behalf of the beneficial owner, the written statement shall contain the particulars of the beneficial owner specified in Subparagraphs *aa)*–*ac)* of Paragraph *a)* of Subsection (2) of Section 7.

(3) In the case set out in Subsection (1) of Section 6, the representative of the customer, who is a legal entity or an organisation not having a legal personality, shall make a written statement about the beneficial owner of the customer as a legal entity or an organisation not having a legal personality and about the data of the beneficial owner as specified in Subparagraph *aa)*–*ac)* of Paragraph *a)* of Subsection (2) of Section 7

(4) In addition to what is contained in Subsections (2)–(3), the service provider may request the customer to supply the particulars of the beneficial owner specified in Subparagraphs *ad)*–*ae)* of Paragraph *a)* of Subsection (2) and Paragraph *a)* of Subsection (3) of Section 7 where it is deemed necessary for the identification of the customer, the business relationship and the transaction order, on the basis of the results of the procedure specified in the internal rules referred to in Section 33 and based on the nature of the business relationship or on the type and value of the transaction order and on the customer's circumstances, with a view to the prevention and combating of money laundering and terrorist financing.

(5) In addition to what is contained in Subsections (2)–(4), the service provider may request the customer to make a statement on whether its beneficial owner is considered a politically exposed person, where it is deemed necessary for the identification of the customer, the business relationship and the transaction order, on the basis of the results of the procedure specified in the internal rules referred to in Section 33 and based on the nature of the business

relationship or on the type and value of the transaction order and on the customer's circumstances, with a view to the prevention and combating of money laundering and terrorist financing. If the beneficial owner is a politically exposed person, the aforesaid statement must also indicate the category of politically exposed persons applicable according to Subsection (2) of Section 4.

(6) 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 a written statement.

(7) Where there is any doubt concerning the identity of the beneficial owner, the service provider shall take measures to check the information concerning the beneficial owner's identity in a publicly available register or in any other register from whose manager it has statutory right to request data.

Section 8/A

(1) The customer is not required to make a written statement referred to in Section 8, if the service provider records the data specified in Subsections (1)–(5) of Section 8 on the basis of documents set out in Subsection (4) of Section 7 and presented to it, and on the basis of publicly available registers or registers from whose manager it has statutory right to request data.

(2) In the case specified in Subsection (1), the service provider shall also record that the data specified in Subsections (1)–(5) of Section 8 were recorded without requesting the customer to make the written statement referred to in Section 8.

Section 9

(1) In the cases referred to in Subsection (1) of Section 6, the service provider is required to record the following information pertaining to the business relationship and the transaction order:

- a)* regarding business relationships, the type, subject matter and the term of the contract;
- b)* regarding transaction orders, the subject matter and the value of the transaction.

(2) In addition to what is contained in Subsection (1), the service provider may also record the particulars of performance (place, time, mode) and may request for the disclosure of information concerning the source of funds, where it is deemed necessary for the identification of the customer, the business relationship and the transaction order, on the basis of the results of the procedure specified in the internal rules referred to in Section 33, based on the nature of the business relationship or on the type and value of the transaction order and on the customer's circumstances in the interest of preventing and combating money laundering and terrorist financing.

(3) The service provider may stipulate the establishment of the business relationship and the completion of the transaction order to the approval of the service provider's executive officer defined in its organizational and operational regulation where it is deemed necessary for the identification of the customer, the business relationship and the transaction order, on the basis of the results of the procedure specified in the internal rules referred to in Section 33 and based on the nature of the business relationship or on the type and value of the transaction

order and on the customer's circumstances, with a view to the prevention and combating of money laundering and terrorist financing.

Section 10

(1) In line with the legal provisions applicable to their activities, service providers are required to conduct ongoing monitoring of the business relationship including the analysis of the transaction orders executed during the existence of that business relationship in order to establish whether a given transaction order is consistent with the information available to the service provider on the customer in accordance with the relevant provisions.

(1a) The service provider may carry out the continuous monitoring of the business relationship referred to in Subsection (1) in the framework of an enhanced procedure specified in the internal rules referred to in Section 33, where it is deemed necessary for the identification of the customer, the business relationship and the transaction order, on the basis of the results of the procedure specified in the internal rules referred to in Section 33 and based on the nature of the business relationship or on the type and value of the transaction order and on the customer's circumstances, with a view to the prevention and combating of money laundering and terrorist financing.

(1b) The service provider shall pay special attention to all complex and unusual transactions, where it is deemed necessary for the identification of the customer, the business relationship and the transaction order, on the basis of the results of the procedure specified in the internal rules referred to in Section 33 and based on the nature of the business relationship or on the type and value of the transaction order and on the customer's circumstances, with a view to the prevention and combating of money laundering and terrorist financing.

(2) Service providers are required to ensure that the data and information as well as documents held in connection with business relationships are kept up-to-date.

(3) During the existence of the business relationship, the customer is required to notify the service provider any change in the data and information supplied in the course of customer due diligence or any change concerning the beneficial owner within five working days of the day when taking cognizance of such changes.

(4) In order to perform the obligation set out in Subsection (3), service providers are required to draw the attention of their customers concerning their obligation to report any and all changes in their particulars.

(5) Where there is no assignment made, either debiting or crediting, to an account maintained by a service provider engaged in the activities referred to in Paragraphs *a)-b)*, *d)* and *l)* of Subsection (1) of Section 1, apart from transaction orders that take several years to mature, the service provider shall request the customer in writing, within 30 days or in the next account statement, to report the changes in his particulars that may have occurred during the aforementioned period.

Section 11

(1) With the exception of Subsections (2)-(5) and (8), service providers are required to carry out the verification of the identity of the customer and the beneficial owner before establishing a business relationship or executing a transaction order.

(2) Service providers may carry out the verification of the identity of the customer and the beneficial owner during the establishment of a business relationship, if it is necessary in order to avoid the interruption of normal conduct of business and where there is little risk of money laundering and terrorist financing occurring. In such cases the verification of identity shall be completed before the first transaction order is executed.

(3) The service providers engaged in the activity referred to in Paragraph *c*) of Subsection (1) of Section 1, in connection with insurance policies within the field of life assurance under Schedule No. 2. to the Insurance Act, may carry out the verification of the identity of the beneficiary under the policy and any other person entitled to receive services of the insurer / insurance provider even after the establishment of the business relation, if they were not known at the time of signature of the contract. In that case, verification of identity shall take place at or before the time of payout or at or before the time the entitled person enforce his / her rights originating from the contract (policy).

(4) The service providers engaged in the activity referred to in Paragraph *a*) of Subsection (1) of Section 1 and entitled to open payment accounts, may open a payment account provided they ensure that transactions are not executed by the customer, the proxy, the authorised signatory or the representative until the completion of the verification of the identity of the customer and the beneficial owner.

(5) The service providers engaged in the activity referred to in Paragraph *l*) of Subsection (1) of Section 1, may open a personal account governed under Act XCVI of 1993 on Voluntary Mutual Insurance Funds (hereinafter referred to as the 'Öpt Act'), provided they ensure that the customer and the beneficiary will not get any service until the completion of verification of the identity of the customer and the beneficial owner. The service providers engaged in employer pension services referred to in Paragraph *c*) of Subsection (1) of Section 1 may open a member account under Act CXVII of 2007 on Employer Pension and its Institutions (hereinafter referred to as the 'Fnyt Act'), provided they ensure that the member, annuitant and the beneficiary will not get any service until the completion of verification of the identity of the customer and the beneficial owner.

(6) Where the service provider is unable to carry out the customer due diligence measures specified in Sections 7-9, it may not carry out a transaction through a payment account, establish a business relationship or execute a transaction order, or it is required to terminate the business relationship with the customer in question.

(7) If the customer is a legal person or an organization not having a legal personality, following completion of the due diligence procedures on the person acting in its name and on its behalf, due diligence procedures shall also be carried out concerning the legal person or the organization not having a legal personality.

(8) The customer due diligence measures specified under Sections 7-9 shall not be repeated if:

a) the service provider has already completed the customer due diligence procedures specified under Sections 7-9 relating to the customer, the proxy, the authorised signatory and the representative in connection with previous transaction orders;

b) the service provider has already carried out the verification of the identity of the customer, the proxy, the authorized signatory and the representative in connection with current transactions in accordance with Subsections (4)-(7) of Section 7; and

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

Section 11/A

(1) In order to perform the obligation in Subsection (2) of Section 6, the service provider shall record the data referred to in Subsection (2) of Section 7 and Paragraph b) of Subsection (1) of Section 9 when completing a transaction order whose amount reaches or exceeds HUF 300,000.

(2) Service providers engaged in the activities referred to in Paragraph a) of Subsection (1) of Section 1 shall, upon completion of a bank transfer or a direct cash deposit - without using the services of any payment service provider - and service providers engaged in the activities referred to in Paragraph c) of Subsection (1) of Section 1 in the case of insurances included in the life insurance branch under Schedule No. 2 of the Insurance Act. – except for pure term insurances without any savings element –, upon completion of any cash deposit in excess of the contractual premiums, shall record the data specified in Subsection (2) of Section 7 and Paragraph b) of Subsection (1) of Section 9.

Simplified customer due diligence procedures

Section 12

(1) In the cases referred to in Paragraphs a), b) and d) of Subsection (1) of Section 6, service providers are required to carry out the customer due diligence measures in Subsection (1) of Section 10 and – where it is deemed necessary for the identification of the customer or the business relationship or transaction order with a view to the prevention and combating of money laundering and terrorist financing – may record the data specified in Subsection (2) of Section 7 and request the presentation of documents specified in Subsection (4) of Section 7, if its customer is:

a) a service provider engaged in the activities referred to in Paragraphs a)-e) and l) of Subsection (1) of Section 1 within the territory of the European Union, or a service provider that is engaged in the activities referred to in Paragraphs a)-e) and l) of Subsection (1) of Section 1 and that has its registered office in a third country which imposes requirements equivalent to those laid down in this Act and supervised for compliance with those requirement;

b) a listed company whose securities are admitted to trading on a regulated market in one or more Member States, or a listed company from a third country that is subject to disclosure requirements consistent with Community legislation;

c) a supervisory body mentioned under Section 5;

d) a local government, the budgetary organ of a local government, or a central administrative body other than those covered in Paragraph c)

e) the European Parliament, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Court of Auditors, the European Economic and Social Committee, the Committee of the Regions, the European Central Bank, the European Investment Bank or any other institution or body of the European Union.

(2) Where a third country meets the conditions laid down in Paragraphs a)-b) of Subsection (1), the service provider shall inform the competent supervisory body mentioned under Section 5, which is to forward that information to the minister in charge of the money, capital and insurance markets (hereinafter referred to as ‘minister’) without delay.

(3) The minister informs the Commission and the member states of cases where he considers that a third country meets the conditions laid down in Paragraphs a)-b) of Subsection (1).

Section 13

(1) In the cases referred to in Paragraphs a), b) and d) of Subsection (1) of Section 6, service providers are required to carry out the customer due diligence measures specified in Subsection (1) of Section 10 and – where it is deemed necessary for the identification of the customer or the business relationship or transaction order with a view to the prevention and combating of money laundering and terrorist financing – may record the data specified in Subsection (2) of Section 7 and request for the presentation of documents specified in Subsection (4) of Section 7,

a) insurance policies within the field of life assurance under Schedule No. 2 to the Insurance Act, where the annual premium is no more than two hundred and sixty thousand forints or the single premium is no more than six hundred and fifty thousand forints;

b) insurance policies for pension schemes if there is no surrender clause and the funds payable to the insured person cannot be used as collateral for any credit or loan arrangement;

c) the electronic money specified in Point 5.2 of Chapter I of Schedule No. 2 to the Hpt Act, if the amount limit made available to the holder of the electronic money by the issuer of electronic money :

1. in the case of non-rechargeable electronic money, is no more than sixty-five thousand forints;

2. in the case of electronic money that is rechargeable, is no more than sixty-five thousand forints in the given calendar year, except when an amount of two hundred and sixty thousand forints or more is redeemed by the issuer of electronic money in that same calendar year upon the electronic money holder’s request.

(2) Where a party entering into a contract with an insurance company purchases life insurance under the same policy to the benefit of more than one person (group insurance), the insurance company in this case is required to apply customer due diligence measures only in respect of the contracting party.

(3) The insurance company is not required to identify the customer, if an independent insurance intermediary, in the framework of its insurance intermediating activity, has previously already identified that customer.

Enhanced customer due diligence procedures

Section 14

(1) Service providers are required to record all data and particulars specified in Subsections (2)-(3) of Section 7, where the customer has not been physically present for identification purposes or for the verification of his identity.

(2) For the purposes of verification of the identity of the customer, the customer is required to submit to the service provider certified copies of the documents specified in Subsection (4) of Section 7 containing the data specified in Subsections (2)-(3) of Section 7.

(3) Certified copies of the documents referred to in Subsection (2) shall only be accepted for the identification and verification of the identity of the customer, if:

a) it was prepared by a Hungarian consulate officer or a notary public, and certified accordingly; or

b) the Hungarian consulate officer or the notary public has provided an endorsement for the copy to verify that the copy is identical to the original presented; or

c) 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 consulate officer has provided a confirmatory certification of the signature and seal of the said authority.

(4) For opening a customer account defined in Point 130 of Act CXX of 2001 on the Capital Market, a securities account defined in Point 46 of the same Act, or a securities deposit account, the customer may also submit the documents determined for the verification of identity in Subsection (4) of Section 7 as well as the statement under Section 8 in electronic form – particularly by sending the scanned document in e-mail – or via fax, where there is no information, fact or circumstance indicating money laundering or terrorist financing. In such cases, for opening the account the customer may also prove the existence of its payment account from which deposits to the customer account or to which withdrawals from the customer account are made (hereinafter referred to as ‘verified payment account’) by sending the relevant documents electronically or via fax according to the provisions of this Subsection. Only accounts kept by a service provider defined in Subsections (1) and (2) of Section 18 may be accepted as verified payment accounts. Until the customer appears in person for identification and verification of identity or the documents under Subsections (2) and (3) are submitted, with the exception of settling transactions relating to customer accounts, securities accounts or securities deposit accounts, only cash may be paid via simple bank transfer and exclusively in respect of the customer account opened in accordance with this Subsection, in a manner that cash deposits may only be made from the customer’s verified payment account and cash withdrawals may only be made to the customer’s said verified payment account.

(5) For the purpose of verifying the data recorded under Subsection (4) and the data identifying the customer, the service provider keeping the customer account, securities account or securities deposit account, shall, by sending the natural person customer’s personal identification data, request data from the service provider keeping the verified payment account about the identification of the customer in respect of the verified payment account and about the authenticity of the data supplied in respect of the customer account, securities account or securities deposit account. The requested service provider shall supply the requested data within eight days. If the requested service provider keeps no payment account for the customer, it shall, immediately after supplying the requested data, delete all information received from the service provider keeping the customer account, the securities

account or the securities deposit account during the request for data procedure.

Section 15

(1) Service providers engaged in the activity referred to in Paragraph *a*) of Subsection (1) of Section 1 are required, before establishing correspondent banking relationships with service providers having their registered offices in a third country, to:

a) prepare a comprehensive assessment on the service provider having its registered office in the third country, for the purposes of assessing and evaluating its system of means applied against money laundering and terrorist financing;

b) ascertain the fact that the service provider having its registered office in the third country has carried out the verification of the identity of the customer having a direct access to the correspondence account, and performs ongoing monitoring on the direct access to the correspondence account; and

c) ascertain the fact that the service provider having its registered office in the third country is able to provide the relevant customer due diligence data on request.

(2) Establishing a correspondent banking relationship with a service provider having its registered office in a third country, can take place only after the approval of the executive officer specified in the organisational and operational rules of the service provider engaged in the activity referred to in Paragraph *a*) of Subsection (1) of Section 1.

(3) Service providers engaged in the activity referred to in Paragraph *a*) of Subsection (1) of Section 1 are prohibited to establish or maintain a correspondent banking relationship with a shell bank or with a service provider that maintains a correspondent banking relationship with a shell bank.

Section 16

(1) Customers residing abroad are required to make a written statement for the service provider declaring whether they are classified as politically exposed persons according to the law of their country. If a customer residing abroad is classified as a politically exposed person, the aforementioned statement shall also indicate the paragraph of Subsection (2) of Section 4 on the basis of which he/she is classified as a politically exposed person.

(1a) If a customer residing in another Member State or in a third country is considered politically exposed person, the statement shall, in addition to the data defined in Subsection (1), also indicate data concerning the source of funds.

(2) Where there is any doubt concerning the veracity of the abovementioned statement, the service provider is required to take the necessary measures in the interest of checking the statement submitted under Subsection (1) in registers available according to the legal provisions for this purpose or in registers that are openly accessible to the public.

(3) In case of a foreign politically exposed person, the establishment of the business relationship or the execution of a transaction order may take place only after the approval of the executive officer specified in the organisational and operational rules of the service provider.

Section 17

(1) In cases of exchanging money in the amount of five hundred thousand forints or above, service providers providing the currency exchange service are required to carry out the identification procedure with respect to all of the data listed under Subsections (2)-(3) of Section 7 and to verify the customer's identity, furthermore they are required to carry out the customer due diligence measures specified under Sections 8-9.

(2) The transaction receipt shall indicate the data listed in Subparagraphs *aa)-ab)* and *ad)* of Paragraph *a)* and Subparagraphs *ba)-bc)* of Paragraph *b)* of Subsection (2) of Section 7, and, in case of foreign natural persons, the Hungarian place of abode, as well.

(3) The obligation of carrying out the customer due diligence measures specified in Subsection (1) shall also apply to individual transaction orders linked in effect, if their combined value reaches five hundred thousand forints. In this case due diligence measures shall be carried out at the time of acceptance of the transaction order the execution of which brings the combined value of the linked transaction orders to the threshold of five hundred thousand forints.

Customer due diligence measures carried out by other service providers

Section 18

(1) Service providers are entitled to accept the outcome of the customer due diligence procedures laid down in Sections 7-9, if the customer due diligence measures were carried out by a service provider that is engaged in the activities referred to in Paragraphs *a)-e)* and *l)* of Subsection (1) of Section 1 within the territory of Hungary, with the exception of service providers carrying on money transmission and currency exchange activities.

(2) Service providers are entitled to accept the outcome of customer due diligence procedures laid down in Sections 7-9, if the customer due diligence measures were carried out by a service provider that is engaged in the activities referred to in Paragraphs *a)-e)* and *l)* of Subsection (1) of Section 1, with the exception of service providers carrying on money transmission and currency exchange activities:

- a)* within an other member state of the European Union; or
- b)* within a third country that meets the requirements laid down in Subsection (6) and Section 19.

(3) Service providers engaged in the activities referred to in Paragraphs *g)-h)* and *m)* of Subsection (1) of Section 1 are entitled to accept the outcome of customer due diligence procedures laid down in Sections 7-9, if the customer due diligence measures were carried out by a service provider that is engaged in the activities referred to in Paragraphs *g)-h)* and *m)* of Subsection (1) of Section 1 within the territory of Hungary.

(4) Service providers engaged in the activities referred to in Paragraphs *g)-h)* and *m)* of Subsection (1) of Section 1 are entitled to accept the outcome of customer due diligence procedures laid down in Sections 7-9, if the customer due diligence measures were carried out by a service provider that is engaged in the activities referred to in Paragraphs *g)-h)* and *m)* of Subsection (1) of Section 1:

- a)* within the territory an other member state of the European Union; or

b) within a third country that meets the requirements laid down in Subsection (6) and Section 19.

(5) The outcome of customer due diligence procedures specified in Subsections (2) and (4) may be accepted even if the documents or data on which these requirements have been based are different to those determined in this Act.

(6) If the customer due diligence procedures were carried out by a service provider that is engaged in the activities referred to in Paragraphs *a)-h)*, *l)* and *m)* of Subsection (1) of Section 1, with the exception of service providers carrying on money transmission and currency exchange activities, the outcome of customer due diligence procedures may be accepted according to Subsections (2) and (4), if the service provider:

a) is included in the mandatory professional register; and

b) applies customer due diligence procedures and record keeping requirements as laid down or equivalent to those laid down in this Act and its supervision is executed in accordance with the requirements laid down or equivalent to those laid down in this Act, or its registered office is in a third country, which applies equivalent requirements to those laid down in this Act.

(7) Service providers are required to inform the supervisory body mentioned under Section 5 if a third country meets the conditions laid down in Paragraph *b)* of Subsection (6). The supervisory body shall forward that information to the minister without delay.

(8) The minister shall inform the Commission and the Member States of cases where a third country meets the conditions laid down in Paragraph *b)* of Subsection (6).

Section 19

(1) In the cases referred to in Subsections (1)-(4) of Section 18, service providers shall be authorized to make available to other service providers data and information obtained for the purposes of carrying out due diligence procedures laid down in Sections 7-9 subject to the prior consent of the customer affected.

(2) In the cases referred to in Subsections (1)-(4) of Section 18, subject to the conditions specified in Subsection (6) of Section 18, if the service provider performing the customer due diligence procedure and the service provider accepting the results of the customer due diligence procedure have agreed on the disclosure of the results of the customer due diligence procedure, the service provider that has carried out the customer due diligence measures shall disclose without delay, at the written request of the service provider accepting the outcome of customer due diligence procedures, a copy of the data and information obtained for the purposes of identification and verification of identity of the customer and the beneficial owner, and a copy of other relevant documentation on the identity of the customer or the beneficial owner - subject to the prior consent of the customer affected - to the service provider accepting the results of the customer due diligence procedure..

Section 20

In the cases specified in Subsections (1)-(4) of Section 18, as regards compliance with the requirements set out in Section 7-9, the responsibility is to be borne by the service provider accepting the outcome of the customer due diligence procedures carried out by an other service provider.

Section 21

Sections 18-20 shall not apply to outsourcing agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the service provider.

Information on the payer accompanying the transfers of funds

Section 22

(1) The Authority and the authority operating as the financial intelligence unit shall function as the “authorities responsible for combating money laundering or terrorist financing” as described in Article 14 of the Regulation.

(2) For the purposes specified in Article 14 of the Regulation, upon the request of the authorities referred to in Subsection (1) acting within their competence, service providers are required to hand over to them the information on the payer as specified in Article 4 of the Regulation.

(3) The Authority shall function as the "authority responsible for application" as described in Paragraph (2) of Article 15 of the Regulation, and as the "competent authority" as described in Paragraph (3) thereof, while, in respect of the MNB, the authority operating as the financial intelligence unit shall have the same functions.

(4) As carrying on supervision the Authority shall act in accordance with the provisions of the Act on the General Rules of Administrative Proceedings and Services, respecting the derogations set out in Act on the Hungarian Financial Supervisory Authority (hereinafter referred to as the ‘HFSA Act’), furthermore, the authority operating as the financial intelligence unit shall act in accordance with the APS Act.

(5) 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, consistent with the weight of the infringement, shall take the measures specified under Paragraphs *b)-e)* of Subsection (1) of Section 35 and may also take the measures specified below:

a) call upon the service provider to introduce the necessary measures to comply with the provisions of the Regulation, and to eliminate the revealed deficiencies;

b) prohibit the service provider from engaging in money transmission services before the infringement is terminated.

(6) The fine referred to in Paragraph *e)* of Subsection (1) of Section 35 may be imposed upon any service provider which fails to meet the obligations of the Regulation and of the resolution of the Authority, or meets them with delay or deficiency.

(7) 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 operating as the financial intelligence unit, consistent with the weight of the infringement, shall apply the measures specified under Paragraphs *c)-d)* of Subsection (1) of Section 35 and may call upon the service provider to introduce the necessary measures to comply with the provisions of the Regulation, and to eliminate the revealed deficiencies.

(8) In cases set out in Paragraph (4) of Article 3 and in Paragraph (4) of Article 5 of the Regulation, when calculating the amount of the transferred money in euro, the official exchange rate published by MNB on the day when the order for the money transmission was received shall apply; in cases of currencies that are not included in the MNB Bulletin for the conversion of currencies the exchange rate translated into euro and included in the publication of MNB valid on the day when the order for the money transmission was accepted has to be applied.

(9) The "national identification number" referred to in Paragraph (2) of Article 4 of the Regulation shall be construed as the numbers specified in Subparagraph *ad*) of Paragraph *a*) and Subparagraph *bc*) of Paragraph *b*) of Subsection (2) of Section 7.

(10) Service providers are not required to apply the provisions of the Regulation with respect to money transmissions within Hungary that are in compliance with the conditions set to in Paragraph (6) of Article 3 of the Regulation.

Reporting obligation

Section 23

(1) In the event of noticing any information, fact or circumstance indicating money laundering or terrorist financing, the executive officer, employee or contributing family member of the service provider shall, without delay, submit a report to the person referred to in Subsection (3) of this Section. The report shall contain:

- a*) the information and data the service provider has recorded pursuant to Sections 7-9;
- b*) a brief description of the information, fact or circumstance indicating money laundering or terrorist financing; and
- c*) the documents supporting the detailed description of information, fact or circumstance indicating money laundering or terrorist financing, if available.

(2) The executive officer, employee and contributing family member of the service provider shall examine any information, fact or circumstance indicating money laundering or terrorist financing in the case of the transaction order performed or to be performed or the transaction order initiated by the customer but not yet performed, as well as in the case specified in Subsection (6) of Section 11.

(3) Service providers shall, within five working days from starting its activity, designate one or more persons (hereinafter referred to as 'designated person') – depending on the structure of the organization – to forward without delay the reports received from the executive officer, employee or contributing family member of the service provider to the authority operating as the financial intelligence unit. Service providers are required to notify the authority operating as the financial intelligence unit concerning the appointment of the designated person, including the name and the position of such officer, and any subsequent changes therein, within five working days of the date of appointment or the effective date of the change.

(4) The designated person specified in Subsection (3) in the name of the service provider shall submit the report to the authority operating as the financial intelligence unit in the form of a secure electronic message, and the authority operating as 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.

(5) Prior to the submission of the report referred to in Subsection (4), the service provider may not carry out a transaction order.

(6) The designated person specified in Subsection (3) in the name of the service provider shall comply with the obligation of reporting referred to in Subsection (4) after carrying out the transaction order, if the carrying out of the transaction cannot be prevented as under Subsection (5) or the filing of the report before carrying out the transaction order is likely to jeopardize efforts to trace the beneficial owner as part of an impending investigation.

(7) If a report is filed in good faith, the executive officer, employee or contributing family member of the service provider and the designated person (hereinafter referred to as 'reporting persons') shall not be held liable if the report ultimately proves to be unsubstantiated.

(8) The authority operating as the financial intelligence unit shall publish an announcement concerning the efficiency of the reports and any proposals it may have to improve such efficiency on its official website semi-annually.

Section 24

(1) The service provider shall suspend the execution of a transaction order, if any information, fact or circumstance indicating money laundering or terrorist financing in connection with the transaction order is emerged and the service provider considers the immediate action of the authority operating as the financial intelligence unit to be necessary for checking the data, fact or circumstance indicating money laundering or terrorist financing. In this case the service provider is required to submit a report without delay to the authority operating as the financial intelligence unit in order to investigate the cogency of the report.

(2) The service provider shall submit the report specified in Subsection (1) to the authority operating as the financial intelligence unit in the form of a secure electronic message, and the authority operating as 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.

(3) Unless otherwise provided by the authority operating as the financial intelligence unit, the service provider shall suspend the completion of the transaction order if it is notified by the authority operating as the financial intelligence unit about any information, fact or circumstance indicating money laundering or terrorist financing in relation to the specific transaction order.

(4) The authority operating as the financial intelligence unit shall examine the report:

- a)* in the case of domestic transaction orders within two working days following the submission of the report under Subsection (1) or the message under Subsection (2);
- b)* in the case of foreign transaction orders within four working days following the submission of the report under Subsection (1) or the message under Subsection (2).

(5) The authority operating as the financial intelligence unit may extend its investigation specified in Subsection (4) by additional three working days, if such extension is required for the disclosure specified in Subsection (1) of Section 26.

(6) The authority operating as the financial intelligence unit shall inform the service provider in writing, if

- a) it extends the investigation under Subsection (5);
- b) the transaction order may be completed before the conclusion of the investigation by the authority operating as the financial intelligence unit.

(7) The service provider shall carry out a suspended transaction order upon receipt of notice from the authority operating as the financial intelligence unit in accordance with Paragraph b) of Subsection (6), or following the expiry of the time limits specified in Subsections (4) and (5) in the absence of a notice from the authority operating as the financial intelligence unit.

(8) If acting in good faith, the service provider and the authority operating as the financial intelligence unit referred to in Subsection (2) shall not be held liable for the suspension of a transaction order if it ultimately can be carried out on the basis of what is contained in Subsection (7).

Section 25

If the supervisory body mentioned under Section 5 obtains any information, fact or circumstance during its regulatory supervision that is to be reported according to Subsection (1) of Section 23, it shall inform the authority operating as the financial intelligence unit without delay.

Section 25/A

(1) When there is any information, fact or circumstance indicating money laundering or terrorist financing, the authority operating as the financial intelligence unit may, in its own capacity or based on the request of a foreign national financial intelligence unit, access the data managed by the service provider.

(2) When there is any information, fact or circumstance indicating money laundering or terrorist financing, the authority operating as the financial intelligence unit may, in its own capacity or based on the request of a foreign national financial intelligence unit, access bank secrets, payment secrets, securities secrets, fund and insurance secrets, occupational retirement pension secrets, and trade secrets managed by the service provider.

(3) The authority operating as the financial intelligence unit may, in its capacity under this Act or in order to comply with the written request of the foreign national financial intelligence unit, contact the service providers in respect of data or secrets referred to in Subsections (1) and (2), respectively. The service providers shall disclose the data or secret indicated in the request to the authority operating as the financial intelligence unit.

(4) When there is any information, fact or circumstance indicating money laundering or terrorist financing, the authority operating as the financial intelligence unit may, in its own capacity or based on the request of a foreign national financial intelligence unit, access the data managed by central administrative agencies, courts or supervisory bodies mentioned

under Section 5.

(5) When there is any information, fact or circumstance indicating money laundering or terrorist financing, the authority operating as the financial intelligence unit may, in its own capacity or based on the request of a foreign national financial intelligence unit, access the data qualifying as tax or customs secret.

(6) The administrative agencies, courts and supervisory bodies mentioned under Section 5 shall disclose the data or secrets referred to in Subsections (4) and (5) to the authority operating as the financial intelligence unit, requested by the latter in its capacity under this Act or in order to comply with the written request of the foreign national financial intelligence unit.

(7) When there is any information, fact or circumstance indicating money laundering or terrorist financing, the authority operating as the financial intelligence unit may initiate a proceeding falling within the competence of the central administrative body or the supervisory body mentioned under Section 5, together with sending all the information which is necessary for the institution and conduct of the proceeding and which may be managed by the organ conducting the proceeding. The requested party shall inform the authority operating as the financial intelligence unit about the result of the conducted proceeding.

(8) When there is any information, fact or circumstance indicating money laundering or terrorist financing, the authority operating as the financial intelligence unit may, in its own capacity or based on the request of a foreign national financial intelligence unit, in respect of the crimes determined in Subsection (1) of Section 26, in the interest of fulfilling its analysing-assessing duty specified in this Act, request the disclosure of data – including data obtained by collecting secret information – from the investigation authority and such request may not be rejected by the investigation authority, except for the case referred to in Subsection (10).

(9) In addition to the access granted under Subsection (8), when there is any information, fact or circumstance indicating money laundering or terrorist financing, the authority operating as the financial intelligence unit may, in its own capacity or based on the request of a foreign national financial intelligence unit, in respect of the crimes determined in Subsection (1) of Section 26, in the interest of fulfilling its analysing-assessing duty specified in this Act, take over data with direct access from the data base of the investigation authority of the National Tax and Customs Administration (hereinafter referred to as ‘NAV’). The direct access shall be guaranteed by the investigation authority of NAV.

(10) The head of the investigation authority may in exceptional cases reject the disclosure of data under Subsection (8) and may exclude direct access guaranteed under Subsection (9), if such disclosure of or direct access to data would be in conflict with the interests of an investigation or secret data collection in progress or would violate any international convention.

- (11) The head of the investigation authority may
- a) prohibit;
 - b) restrict;
 - c) make conditional to prior consent

the delivery of the disclosed data to any other bodies listed in Subsection (1) of Section 26 and Subsection (1) of Section 26/A.

(12) The authority operating as the financial intelligence unit may set a deadline of 8 to 30 days for the disclosure of the data specified in Subsections (1)–(6) and (8). The requested party shall, within the set deadline, disclose the requested data or inform the requesting party about the obstacle to compliance.

(13) During the period of suspension referred to in Subsections (1)–(2) of Section 24, the authority operating as the financial intelligence unit may, in justified cases, set a deadline shorter than the one determined in Subsection (12) for the disclosure of the data specified in Subsections (1)–(6) and (8).

(14) The authority operating as the financial intelligence unit may only use the data or secret accessed under Subsections (1)–(9) for the purposes defined in Subsection (1) of Section 26/A and in the interest of fulfilling its analysing-assessing duty specified in Subsection (1) of Section 26/B.

Section 26

(1) The authority operating as the financial intelligence unit shall be authorized to use the information obtained under this Act and the 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 only for the purposes of combating money laundering and terrorist financing, and for the purposes of prevention, detection and investigation of the following acts, and to disseminate such information to other investigating authorities, the public prosecutor, the national courts, the national security service, the EUROPOL under the Act on International Cooperation or to authority responsible for internal prevention, investigation and counter terrorism under the Act of the Hungarian Police:

a) Tax fraud, Excise violation, Illegal trafficking of excise goods, Illegal importation and the Violation of the financial interest of the European Communities, as applicable until 31 December 2011,

b) Kidnapping (Section 175/A of the Act IV of 1978), Trafficking in human beings (Section 175/B of the Act IV of 1978), Crimes with illegal pornographic material (Section 204 of the Act IV of 1978), Promotion of prostitution (Section 205 of the Act IV of 1978), Living on earnings of prostitution (Section 206 of the Act IV of 1978), Pandering (Section 207 of the Act IV of 1978), Smuggling of human beings (Section 218 of the Act IV of 1978), Abuse of authority (Section 225 of the Act IV of 1978), Harboring a criminal (Section 244 of the Act IV of 1978), Bribery (Section 250-255/A of the Act IV of 1978), Influence peddling (Section 256 of the Act IV of 1978), Bribery in international relations (Section 258/B-D of the Act IV of 1978), Abuse of a function and indirect bribery in international relations (Section 258/E of the Act IV of 1978), Acts of terrorism (Section 261 of the Act IV of 1978), Violation of international economic restrictions (Section 261/A of the Act IV of 1978), Illegal possession of explosive or other destructive devices (Section 263 of the Act IV of 1978), Illegal possession of firearms or ammunition (Section 263/A of the Act IV of 1978), Criminal misuse of military items and services, and dual-use items and technology (Section 263/B of the Act IV of 1978), Affiliation with organized crime (Section 263/C of the Act IV of 1978),

Misuse of radioactive substance (Section 264 of the Act IV of 1978), Crimes with weapons prohibited by international convention (Section 264/C of the Act IV of 1978), Unlawful gambling (Section 267 of the Act IV of 1978), Misuse of harmful consumer goods (Section 279 of the Act IV of 1978), Damaging of the environment (Section 280 of the Act IV of 1978), Damaging the natural environment (Section 281 of the Act IV of 1978), Violation of waste management regulations (Section 281/A of the Act IV of 1978), Misuse of narcotic drugs (Section 282, 282/A, 282/B, 282/C, 283 of the Act IV of 1978), Illegal possession of drug precursors (Section 283/A of the Act IV of 1978), Money laundering (Section 303-303/A of the Act IV of 1978), Failure to comply with the reporting obligation related to money laundering (Section 303/B of the Act IV of 1978), Unauthorized financial activities (Section 298/D of the Act IV of 1978), Budget fraud (Section 310 of the Act IV of 1978), Embezzlement (Section 317 of the Act IV of 1978), Fraud (Section 318 of the Act IV of 1978), Misappropriation of funds (Section 319 of the Act IV of 1978) and all economic crimes (Chapter XVII of the Act IV of 1978) and crimes against property (Chapter XVIII of the Act IV of 1978) under the Act IV of 1978 on the Criminal Code applicable until 30 June 2013

c) Drug trafficking (Section 176-177 of the Criminal Code), Possession of narcotic drugs (Section 178-179 of the Criminal Code), Inciting substance abuse (Section 181 of the Criminal Code), Aiding in the manufacture or production of narcotic drugs (Section 182 of the Criminal Code), Criminal offenses with drug precursors (Section 183 of the Criminal Code), Criminal offenses with harmful consumer goods (Section 189 of the Criminal Code), Kidnapping (Section 190 of the Criminal Code), Trafficking in human beings (Section 192 of the Criminal Code), Pandering (Section 200 of the Criminal Code), Procuring for prostitution or sexual act (Section 201 of the Criminal Code), Living on earnings of prostitution (Section 202 of the Criminal Code), Child pornography (Section 204 of the Criminal Code), Environmental offenses (Section 241 of the Criminal Code), Damaging the natural environment (Section 242-243 of the Criminal Code), Violation of waste management regulations (Section 248 of the Criminal Code), Misappropriation of radioactive materials (Section 250 of the Criminal Code), Harboring a criminal (Section 282 of the Criminal Code), Active corruption (Section 290 of the Criminal Code), Passive corruption (Section 291 of the Criminal Code), Active corruption of public officials (Section 293 of the Criminal Code), Passive corruption of public officials (Section 294 of the Criminal Code), Active corruption in court or regulatory proceedings (Section 295 of the Criminal Code), Passive corruption in court or regulatory proceedings (Section 296 of the Criminal Code), Indirect corruption (Section 298 of the Criminal Code), Abuse of a function (Section 299 of the Criminal Code), Abuse of authority (Section 305 of the Criminal Code), Acts of terrorism (Section 314-316 of the Criminal Code), Failure to report a terrorist act (Section 317 of the Criminal Code), Terrorist financing (Section 318 of the Criminal Code), Participation in a criminal organization (Section 321 of the Criminal Code), Criminal offenses with explosives or blasting agents (Section 324 of the Criminal Code), Criminal offenses with firearms and ammunition (Section 325 of the Criminal Code), Criminal offenses with weapons prohibited by international convention (Section 326 of the Criminal Code), Violation of international economic restrictions (Section 327 of the Criminal Code), Criminal offenses with military items and services (Section 329 of the Criminal Code), Criminal offences with dual-use items (Section 330 of the Criminal Code), Illegal immigrant smuggling (Section 353 of the Criminal Code), Unlawful gambling operations (Section 360 of the Criminal Code), and crimes under Chapter XXXV-XLII of the Criminal Code.

(2) In order to fulfil its duties defined in Act CLXXX of 2007 on the implementation of financial assets restricting measures of the European Union as well as on the amendment of certain acts connected therewith (hereinafter referred to as 'Kit Act'), the authority operating as the financial intelligence unit may deliver information to the body responsible for the execution of the financial assets restricting measure.

(3) The data recorded in the data disclosure register kept under Act CXII of 2011 on self-determination regarding personal information and on the freedom of information shall be kept by the authority operating as the financial intelligence unit for 20 years following disclosure.

(4) The authorities specified in Subsection (1) may, in the interest of fulfilling their statutory duties, request data from the data management system of the authority operating as the financial intelligence unit, along with the indication of the purpose of such request.

Section 26/A

(1) The authority operating as the financial intelligence unit may independently share information and cooperate with any foreign national financial intelligence unit, in the course of which it may only disseminate information – obtained under this Act or Act XLVIII of 2007 on the implementation of Regulation 1889/2005/EC of the European Parliament and of the Council (26 October 2005) on controls of cash entering or leaving the Community – to the foreign national financial intelligence unit for the purpose of combating money laundering and terrorist financing.

(2) The authority operating as the financial intelligence unit may enter into a cooperation agreement with the foreign national financial intelligence unit, if such agreement supports information exchange and cooperation under Subsection (1).

Section 26/B

(1) When there is any information, fact or circumstance indicating money laundering or terrorist financing, the authority operating as the financial intelligence unit, acting in its capacity, shall pursue analysing-assessing activity for the purpose of disclosing information specified in Subsection (1) of Section 26 and Subsection (1) of Section 26/A. During its analysing-assessing activity, the authority operating as the financial intelligence unit shall

a) compare the information obtained under this Act or Act XLVIII of 2007 on the implementation of Regulation 1889/2005/EC of the European Parliament and of the Council (26 October 2005) on controls of cash entering or leaving the Community, the information obtained from databases to which it has direct access, public information and information available for anyone, and the information collected to comply with the request under Section 25/A; reveal and interpret all connections between such information;

b) monitor financial transactions and processes related to the information specified in Paragraph a); examine business relationships and transaction orders;

c) make observations and conclusions in the interest of disclosing information with a view to combating money laundering and terrorist financing and preventing, detecting and investigating the crimes defined in Subsection (1) of Section 26.

(2) The authority operating as the financial intelligence unit shall investigate the characteristics of crimes related to the crimes under Subsection (1) of Section 26 and shall monitor the new elements appearing during the commission of such crimes.

(3) As a result of its analysing-assessing activity, the authority operating as the financial intelligence unit shall disseminate information according to Subsection (1) of Section 26.

(4) Pursuant to Subsection (1) of Section 29, the authority operating as the financial intelligence unit shall keep statistics on the combat against money laundering and terrorist financing.

Prohibition of disclosure

Section 27

(1) The reporting persons, the authority operating as the financial intelligence unit, the service provider requested under Subsection (3) of Section 25/A, the central administrative body requested under Subsections (6)–(7) of Section 25/A, the body responsible for the execution of the financial assets restricting measure, and the supervisory body mentioned under Section 5 shall not provide information to the customer concerned or to other third persons on the fact that information has been transmitted in accordance with Section 23, on the contents of such information, on the fact that the transaction order has been suspended under Section 24, on the name of the reporting persons, or on whether a money laundering or terrorist financing investigation is being or may be carried out on the customer, and is required to ensure that the filing of the report, the contents thereof, and the identity of the reporting persons remain confidential.

(2) The prohibition laid down in Subsection (1) shall not cover provision of information by the reporting persons to the supervisory body mentioned under Section 5, the request sent to a service provider under Subsection (3) of Section 25/A, the request sent to a body defined in under Subsections (6)–(7) of Section 25/A and the disclosure of information to the authority specified in under Subsection (1) of Section 26.

(3) In connection with supervision on a consolidated basis conducted under the HptAct, Act CXX of 2001 on the Capital Market, and the Insurance Act, or on supplementary supervision of a financial conglomerate, the prohibition laid down in Subsection (1) shall not prevent disclosure of information between undertakings from Member States, or from third countries, which impose requirements upon such undertakings equivalent with those laid down in this Act, and are supervised for compliance those requirements.

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

(5) Regarding service providers engaged in the activities referred to in Paragraphs *a)-e)*, *g)-h)*, *l)* and *m)* of Subsection (1) of Section 1, the prohibition laid down in Subsection (1) shall not prevent disclosure of information between the two or more service providers involved, provided that:

a) the information refer to the same customer and the same transaction order;

b) of the two or more service providers involved, at least one is engaged in activities defined by this Act, while the other service providers are resident 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 referred to 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 this Act.

(6) Where a third country meets the conditions laid down in Subsection (3)-(5) above, the service providers engaged in the activities referred to in Paragraphs *a)-e)*, *g)-h)*, *l)* and *m)* of Subsection (1) of Section 1 shall inform the supervisory body mentioned under Paragraphs *a)-b)*, *d)-e)*, *g)* of Section 5. The supervisory body mentioned under Paragraphs *a)-b)*, *d)-e)*, *g)* of Section 5 shall forward that information to the minister without delay.

(7) The minister shall inform the Commission and the Member States of the cases referred to in Subsection (6).

Record keeping and statistics

Section 28

(1) Service providers are required to keep on file the data and documents they have obtained in the process of discharging their obligation prescribed under Sections 7-10 and Section 17, or the copies of such documents, the records of compliance with reporting obligations and data transmitting requirements specified in Section 23, and the documents certifying the suspension of the execution of transaction orders by virtue of Section 24, or the copies of such documents, for a period of eight years from the time of recording or the time of reporting (suspension). The time limit for keeping the data or documents, or their copies, obtained under Paragraph *a)* of Subsection (1) of Section 6 shall commence upon the time of termination of the business relationship.

(2) The service providers engaged in activities referred to in Paragraphs *a)-e)*, *l)* and *m)* of Subsection (1) of Section 1 are required to keep records of all executed cash transaction orders in the amount of three million six hundred thousand forints or more (whether in forints or any other currency) in the register mentioned in Subsection (1) for a period of eight years.

Section 28/A

(1) If so requested by the supervisory body mentioned under Section 5, the authority operating as the financial intelligence unit, the investigation authority, the prosecutor's office or the court, the service provider shall keep the data or document defined in Subsections (1)–(2) of Section 28 for a period prescribed in such request but no more than for a period of 10 years.

(2) The data keeping period defined in Subsections (1)–(2) of Section 28 may only be extended upon the request of an authority, if the data or document specified therein is required for an official proceeding in progress or to be launched.

(3) After the final conclusion of the official proceeding specified in Subsection (2) or having failed to launch the planned proceeding, the service provider shall delete the data or document from its records. The authority specified in Subsection (1) shall immediately notify the service provider about the final conclusion of the official proceeding specified in Subsection (2) or about the failure to launch the planned proceeding.

(4) The authority operating as the financial intelligence unit shall keep the data or document accessed pursuant to a statutory provision for 10 years.

Section 29

(1) In cooperation with the investigation authorities, the General Prosecutor's Office and the National Judicial Office, the authority operating as the financial intelligence unit is required to maintain statistics by virtue of which the effectiveness of the system for the combating of money laundering and terrorist financing can be controlled.

(2) The statistics specified in Subsection (1) shall cover:

- a)* the number of suspicious transaction reports made under Section 23;
- b)* the number of transaction orders suspended under Section 24;
- c)* the number of cases for the freezing of assets in connection with terrorist financing under the Act on the Enforcement of the Economic and Financial Restrictive Measures Adopted by the European Union and the number of cases for the freezing of assets by court order, and the forint value of the funds and economic resources frozen by court order;
- d)* the number of suspicious transaction reports made under Section 23 and disseminated by the financial intelligence unit pursuant to Subsection (1) of Section 26;
- e)* the number of criminal proceedings launched – using the information disseminated pursuant to Subsection (1) of Section 26 – on suspicion of money laundering, act of terrorism as defined in Section 261 of Act IV of 1978, act of terrorism as defined in Sections 314–316 of the Criminal Code, failure to report an act of terrorism as defined in Section 317 of the Criminal Code, terrorist financing as defined in Section 318 of the Criminal Code; the qualification of such crimes; the number of suspects; the description and number of coercive measures taken during the investigation; and the manner of conclusion of the investigation;
- f)* in the criminal proceedings referred to in Paragraph *e)*:
 - fa)* the number of cases and the number of persons prosecuted;
 - fb)* the number of court verdicts and the number of persons convicted, the number of cases where any property has been frozen, seized or confiscated, the value of property seized or confiscated, and how much property has been frozen, seized or confiscated.

(3) The investigation authority shall supply the data specified in Paragraph *e)* of Subsection (2), the General Prosecutor's Office shall supply information to the authority operating as the financial intelligence unit relating to Subparagraph *fa)* of Paragraph *f)* of Subsection (2), and the court shall supply the number of final court verdicts 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 *fb)* of Paragraph *f)* on a quarterly basis. The investigation authority, the General Prosecutor's Office and the court may also disclose such data electronically.

(4) Records of the data referred to in Paragraphs *a)*-*d)* of Subsection (2) shall be broken down according to profession.

(5) The authority operating as the financial intelligence unit shall post the aforesaid statistics on its official website annually.

Measures in the case of branches and subsidiaries located in third countries

Section 30

(1) The service providers engaged in the activities referred to in Paragraphs *a)-e)* and *l)* of Subsection (1) of Section 1 are required to apply in their branches and subsidiaries located in third countries measures at least equivalent to those laid down under Sections 6-11, Section 28 and this Section.

(2) The service providers engaged in the activities referred to in Paragraphs *a)-e)* and *l)* of Subsection (1) of Section 1 shall keep their branches and subsidiaries located in third countries informed concerning their internal control and information system (Section 31), and the contents of their internal rules (Section 33).

(3) Where the legislation of the third country does not permit application of such equivalent measures as referred to in Subsection (1), the service providers engaged in the activities referred to in Paragraphs *a)-e)* and *l)* of Subsection (1) of Section 1 shall so inform the supervisory body specified in Paragraphs *a)-b)* of Section 5, which shall forward that information to the minister without delay.

(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 required under Subsection (1).

(5) Where the legislation of the third country does not permit application of the measures required under Subsection (1), the service providers engaged in the activities referred to in Paragraphs *a)-e)* and *l)* of Subsection (1) of Section 1 are required to prepare a comprehensive assessment on their branches and subsidiaries located in third countries.

Internal control and information systems, special training programs

Section 31

Service providers with employees participating in carrying out the activities listed under Subsection (1) of Section 1 are required to establish adequate and appropriate internal control and information systems for the procedures of customer due diligence, reporting and record keeping in order to prevent business relationships and transaction orders through which money laundering or terrorist financing is realized or possible.

Section 32

(1) Service providers are required to ensure that their employees participating in carrying out the activities listed under Subsection (1) of Section 1 are aware of the provisions in force relating to money laundering and terrorist financing, that they are able to recognize business relationships and transaction orders through which money laundering or terrorist financing

may be or is realized and to instruct them as to how to proceed in line with this Act in case a data, fact, circumstance is raised that indicates money laundering or terrorist financing.

(2) Service providers are required to ensure that their employees participating in carrying out the activities listed under Subsection (1) of Section 1 are aware of the provisions of the Act on the Enforcement of the Economic and Financial Restrictive Measures Adopted by the European Union, 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)-(2), service providers with employees participating in carrying out the activities listed under Subsection (1) of Section 1 are required to ensure the participation of their relevant employees in special training programs.

Internal rules

Section 33

(1) For performing their tasks related to the obligations conferred in this Act, service providers are required to prepare internal rules (hereinafter referred to as ‘internal rules’).

(2) The supervisory body mentioned under Section 5 shall approve the internal rules, if they contain the mandatory contents set out in this Act and in the decree implementing it, and if they are not contrary to any legal provision.

(3) For the purposes of drawing up the internal rules, the supervisory bodies mentioned under Section 5 shall, in collaboration with the authority operating as the financial intelligence unit and in agreement with the minister, provide sample rules as non-binding recommendations.

(3a) The sample rules defined in Subsection (3) shall be supervised and, if necessary, modified by the supervisory body mentioned under Section 5 every two years.

(3b) The sample rules defined in Subsection (3) shall be supervised and modified by the supervisory body mentioned under Section 5 in cooperation with the authority operating as the financial intelligence unit and in agreement with the minister, following the amendments of this Act.

(3c) The service provider, if any change is made in the legal regulation, the sample rules provided to it by the supervisory body mentioned under Section 5 or in its internal order of procedure, shall supervise and if necessary modify its internal rules

(4) Service providers engaged in trading in goods may undertake to discharge the obligations set out in this Act by submission of their internal rules to the trade licensing authority. The trade licensing authority, at the same time when it grants approval for the internal rules, shall also register the service provider in question. Only registered service providers engaged in trading in goods shall be authorized to accept cash payments of three million six hundred thousand forints or more.

Supervision, measures

Section 34

(1) The supervisory bodies determined in Paragraphs *a)-c), f)* and *g)* of Section 5 shall, in the process of exercising supervisory functions, ensure the compliance of service providers with the provisions of this Act.

(2) With the exceptions set out in this Act the supervisory bodies determined in Paragraphs *c), f)* and *g)* of Section 5 shall carry out their respective supervisory functions in accordance with the Act on the General Rules of Administrative Proceedings; the supervisory body mentioned under Paragraph *a)* of Section 5 shall carry out its supervisory functions in accordance with the Act on the General Rules of Administrative Proceedings and the HFSA Act; and the supervisory body mentioned under Paragraph *b)* of Section 5 shall carry out its supervisory functions in accordance with the Act on the General Rules of Administrative Proceedings and the Act on the National Bank of Hungary.

(3) The supervisory body determined in Paragraph *d)* of Section 5 shall carry out its supervisory functions in accordance with Act LXXV of 2007 on the Chamber of Hungarian Auditors, the Activities of Auditors, and on the Public Oversight of Auditors (hereinafter referred to as ‘the Auditors Act’).

(4) The supervisory body determined in Subparagraph *ea)* of Paragraph *e)* of Section 5 shall carry out its supervisory functions in accordance with Act XI of 1998 on Attorneys (hereinafter referred to as the ‘Attorneys Act’), and the supervisory body mentioned under Subparagraph *eb)* of Paragraph *e)* of Section 5 shall carry out its supervisory functions in accordance with Act XLI of 1991 on Notaries Public (hereinafter referred to as ‘Kjt Act’).

Section 35

(1) In the case of any infringement of the provisions of this Act or non-compliance with the obligations set out in this Act, the supervisory bodies mentioned under Paragraphs *a)-c), f)* and *g)* of Section 5 may take the following measures consistent with the weight of the infringement:

a) call upon the service provider to take the measures necessary for compliance with the provisions of this Act, and to eliminate the deficiencies;

b) advise the service provider:

ba) to ensure the participation of their relevant employees (executive officers) carrying out the activities listed under Subsection (1) of Section 1 in special training programs, or to hire employees (executive officers) with the appropriate professional skills required for those activities;

bb) to recondition the internal rules according to specific criteria within a prescribed deadline;

bc) to carry out the investigation according to the internal rules and initiate procedure against the person responsible

c) issue a warning to the service provider;

d) conclude in a decision that an infringement has occurred and at the same time dispose for the elimination thereof;

e) order the service provider to cease the unlawful conduct

f) in addition to or independent of the measures listed in Paragraphs a)–e), it may impose a fine of minimum two hundred thousand and maximum five hundred million forints upon the service providers engaged in the activities referred to in Paragraphs a)–e) and l) of Subsection (1) of Section 1, and a fine of minimum fifty thousand and maximum twenty million forints upon the service providers engaged in the activities referred to Paragraphs f), h)–i), j) and k) of Subsection (1) of Section 1..

(2) The measures defined under Subsection (1) shall be imposed upon a service provider – if it is a legal person or an organisation not having a legal personality – where a director of the service provider has committed the infringement for the benefit of the service provider.

(3) The measures defined under Subsection (1) shall be imposed upon a service provider – if it is a legal person or an organisation not having a legal personality – where an employee of the service provider has committed the infringement 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.

(4) While taking measures, the supervisory body mentioned under Paragraphs c), f) and g) of Section 5 shall consider the following:

- a) the seriousness of the infringement or deficiency;
- b) the impact of the infringement or deficiency on the service provider or its customers;
- c) the cooperative attitude exhibited by the persons in charge towards the supervisory body;
- d) recurrence and frequency of infringements;

Section 35/A

(1) When carrying out their supervisory functions, the supervisory body mentioned under Paragraph d) of Section 5 acting in compliance with the Auditors Act, the supervisory body mentioned under Subparagraph ea) of Paragraph e) of Section 5 acting in compliance with the Attorneys Act, and the supervisory body mentioned under Subparagraph eb) of Paragraph e) of Section 5 acting in compliance with the Kjt Act, shall consider the following:

- a) the seriousness of the infringement or deficiency;
- b) the impact of the infringement or deficiency on the service provider or its customers;
- c) the cooperative attitude exhibited by the persons in charge towards the supervisory body;
- d) recurrence and frequency of infringements;

Section 35/B

The supervisory body specified in this Act shall, while exercising its supervisory functions, ensure the service provider's compliance with the Kit Act and with the legal acts of the EU under the Kit Act.

Special provisions relating to attorneys and notaries public

Section 36

(1) The obligation of customer due diligence and reporting prescribed in this Act shall apply to attorneys, with the exception set out in Subsection (3), 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 transactions 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)* buying or selling real estate;
- c)* founding, operating or dissolving a business association or other economic operator.

(2) The customer due diligence and reporting obligations 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 provides public notary services in connection with the preparation and execution of the following transactions in accordance with the Kjt Act

- a)* buying or selling any participation (share) in a business association or other economic operator;
- b)* buying or selling real estate;
- c)* founding, operating or dissolving a business association or other economic operator.

(3) The obligations determined in this Act shall not apply to attorneys, if:

- a)* the data, fact or circumstance indicating money laundering or financing of terrorism become known in connection with providing the defence in criminal proceedings or legal representation before a court, other than the court of registration, during any stage of such defence or representation or at any time thereafter;
- b)* the data, fact or circumstance indicating money laundering or financing of terrorism was become known in connection with the defence or legal representation referred to in Paragraph *a)* or while providing legal advice relating to the questions for the opening of a proceeding.

(4) The obligation determined in this Act shall not apply to notaries public if:

- a)* the data, fact or circumstance indicating money laundering or financing of terrorism become known while providing legal advice relating to the questions for the opening of a proceeding;
- b)* the notary public conducts a non-litigious proceeding.

Section 37

(1) Attorneys and notaries public shall submit the report prescribed in Section 23 with the regional bar association or regional chamber of notaries public, respectively. The employees of attorneys and notaries public (including assistant attorneys) shall submit the report with the attorney or notary public who exercises employer's rights. The attorneys or notaries public exercising employer's rights shall forward the report without delay to the regional bar association or regional chamber of notaries public, respectively. Employees of law firms shall report to the person designated by the members' meeting, who shall forward the report without delay to the bar association with which the law firm is registered.

(2) The presidents of regional bar associations and regional chambers of notaries public shall designate a person to be responsible for forwarding without delay the reports received from the persons referred to in Paragraph *b)* of Subsection (1) of Section 2 to the authority operating as the financial intelligence unit. The regional bar associations and regional chambers of notaries public are required to notify without delay the authority operating as the financial intelligence unit about the designated person and also when the designated person is replaced.

(3) With regard to law firms, the members' meeting may decide whether the obligations prescribed in Subsection (1) of Section 23 and in Sections 31-32 are to be fulfilled by the law firm or by the members.

Section 38

(1) In respect of discharging the responsibilities prescribed in this Act, the Hungarian Bar Association shall draw up uniform internal rules for individual lawyers and single-member law firms that shall be treated as the internal rules of individual lawyers and single-member law firms in conformity with Section 33. The aforesaid uniform internal rules shall be approved by the minister responsible for justice.

(2) In respect of discharging the responsibilities prescribed in this Act, the law firms not mentioned in Subsection (1) are required to draw up internal rules, and to present them for approval to the competent regional bar association. The Hungarian Bar Association shall draw up standard rules in compliance with Subsection (3) of Section 33, and it shall be approved by the minister responsible for justice.

(3) In respect of discharging the responsibilities prescribed in this Act, the Hungarian Chamber of Notaries Public shall draw up guidelines for notaries public that shall be treated as the internal rules of notaries public.

(3a) The uniform internal rules mentioned in Subsection (1) and the sample rules mentioned in Subsection (2) shall be reviewed and, if necessary, amended by the Hungarian Bar Association, the guidelines mentioned in Subsection (3) shall be reviewed and, if necessary, amended by the Hungarian Association of Notaries Public every two years.

(3b) The uniform internal rules mentioned in Subsection (1) and the sample rules mentioned in Subsection (2) shall be reviewed and, if necessary, amended by the Hungarian Bar Association, the guidelines mentioned in Subsection (3) shall be reviewed and, if necessary, amended by the Hungarian Association of Notaries Public following the amendments of this Act.

(3c) The law firm not mentioned under Subsection (1), if any change is made in the legal regulation, the sample rules provided to it by the Hungarian Bar Association or in its internal order of procedure, shall supervise and, if necessary, modify its internal rules.

(4) Fulfilment of the reporting obligation by attorneys and notaries public shall not constitute a violation of the confidentiality requirements prescribed in specific other legislation.

(5) 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 Kjt Act.

Closing and authorizing provisions

Section 39

(1) This Act, with the exception of Subsections (2)-(9), shall enter into force on 14 December 2007.

(2) *[no longer in effect]*

(3) Sections 1-38, Section 40, Sections 42-43, Sections 46-51, Sections 54-55, and Section 56 shall enter into force on 15 December 2007.

(4) Subsection (10) shall enter into force on 16 December 2007.

(5) Subsection (12) and Section 52 shall enter into force on 2 January 2008.

(6) Subsection (13) shall enter into force on 3 January 2008.

(7) Subsections (1)-(2) of Section 44 shall enter into force on 15 December 2008.

(8) Subsection (3) of Section 44 shall enter into force on 1 January 2009.

(9) Subsection (11) shall enter into force on 2 January 2009.

(10) *[no longer in effect]*

(11) *[no longer in effect]*

(12) *[no longer in effect]*

(13) *[no longer in effect]*

Section 40

[no longer in effect]

Section 41

[no longer in effect]

Section 42

By way of derogation from Subsection (6) of Section 11, the service provider is required to refuse the execution of a transaction order after 31 December 2014, if:

- a)* it has established a business relationship with the customer prior to 1 July 2013;
- b)* the customer failed to appear at the service provider personally or by way of a representative until 31 December 2014 for the purpose of carrying out customer due diligence procedures; and
- c)* regarding the customer, the outcome of the customer due diligence procedures specified under Sections 7-10 is not fully available on 31 December 2014.

Section 43

(1) The minister is hereby authorized to publish - by way of a decree - the list of third countries which impose requirements equivalent to those laid down in this Act, and to publish - by way of a decree - the list of third countries whose nationals are not permitted to benefit

from the simplified customer due diligence procedures by virtue of the Commission decisions adopted according to Paragraph (4) of Article 40 of Directive 2005/60/EC.

(2) The minister is hereby authorized to lay down in a decree the mandatory content of internal rules.

Section 44

[no longer in effect]

Section 45

(1) Following the entry of this Act into force, the supervisory body mentioned under Section 5 shall make available the model rules within forty-five days after the time of this Act entering into force.

(2) Service providers already existing at the time of this Act entering into force are required to amend their internal rules within ninety days of the time of this Act entering into force to comply with the provisions of this Act.

(3) In addition to satisfy the requirements set out in specific other legislation that are to be met for obtaining a license permit, the service providers listed under Paragraphs *a)-e)*, *i)* and *l)* of Subsection (1) of Section 1 established after the time of this Act entering into force shall submit also their internal rules for approval to the competent supervisory body mentioned under Section 5 together with the license application.

(4) The service providers commencing the activities referred to in Paragraph *a)* of Subsection (1) of Section 1, by providing payment services according to Subparagraph *g)* of Point 9 of Chapter I of *Schedule No. 2* to the HptAct, as well as service providers commencing the activities referred to in Paragraphs *f)-h)*, *j)* and *m)* of Subsection (1) of Section 1 are required to draw up their internal rules and submit it for approval to the supervisory body determined in Section 5 within ninety days following the commencement of operations.

(5) The Hungarian Bar Association shall draw up internal rules for individual lawyers and single-member law firms, and the Hungarian Chamber of Notaries Public shall draw internal rules for notaries public within ninety days following the time of this Act entering into force.

(6) Service providers engaged in trading in goods, if not listed in the register referred to in Subsection (4) of Section 33, may accept cash payments of three million six hundred thousand forints or more only until 15 March 2008.

Modified legal provisions

Section 46

[no longer in effect]

Section 47

[no longer in effect]

Section 48

[no longer in effect]

Section 49

[no longer in effect]

Section 50

[no longer in effect]

Section 51

[no longer in effect]

Section 52

[no longer in effect]

Section 53

[no longer in effect]

Section 54

[no longer in effect]

Section 55

[no longer in effect]

Compliance with the legal provisions of the European Communities

Section 56

(1) This Act serves the purpose of conformity with the following legislation of the Communities:

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

b) Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of ‘politically exposed person’ and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.

(2) This Act contains provisions for the implementation of Regulation (EC) No. 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds.