Act LIII of 2017

on Preventing and Combating Money Laundering and Terrorist Financing

The aim of this Act is to prevent and combat the laundering of money or things of a monetary value originating from criminal offenses via activities exposed to the threat of money laundering and the supporting of terrorism with money or things of a monetary value in order to effectively enforce the prohibition of money laundering and terrorist financing. In order to facilitate the foregoing, the Parliament declares the following Act:

1. Scope of the Act

Section 1 (1) The scope of this Act shall cover any

a) credit institution;

b) financial service provider;

c) institution for occupational retirement provision;

d) voluntary mutual insurance fund;

e) entity taking in and delivering international post money orders;

f) entity engaged in activities related to real property transactions;

g) entity engaged in auditor activity;

h) entity carrying out accounting, tax expert, certified tax expert or tax advisory activity based on agency or work relations;

i) entity operating casinos or card rooms or organising betting not qualifying as remote gambling, remote gambling or online casino games;

j) trader of precious metals or items made of precious metals;

k) person trading in goods who accepts a total amount of cash payments of HUF 3,000,000 or more in the course of its activity;

l) attorney, law office, European Community lawyer, European Community lawyers' office (hereinafter collectively referred to as: "attorney"), registered in-house legal counsel, notary public;

m) trust;

n) service provider engaged in exchange services between virtual currencies and legal tenders, or virtual currencies;

o) custodian wallet provider;

p) service provider trading or acting as intermediaries in the trade of works of art, antiques, where the value of the transaction or a series of linked transactions amounts to HUF 3,000,000 or more;

q) service provider storing, trading or acting as intermediaries in the trade of works of art, antiques, when this is carried out by free ports, where the value of the transaction or a series of linked transactions amounts to HUF 3,000,000 or more; and

r) registered office service provider

established in or having a branch or place of business in Hungary (hereinafter referred to as: "service provider"), with the differences specified in Subsections (3) and (4).

(1a) The scope of this Act shall cover any entity established in Hungary or any other Member State of the European Union or in a third country, and which – by means of a permanent business unit established in Hungary, including branches as well – directly provides the customers with any of the services specified in Subsection (1) in the form of a permanent domestic operation [the content of Subsection (1) and this Subsection hereinafter collectively: "service provider"].

(2) The scope of this Act shall cover

a) customers of the service provider, as well as those with right of disposal over them and their representatives and proxies;

b) executive officers, employees and assisting family members of the service provider;

c) persons engaged in attorney activities as junior in-house legal counsels registered with the bar association under the direction of a registered in-house legal counsel (hereinafter referred to as: "junior in-house legal counsel").

(3) The scope of this Act shall cover the supervisory body specified in Section 5.

(4) The scope of this Act shall not cover

a) the service provider's activity related to a support that may be provided by the employer to its employee exempted from tax or with tax benefits pursuant to the Act on Personal Income Tax, if the sum granted as support may be used only for a certain scope of goods or services specified in the Act on Personal Income Tax,

b) the financial service provider's credit reference service and activity related to the operation of a payment system, as set out in Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (hereinafter referred to as: "Credit Institutions Act").

c) the performance of payments into payment accounts made as taxes, penalties and duties.

(5) The scope of this Act covers the Hungarian Central Bank (Magyar Nemzeti Bank, hereinafter referred to as: "MNB") only in regards to its supervisory activity and the provisions where the Act expressly names the MNB.

(6) The provisions of this Act relating to the establishment of business relationships shall apply *mutatis mutandis* also to notaries public carrying out the activities specified in Section 73(2).

Section 2 Section 26 shall apply to the service providers specified in Section 1(1)(a), (b) and (e) and the MNB, when such service provider or the MNB provides the money transfer service specified in Article 3(9) of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (hereinafter referred to as: "Regulation").

2. Definitions

Section 3 For the purposes of this Act, the following terms shall have the following meaning:

1. tax adviser, tax expert, certified tax expert: any person with professional qualifications obtained in accordance with the professional and exam requirements issued by the minister responsible for tax policy who possesses a license for tax advisory, tax expert or certified tax expert activities and is listed in the registry of tax advisors, tax experts and certified tax experts specified in the Act on the Rules of Taxation.

2. parent entity: any undertaking with dominant influence over another undertaking;

3. identification: recording of the data specified in Sections 7(2), 8(2) and (3) and 9(1) and (2) in a retrievable manner;

4. person trading in goods: the entity selling a product to the buyer, the trader or the processor in the scope of commercial activity;

5. commodity dealer: the commodity dealer defined in Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Rules of their Activities (hereinafter referred to as: "Investment Firms Act");

6. group: a group of undertakings consisting of a parent entity, its subsidiaries and branches and all undertakings in which the parent entity or any of its subsidiaries has dominant influence or holds interest;

7. electronic money: electronic money as defined in the Credit Institutions Act;

8. institution issuing electronic money: institution issuing electronic money as defined in Act CCXXXV of 2013 on Certain Payment Service Providers (hereinafter referred to as: "Payment Service Provider Act");

9. dominant influence: dominant influence as used in the definition of "parent entity" in Act C of 2000 on Accounting (hereinafter referred to as: "Accounting Act"), or a relationship between a person and an undertaking, based on which

a) the person with influence may decide on the division of the profits of the undertaking, reallocation of the undertaking's profits or losses or the strategy, business policy or sales policy of the undertaking;

b) it becomes possible to coordinate management of the company with the management of another company in order to achieve a common goal, regardless of whether the agreement was set out in the bylaws (articles of association) or another written contract,

c) joint control takes place via the partially identical composition (amounting to the majority necessary for making decisions) or fully identical composition of the undertakings' management and/or supervisory board, or

d) the person with influence exercises significant influence on the operation of another undertaking without capital relations;

10. activity belonging to the life insurance sector: activity belonging to the life insurance sector as defined in Annex 2 to Act LXXXVIII of 2014 on Insurance Activity (hereinafter referred to as: "Insurance Act");

11. European Union: the European Union and the European Economic Area;

12. fictive bank: a credit institution, financial service provider or organisation engaged in activity identical to those carried out by credit institutions or financial service providers that has no main office in its state of residence and is not a member of any regulated financial group;

13. negotiable voucher: negotiable voucher as defined by the Credit Institutions Act;

14. main office: the location where the service provider actually conducts its activity and which is the place of the service provider's central decision making;

15. third country: any state outside the European Union;

16. credit institution: the credit institution specified in the Credit Institutions Act, excluding the MNB;

17. *activity related to real property transactions:* mediation of the transfer of ownership, mediation of the lease rights of real property as a business where the monthly lease fee reaches or exceeds HUF 500,000 per transaction, as well as the sale and purchase of real property in own ownership as a business;

18. organisation without legal personality: an entity that is neither a legal person nor a natural person;

19. risk sensitivity approach: the procedure for preventing and combating money laundering and terrorist financing established based on the nature and amount of the business relationship or transaction order and the internal risk assessment specified in the internal rule specified in Section 65 based on the customer's circumstances;

19a. risk level: with regard to permanent business relationships the classification by which the scope and level of necessary customer due diligence measures is determined for the given customer;

20. accounting activity: accounting services as defined in the Accounting Act;

21. authority operating as a foreign financial intelligence unit: the authority of another Member State of the European Union or a third country, which – in particular with regard to the requirements of the Financial Action Task Force and the Egmont Group – carries out tasks identical or similar to those of authorities operating as a financial intelligence unit;

21a. external control function: assessment of the internal rules of procedure carried out by a party independent from the service provider to determine whether the service provider, based on the internal rules of procedure, is able to comply with the obligations provided in this Act and in the law based on the authorisation of this Act.

22. subsidiary: any undertaking, the operation of which is under the dominant influence of another undertaking. All subsidiaries of a subsidiary shall be considered as a subsidiary of the parent entity;

22a. custodian wallet provider: an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies;

23. correspondent relationship:

a) the provision of certain financial or investment services by a credit institution to another credit institution, including in particular the management of a payment account, cash supply, international transfer of funds, settlement of cheques and foreign exchange transactions;

b) relationship between two or more credit institutions or financial service providers providing similar services, including in particular the settlement of securities transactions and payment operations;

24. national risk assessment: the national-level assessment suitable for identifying, assessing, interpreting and continually reviewing the risks of money laundering and terrorist financing, as well as for establishing the national risk management procedures;

25. financial institution: financial institution as defined by the Payment Service Provider Act, as well as the institution operating the Post Settlement Centre (Posta Elszámoló Központ);

26. money laundering: the criminal conducts specified in Section 303-303/A of Act IV of 1978 on the Criminal Code – in force until 30 June 2013 – and in Sections 399-400 of Act C of 2012 on the Criminal Code (hereinafter referred to as: "Criminal Code");

27. authority operating as financial intelligence unit: the organisational unit of the National Tax and Customs Administration specified in a law;

28. financial service provider:

a) financial undertakings,

b) organisations carrying out fund processing activity not qualifying as a financial undertaking, in regards to their fund processing activity,

c) financial institutions, in regards to their activity falling under the scope of payment services,

d) institutions issuing electronic money, in regards to the issuing of electronic money and their activity falling under the scope of payment services,

e) voucher issuers,

f) currency exchange offices,

g) insurance companies, provided that they hold a license for activities belonging to the life insurance sector, in regards to these activities,

h) multi-agents and brokers as defined in the Insurance Act, in regards to their activities related to contracts belonging to the life insurance sector,

i) senior multi-agents and brokers as defined in the Credit Institutions Act,

j) investment firms,

k) commodity dealers, in regards to their activity falling under the scope of commodity trading services,

l) investment funds, in regards to their investment unit trading activity and their activity specified in the Investment Firms Act,

m) market operators, in regards to their activity specified in Act CXX of 2001 on the Capital Market (hereinafter referred to as: "Capital Market Act") and the Investment Firms Act;

28a. proof of source of funds: data or supporting documents which prove the legal source of funds involved in the transaction, thus in particular contracts or other official documents resulting from inheritance, compensation, civil law relationships naming the corresponding entitlements, certificate of income from employment, certificate of income from external service, other certificate of income, supporting documents relating to exchange rate gains, winnings or dividend;

29. financial undertaking: a financial undertaking as defined in the Credit Institutions Act;

30. currency exchange office: a broker carrying out currency exchange services pursuant to an agency contract concluded with a credit institution;

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

31a. registered office service provider: a registered office service provider as defined in the Act on the Rules of Taxation;

32. official certificate suitable for the proof of identity: identity cards, passports and card-form driver's licenses;

33. verification of identity (verification): verification of the identity of a customer, proxy, person with right of disposal or representative in accordance with Section 7(3)-(9) or of the beneficial owner in accordance with Sections 8(5) and 9(4);

34. executive officer of service provider: the natural person who is entitled to represent or exercise decisive powers on behalf or management powers within a legal person or organisation without legal personality;

35. executive officer of service provider specified in the internal rule as per Section 65: the natural person specified by the executive officer of the service provider in the internal rule specified in Section 65 with regard to the following criteria:

a) has appropriate knowledge in regards to the extent to which the service provider is exposed to the risks of money laundering and terrorist financing, and

b) has appropriate managerial powers to initiate or make decisions influencing exposure to risks;

36 terrorist financing: providing or collecting the material assets required for committing the criminal offence specified in Section 261(1) and (2) of Act IV of 1978, and the criminal conducts specified in Section 318 of the Criminal Code;

37. individual transaction orders linked in effect:

a) transactions ordered by a single customer within the same year under the same pretext and in regards to the same subject,

b) in the case of currency exchange offices, transactions ordered by a single customer within the same week with a value of HUF 100,000 or more,

c) in regards to the service providers specified in Section 1(1)(k), the payments and payment orders taking place based on instalment purchase;

38. beneficial owner:

a) the natural person who holds, either directly or indirectly, at least 25% of the voting rights or capital of a legal person or organisation without legal personality in accordance with Section 8:2(4) of Act on the Civil Code (hereinafter referred to as: "Civil Code") or otherwise exercises the actual control over the legal person or organisation without legal personality, if the legal person or organisation without legal personality is not a company listed on a regulated market subject to the publication rules set out in Community legislation or other equivalent international regulations,

b) the natural person who has dominant influence over a legal person or organisation without legal personality in accordance with Section 8:2(2) of the Civil Code,

c) the natural person on whose behalf a transaction is executed or who otherwise exercises actual control over the activity of a customer who is a natural person,

d) in regards to foundations, the natural person

da) who is the beneficiary of at least 25% of the foundation's assets, if the prospective beneficiaries have already been specified,

db) for whose benefit the foundation was established or is operated, if the prospective beneficiaries have not been specified yet,

dc) who is a member of the foundation's management body or exercises dominant influence over at least 25% of the foundation's assets, or

dd) who acts as the representative of the foundation in the absence of a natural person specified in Subparagraphs *da)-dc)*,

e) in regards to trust agreements, the following persons:

ea) the trustor(s); where the trustor is not a natural person, its beneficial owner in accordance with Paragraph *a)* or *b)*,

eb) the trustee(s); where the trustee is not a natural person, its beneficial owner in accordance with Paragraph *a)* or *b)*,

ec) the beneficiary or group of beneficiaries; where the beneficiary is not a natural person, its beneficial owner in accordance with Paragraph *a)* or *b)*,

ed) the natural person who otherwise controls the managed assets, and

ee) as the case may be, the person(s) controlling the trust activity; where the person controlling the trust activity is not a natural person, its beneficial owner in accordance with Paragraph *a)* or *b)*, and

f) in the absence of a natural person fitting the description set out in Paragraphs *a)* and *b)*, the executive officer of the legal person or organisation without legal personality;

39. voucher issuer: service provider with license for issuing negotiable vouchers;

40. guide: the following instructional documents issued for service providers by the supervisory body specified in Section 5 in its supervisory activity set out in this Act:

a) the decree issued for the service providers specified in Section 1(1)(a)-(f), (h)-(k) and (m)-(r),

b) the mandatory guide issued for the service providers specified in Section 1(1)(g), and

c) the mandatory guide and code issued for the service providers specified in Section 1(1)(l)

(hereinafter collectively referred to as: "guide");

41. customer:

a) who enters into a business relationship with the service provider or orders a transaction at the service provider, and

b) in regards to the service provider specified in Section 1(1)(f), who requests a quotation for the sale and purchase or leasing of the real property;

42. customer due diligence:

a) in the case specified in Section 6, the identification of the customer, the customer's classification by risk level (risk rating), verification of identity, understanding the aim and nature of the business relationship and the transaction order, along with the permanent monitoring of the same;

b) the customer due diligence measures performed at the time of a player's registration by the service provider operating a casino or card room or organising remote gambling or online casino games;

43. transaction:

a) any operation associated with the use of a service belonging to the service provider's scope of professional activities in the course of a business relationship, or

b) transaction orders;

44. *transaction order:* a transaction that is an ad hoc legal relationship between the customer and the service provider for the use of a service belonging to the service provider's scope of professional activities specified in Section (1)(a)-(e), (g)-(h) and (j)-(r);

45. business relationship:

a) the permanent legal relationship between the customer and the service provider established by a contract for the use of a service belonging to the scope of professional activities specified in Section 1(1)(a)-(e), (g)-(h), and (j)-(r),

b) in regards to service providers operating a casino or card room, the permanent legal relationship established via the first entry to the territory of the casino or card room, or in regards to organisers of remote gambling and online casinos, the registration of the player,

c) in regards to the service provider specified in Section 1(1)(f), the legal relationship between the customer and the service provider for the use of a service belonging to the service provider's scope of activities,

46. proof of source of wealth: the customer's declaration presenting the source of the customer's assets of a value exceeding HUF 3,000,000, including tangible or intangible assets;

47. virtual currency: a digital representation of value that is not issued or guaranteed by a central bank or a public authority; it does not possess a legal status of legal tender; it can be stored electronically, is accepted as a means of exchange, and thus can particularly be transferred and traded electronically;

Section 4 (1) For the purposes of this Act, the term "politically exposed person" shall mean any natural person who holds an important public function or held an important public function in at least the year preceding the

performance of the customer due diligence measures. The service provider shall be entitled to determine a period exceeding one year in its internal rule specified in Section 65 based on a risk sensitivity approach.

(2) For the purposes of Subsection (1), the following qualify as persons holding an important public function:

a) the head of state, the head of government, ministers, vice-ministers, secretaries of state, in Hungary: the Head of State, the Prime Minister, ministers, secretaries of state,

b) Parliament representatives and members of similar legislative bodies, in Hungary: Parliament representatives and nationality spokesmen,

c) members of the governing body of political parties, in Hungary: members and officers of the governing body of political parties,

d) members of the supreme court, the constitutional court or any high-level judicial body whose decisions cannot be appealed against, in Hungary: members of the Constitutional Court ("Alkotmánybíróság"), Courts of Appeal ("ítélőtáblák") and the Supreme Court ("Kúria"),

e) members of the Board of Directors of the court of auditors and the central bank, in Hungary: the Chair and Vice Chair of the State Audit Office ("Számvevőszék"), the Monetary Council and the Financial Stability Council,

f) ambassadors, chargés d'affaires and high-ranking officers of armed forces, in Hungary: the head of the central body of the policing body and his/her deputy, as well as the Chief of Staff of the Hungarian Defence Forces and his/her deputies,

g) members of the directing, controlling or supervisory bodies of undertakings in the majority ownership of the state, in Hungary: the executive officers of undertakings in the majority ownership of the state and the members of the managing bodies of such undertakings having management or supervisory powers,

h) heads of international organisations, their deputies and members of the managing bodies of such organisations or any person holding an equivalent function.

(3) For the purposes of this Act, the politically exposed person's spouse or partner; biological, adopted, step- or fostered child and any spouse, partner of biological, adopted, step- or fostered child shall be considered as a relative of the politically exposed person.

(4) For the purposes of this Act, the following shall be considered as persons in close relations with a politically exposed person:

a) any natural person who is the beneficial owner of a legal person or organisation without legal personality jointly with any of the persons specified in Subsection (2), or is in a close business relationship with such a person;

b) any natural person who is the sole owner of a legal person or organisation without legal personality established for the benefit of any of the persons specified in Subsection (2).

(5) The minister responsible for regulating the financial, capital and insurance market (hereinafter referred to as: "minister") shall inform the European Commission (hereinafter referred to as: "Commission") and the Member States of the categories of persons holding important public function as provided in Subsection (2), including those referring to international organisations as provided in Paragraph *h)* of Subsection (2).

Section 5 For the purposes of this Act, the following shall be considered as supervisory bodies:

a) in regards to the service providers specified in of Section 1(1)(a)-(e), the MNB acting in the scope of its duties related to supervision of the financial intermediary system (hereinafter referred to as: "Supervisory Body");

b) in regards to the service providers specified in Section (1)(1)(i), the gambling supervisory body;

c) in regards to the service providers specified in Section 1(1)(g), the Hungarian Chamber of Auditors;

d) in regards to the service providers specified in Section 1(1)(l), in accordance with the specific different provisions applicable to attorneys, registered in-house legal counsels and notaries public pursuant to this Act:

da) for attorneys and registered in-house legal counsels, the chamber which they are a member of (hereinafter referred to as: "regional bar association"),

db) for notaries public, the chamber which they are a member of (hereinafter referred to as: "regional chamber of notaries public");

e) in regards to the service providers specified in Section 1(1)(j), (k), (p) and (q), the trade licensing authority;

f) in regards to the service providers specified in Section 1(1)(f), (h), (n), (o) and (r), the authority operating as financial intelligence unit (hereinafter referred to as: "financial intelligence unit");

g) in regards to the service providers specified in Section 1(1)(m), the office specified in the Act on Trusts and the Rules of Their Operation (hereinafter referred to as: "Office").

3. Customer due diligence obligation

Section 6 (1) The service provider shall conduct the customer due diligence

a) when establishing a business relationship;

b) when executing a transaction order with an amount of at least HUF 4,500,000;

c) in the case of persons trading in goods, when executing a transaction order with an amount of at least HUF 3,000,000 in cash;

d) when executing a transaction order with an amount exceeding HUF 300,000 qualifying as a transfer of funds as defined in Article 3(9) of the Regulation;

e) in regards to organisers of betting not qualifying as remote gambling, prize payments with an amount of at least HUF 600,000 in the case of betting not qualifying as remote gambling not organised via telecommunications equipment or systems, and withdrawals from player balances in an amount of at least HUF 600,000 in the case of betting not qualifying as remote gambling organised via telecommunications equipment and systems;

f) when data, facts or circumstances indicating money laundering or terrorist financing arise, provided that no due diligence has been performed in accordance with Paragraphs *a)-e)* or *i)* yet;

g) if doubts arise as to the authenticity or appropriateness of previously recorded customer data,

h) where a change in customer identification data is recorded, and it becomes necessary to repeat the customer due diligence based on a risk sensitivity approach;

i) in the case of a currency exchange with an amount of at least HUF 300,000.

(2) The due diligence obligation specified in Paragraphs *b)*, *c)* and *i)* of Subsection (1) shall cover individual transaction orders linked in effect if their aggregate value is equal to or higher than the amount specified in Paragraphs *b)*, *c)* and *i)* of Subsection (1). In this case, the due diligence shall be performed at the time of acceptance of the transaction order with which the joint aggregate value of the transaction orders reaches the amount specified in Paragraphs *b)*, *c)* and *i)* of Subsection (1).

Section 6/A In the event of establishing a business relationship, the service provider shall perform and record in writing the customer's risk classification for the purpose of customer due diligence.

4. Customer due diligence measures

Section 7 (1) The service provider shall, in the cases specified in Section 6(1)(a) and (e)-(h), identify the customer, the proxy thereof, the person with right of disposal acting with the service provider and the representative acting with the service provider, and shall also perform a verification of their identity.

(2) The service provider shall record the following data in the scope of the identification:

a) if a natural person, his/her:

aa) first and last name,

ab) first and last name at birth,

ac) citizenship,

ad) place and date of birth,

ae) mother's maiden name,

af) residential address or, in the absence thereof, the current place of residence,

ag) identification document's type and number;

b) if a legal person or organisation without legal personality,

ba) its name and abbreviated name,

bb) its registered office's address or, for undertakings established abroad, Hungarian branch's address (if any),

bc) its main activity,

bd) the name and position of the persons with right to act on its behalf,

be) the data of the person authorised to accept service (if any) listed in Subparagraph *aa)* and *af)* of Paragraph *a)*,

bf) if a legal person registered in the company registry court's records, its company registration number, or if other legal person, the number of the decision relating to its establishment (entry into the records, registration) or its registration number,

bg) its tax number.

(3) The service provider shall require that the following instruments be presented for the verification of identity, or shall be entitled to query data from authentic records:

a) if a natural person:

aa) if a Hungarian citizen, his/her official certificate suitable for the proof of identity and official certificate certifying residential address; the latter is required where his/her residential address or current place of residence is in Hungary,

ab) if a foreign citizen, his/her travel document or identity card – provided that it entitles the person to stay in Hungary –, document certifying the right of residence or document providing right of residence, official certificate certifying Hungarian residential address, if his/her residential address or current place of residence is in Hungary;

b) if a legal person or organisation without legal personality, then in addition to presentation of the instrument specified in Paragraph *a)* of the person entitled to act on its behalf or as its agent, the instrument not older than thirty days certifying that

ba) the company was registered by the company registry court, or the company submitted its application for registration; in the case of a private entrepreneur, the commencement of the entrepreneurship activity was reported, or the private entrepreneur was registered,

bb) for domestic legal persons not subject to Subparagraph *ba)* of Paragraph *b)*, if the establishment thereof requires registration by an authority or court, that the registration took place,

bc) for foreign legal persons or organisations without legal personality, that they were registered or entered into the records in accordance with the laws of their country of establishment;

c) prior to submitting an application for registration with a court or authority to the respective court or authority, the memorandum of association of the legal person or organisation without legal personality.

(3a) The verification of the data specified in Subparagraph *ab)-ac)* and *ae)* of Paragraph *a)* of Subsection (2) may be omitted where such data is not included in the instrument presented in the course of the verification of identity.

(3b) In the case specified in Subsection (3a), the service provider shall also record the information that the data specified in Subparagraphs *ab)-ac)* and *ae)* of Paragraph *a)* of Subsection (2) were recorded in omission of the verification.

(4) In the case specified in Paragraph *c)* of Subsection (3), legal persons or organisations without legal personality shall certify within thirty days as of registration or entry into the records by the authority or court that such registration or entry into the records took place, and the service provider shall record the company registration number or other registration number.

(5) In order for the verification of identity, the service provider shall check the validity of the document certifying identity presented in accordance with Subsection (3), and, at the same time, shall also verify the authenticity of the document.

(6) In the course of the verification of identity, the service provider shall check the validity of the power of attorney for proxies, the right of disposal for persons with right of disposal, and the right of representation for representatives.

(7) If this is justified for the identification of the customer and the business relationship based on the risk sensitivity approach, then for the purpose of verification of identity, the service provider shall be entitled – instead of or in addition to the measures specified in Subsections (2)-(6) – to verify data relating to identity based on authentic records, from the operator of which the service provider is entitled to request data.

(8) For the purpose of preventing and combating money laundering and terrorist financing, the appropriate fulfilment of the obligations specified in this Act, the comprehensive fulfilment of the customer due diligence obligation, as well as for ensuring the efficiency of supervisory activity, in order to perform the verification of identity, the service provider shall make a copy of the instrument presented pursuant to Subsection (3) containing the data specified in Subsection (2), including any and all personal data indicated, but with the exception of the side of the official certificate certifying residential address which includes the personal identification number.

(8a) The service provider shall process all personal data obtained in the course of fulfilling its obligation specified in Subsection (8) and indicated in the instrument specified in Subsection (3), with the exception of the personal identification number included on the back side of the official certificate certifying residential address.

(9) The service provider operating a casino or card room shall be entitled to record the image of a natural person and to record video footage of the activity thereof within the facility, as well as to store the image in its electronic records, in order for preventing and combating money laundering and terrorist financing, for ensuring that the data it obtains in the course of the customer due diligence measures and the player's transactions can be linked and for the efficiency of the supervisory activity. The service provider operating a casino or card room shall retain video footage for 45 days as of its recording, and, when notified by the supervisory body specified in Section 5, shall extend this deadline until the closing of the supervisory body's procedure.

(10) The service provider may also perform the measures specified in Subsections (2)-(6) via a secure, protected electronic communications equipment operated by the service provider and preliminarily audited in the manner specified by the supervisory body provided in Section 5.

(11) The supervisory body specified in Section 5 shall issue a guide for the implementation of those specified in Subsection (10).

Section 8 (1) In the case specified in Section 6(1), the natural person customer shall – in the manner specified by the service provider – declare in writing in person or via a secure, protected electronic communications equipment operated by the service provider and preliminarily audited in the manner specified by the supervisory body provided in Section 5 if it acts on behalf or for the benefit of the beneficial owner.

(2) The service provider shall request disclosure of the following data relating to the beneficial owner in the declaration specified in Subsection (1):

a) his/her first and last name,

b) his/her first and last name at birth,

c) his/her citizenship,

d) his/her place and date of birth,

e) his/her residential address or, in the absence thereof, the current place of residence.

(3) The service provider shall, in addition to requesting the data specified in Subsection (2), also request the customer to make a declaration regarding whether the beneficial owner qualifies as a politically exposed person. If the beneficial owner is a politically exposed person, the declaration shall indicate based on which Paragraph of Section 4(2) the beneficial owner qualifies as a politically exposed person.

(4) If any doubt arises as to the identity of the beneficial owner, the service provider shall take any further measure prescribed by the supervisory body until the identity of the beneficial owner is established.

(5) The service provider shall verify the data relating to the identity of the beneficial owner based on the instrument presented to it, publicly accessible registries or other registries, from the operator of which the service provider is entitled to request data.

Section 9 (1) In the case specified in Section 6(1), the representative of a customer who is a legal person or organisation without legal personality shall – based on the accurate and up-to-date records kept by the customer – make a declaration in writing in person or via a secure, protected electronic communications equipment operated by the service provider and preliminarily audited in the manner specified by the supervisory body provided in Section 5 regarding the beneficial owner of the legal person customer or customer who is an organisation without legal personality, and the service provider shall request the following additional data relating to the beneficial owner to be disclosed in the declaration:

a) his/her first and last name,

b) his/her first and last name at birth,

c) his/her citizenship,

d) his/her place and date of birth,

e) his/her residential address or, in the absence thereof, the current place of residence,

f) the nature and extent of the ownership interest.

(1a) The representative of the customer as a legal person or organisation without legal personality shall mark all natural persons who fulfil the requirements in Section 3(38) as beneficial owners in the declaration to be made under Subsection (1).

(2) The service provider shall, in addition to requesting the data specified in Subsection (1), also request the customer to make a declaration regarding whether its beneficial owner qualifies as a politically exposed person. If the beneficial owner is a politically exposed person, the declaration shall indicate based on which Paragraph of Section 4(2) the beneficial owner qualifies as a politically exposed person.

(2a) In the case specified in Section 6(1)(a), the customer shall prove the forwarding of data of the beneficial owner to the central records specified in Section 25(1) by means of an instrument.

(3) If any doubt arises as to the identity of the beneficial owner, the service provider shall take any further measure prescribed by the supervisory body until the identity of the beneficial owner is established, including the understanding of the customer's ownership and control system.

(4) The service provider shall verify the data relating to the identity of the beneficial owner based on the instrument presented to it, publicly accessible registries or other registries, from the operator of which the service provider is entitled to request data.

(5) The customer's declaration specified in Subsection (1) may be omitted based on the risk sensitivity approach when the service provider records the data specified in Subsections (1) and (2) based on the instruments presented to it, publicly accessible registries or other registries, from the operator of which the service provider is entitled to request data.

(6) In the case specified in Subsection (5), the service provider shall also record the information regarding that the data specified in Subsections (1) and (2) were recorded in omission of the customer's declaration specified in Subsection (1).

(7) The service provider shall keep records of the measures taken for the identification of the beneficial owner and the verification of the beneficial owner's identity under Subsections (1)-(6).

(8) If the beneficial owner of the customer as a legal person or organisation without legal personality is the executive officer pursuant to Section 3(38)(f), the service provider shall identify the executive officer and perform

the verification of his/her identity. The service provider shall record the customer due diligence measures, and the information of it could not execute such measures.

Section 9/A (1) The natural person customer shall declare towards the service provider in writing in person or via a secure, protected electronic communications equipment operated by the service provider and preliminarily audited in the manner specified by the supervisory body provided in Section 5 whether it qualifies as a politically exposed person, a close relative of a politically exposed person, or as a person in close relation with a politically exposed person. If the natural person customer qualifies as a politically exposed person, a close relative of a politically exposed person, or as a person in close relation with a politically exposed person, the declaration shall indicate based on which Paragraph of Section 4(2)-(4) the natural person customer qualifies as a politically exposed person, a close relative of a politically exposed person, or as a person in close relation with a politically exposed person.

(2) If the natural person customer qualifies as a politically exposed person, a close relative of a politically exposed person, or as a person in close relation with a politically exposed person, the declaration, in addition to the data specified in Subsection (1), shall also include information on the source of funds and wealth.

(3) The service provider shall take measures for verifying the declaration made pursuant to Subsection (1) in the records available for this purpose by law or in a publicly accessible registry, as well as shall keep records of the measures taken for the purpose of such verification.

(4) The customer's declaration specified in Subsection (1) may be omitted when the service provider records the data specified in Subsection (1) based on the instruments presented to it, publicly accessible registries or other registries, from the operator of which the service provider is entitled to request data.

(5) In the case specified in Subsection (4), the service provider shall also record the information regarding that the data specified in Subsection (1) were recorded in omission of the customer's declaration specified in Subsection (1).

Section 9/B (1) In the case of insurances belonging to the life insurance group specified in Annex 2 to the Insurance Act, the customer shall declare towards the insurer in writing in person or via a secure, protected electronic communications equipment operated by the service provider and preliminarily audited in the manner specified by the supervisory body provided in Section 5 whether the beneficiary or the person entitled to service from the insurer based on the insurance contract and the beneficial owner thereof qualifies as a politically exposed person, a close relative of a politically exposed person, or as a person in close relation with a politically exposed person. If the beneficiary or the person entitled to service from the insurer based on the insurance contract qualifies as a politically exposed person, a close relative of a politically exposed person, or as a person in close relation with a politically exposed person, the declaration shall indicate based on which Paragraph of Section 4(2)-(4) he/she qualifies as a politically exposed person, a close relative of a politically exposed person, or as a person in close relation with a politically exposed person.

(2) The customer may make the declaration specified in Subsection (1) also after the establishment of the business relationship. In this case, the declaration shall be made concurrently with the or prior to the payment or concurrently with or prior to the partial or complete assignment of the insurance.

(3) If the authenticity of the declaration made pursuant to Subsection (1) is questionable, the service provider shall take measures for verifying the declaration made pursuant to Subsection (1) in the records available for this purpose by law or in a publicly accessible registry.

(4) The customer's declaration specified in Subsection (1) may be omitted when the service provider records the data specified in Subsection (1) based on the instruments presented to it, publicly accessible registries or other registries, from the operator of which the service provider is entitled to request data.

(5) In the case specified in Subsection (4), the service provider shall also record the information regarding that the data specified in Subsection (1) were recorded in omission of the customer's declaration specified in Subsection (1).

Section 10 (1) In the case specified in Section 6(1), the service provider shall record the following data regarding the business relationship:

a) the type, subject matter and term of the contract,

b) in order to determine the manner of customer due diligence, the customer' risk level (average, high or low),

c) the circumstances of performance (location, time, manner),

d) information on the purpose and planned nature of the business relationship.

(2) In addition to the data specified in Subsection (1), the service provider shall – based on a risk sensitivity approach – request disclosure of the information relating to the source of the funds and, in order for the verification of these information, the presentation of the documents relating to the source of the funds.

(3) The service provider may, based on a risk sensitivity approach, make establishment of the business relationship subject to the approval of the executive officer of the service provider specified in the internal rule specified in Section 65.

(4) The service provider may also perform the measures specified in Subsections (1)-(2) via a secure, protected electronic communications equipment operated by the service provider and preliminarily audited in the manner specified by the supervisory body provided in Section 5.

(5) In the event of a change in the data, the service provider shall perform only that customer due diligence measure which is necessary for recording the changed data, if the service provider's comprehensive due diligence obligation provided in Section 6(1)(g) does not prevail.

Section 11 (1) The service provider shall, in accordance with the statutory requirements relating to its activity, continuously monitor the business relationship – including the analysis of transactions performed during the existence of the business relationship – in order to determine whether the transaction concerned is in accordance with the data available to the service provider regarding the customer by law, and whether based on this it is necessary to perform measures against the customer in the scope of preventing money laundering.

(2) In the course of its continuous monitoring activity, the service provider shall monitor whether the customer's risk level was recorded in conformity with the data available. In the case of determining a change to the risk level, the service provider shall immediately carry out the measures corresponding to the customer's actual risk level which have not been performed yet, and shall adjust the analysis of the transactions completed to the risk level.

(3) The service provider shall, based on a risk sensitivity approach, pay particular attention to all transactions and financial operations which are

a) complex,

b) uncommon, thus in particular which

ba) represent an uncommonly large-value, or

bb) were executed in an uncommon transaction type, or

c) lack any legitimate purpose.

(4) The service provider specified in Section 1(1)(i) shall, based on a risk sensitivity approach, monitor the activity of the customer executing a financial transaction with a value of HUF 2,000,000 or more in the same calendar or game day in the scope of an enhanced procedure.

Section 12 (1) The service provider shall ensure that all data and instruments available regarding the customer under Sections 7-10 – along with the customer's risk classification – are up-to-date, thus the service provider shall verify the data available to it regarding its customers, in particular in the event of becoming aware of any change to the data and instruments available regarding the customer, for the purpose of verifying the data of the beneficial owner by law, or in order to comply with the obligation to cooperate in the field of taxation.

(2) The service provider shall comply with its verification obligation and perform the verification prescribed in Subsection (1) based on a risk sensitivity approach annually for high risk level, and at least in every five years for low risk level. If in the course of the verification any doubt arises on the part of the service provider as to the up-to-date state of the data and declarations, it shall repeat the customer due diligence measures in order to eliminate any such doubt.

(3) During the existence of a business relationship, the customer, the customer's proxy, the person with right of disposal acting with the service provider, and the representative acting with the service provider shall notify the service provider regarding any changes in the data disclosed in the scope of the customer due diligence and the beneficial owner within five business days as of becoming aware thereof.

(4) In order for the fulfilment of the obligation specified in Subsection (3), the service provider shall call the attention of its customer, its customer's proxy, the person with right of disposal and the representative to their obligation to provide notice of changes in the data.

(5) If the service provider cannot contact the customer at the communication channels provided by the customer even though the customer initiates the execution of transactions, the service provider shall, based on a risk sensitivity approach and not more than two times within three months, attempt to call the customer in writing, in a proven manner by post, to contact the service provider, by informing the customer of the potential legal consequences at the same time. Following the second unsuccessful notification, the service provider shall refuse to execute transactions of a value reaching HUF 4,500,000 until the customer or the customer's proxy contacts the service provider.

Section 13 (1) The service provider shall perform the verification of the identity of the customer and the beneficial owner prior to establishing a business relationship, excluding the cases set out in Subsections (2)-(6).

(2) The service provider may perform the verification of the identity of the customer and the beneficial owner also during the existence of the business relationship when this is necessary in order to avoid interruption of its regular operation, and when the probability of money laundering and terrorist financing is low. In this case, the verification shall be completed before the first transaction is executed.

(3) (3) For insurances belonging to the life insurance group specified in Annex 2 to the Insurance Act prior to establishing the business relationship, the insurer shall, in addition to identifying the customer and the beneficial owner and performing the verification of their identity:

a) determine the name of any beneficiary and any person entitled to service from the insurer based on the insurance contract known at the time of conclusion of the contract, and

b) record all information relating to any beneficiary and any person entitled to service from the insurer based on the insurance contract not known at the time of conclusion of the contract necessary for subsequent identification;

(4) For insurances belonging to the life insurance group specified in Annex 2 to the Insurance Act, when the identity of the beneficiary, the person entitled to service from the insurer based on the insurance contract, or of the person entitled to accept performance determined by the beneficiary is not known upon the conclusion of the contract, the verification of the beneficiary, the person entitled to service from the insurer based on the insurance contract, or of the person entitled to accept performance determined by the beneficiary shall be performed at the latest concurrently with the payment or the entitled person's enforcement of the rights originating from the contract (policy).

(5) Service providers entitled to open payment accounts and service providers entitled to open customer accounts, securities accounts and securities deposit accounts shall, when the statutory requirements thereof are met, be entitled to open accounts, provided that they ensure that the customer, the proxy, the person with right of disposal and the representative cannot perform any operations until the customer and the beneficial owner has been identified and the verification of their identity has been performed.

(6) When the statutory requirements thereof are met, mutual insurance funds shall be entitled to open personal accounts as defined in Act XCVI of 1993 on Mutual Insurance Funds (hereinafter referred to as: "Insurance Fund Act"), provided that they ensure that the customer and the service beneficiary cannot receive services until the verification of the identity of the customer and the beneficial owner has been performed. If a member dies, the service provider shall identify the person designated as beneficiary for the event of death or the inheritor prior to executing the transaction. When the statutory requirements thereof are met, institutions for occupational pension provision shall be entitled to open member accounts as defined in Act CXVII of 2007 on Occupational Pension and its Institutions (hereinafter referred to as: "Occupational Pension Act"), provided that they ensure that the member, the annuitant and the beneficiary cannot receive service until the verification of the identity of the member and the beneficial owner has been performed.

(7) Trusts shall record all information relating to any beneficiary not known at the time of conclusion of the contract required for subsequent identification and the verification of identity. In this case, the verification of identity shall take place concurrently with or prior to the payment or concurrently with or prior to the beneficiary enforcing its rights originating from the contract.

(8) If the service provider is unable to perform the customer due diligence measures specified in Sections 7-10, it shall, in relation to the customer concerned, refuse to perform operations, establish business relationships or execute transactions through the payment account based on the customer's order, and shall terminate its business relationship therewith.

(9) If the customer is a legal person or an organisation without legal personality, after performing the due diligence on the person acting on its behalf or as its agent, the due diligence shall be performed also on the legal person or organisation without legal personality.

(10) Repeated performance of the customer due diligence measures specified in Sections 7-10 may be omitted where

a) the service provider has already performed the customer due diligence measures specified in Sections 7-10 related to another business relationship or transaction order in regards to the customer, the proxy, the person with right of disposal and the representative,

b) it has established the identity of the customer, the proxy, the person with right of disposal and the representative in relation to the present business relationship or transaction order pursuant to Section 7(2)-(6), and

c) no change took place in regards to the data specified in Sections 7(2), 8(2) and (3), 9(1) and (2) and 10(1)(b).

Section 14 (1) When executing a transaction order with an amount less than HUF 4,500,000 – or a currency exchange with an amount HUF 100,000 or more –, the service providers specified in Section 1(1)(a-d) shall, for the purpose of preventing and combating money laundering and terrorist financing, record the data specified in Section 7(2)(a)(aa) and (ad) for natural person customers, or the data specified in Section 7(2)(b)(ba) and (bb) and Section 14/A(2)(a) for customers who are legal persons or organisations without legal personality, and may request that the instruments specified in Section 7(3) be presented.

(2) By derogation from Subsection (1), when a cash payment with an amount less than 300,000 – which is in addition to the fee required under the contract – is made, service providers engaged in the activity specified in

Section 3(28)(g) shall, for the purpose of preventing and combating money laundering and terrorist financing, record the data specified in Section 7(2)(a)(aa) and (ad), or – for customers who are legal persons or organisations without legal personality – the data specified in Section 7(2)(b)(ba) and (bb) and Section 14/A(2)(a), and may request that the instruments specified in Section 7(3) be presented.

(3) By derogation from Subsection (1), when executing a transaction order – except for payments to a payment account with an amount less than 300,000 initiated in Hungary relating to the use of goods or services to be provided in Hungary –, the institution operating the Post Settlement Centre specified in Section 3 25. shall, for the purpose of preventing and combating money laundering and terrorist financing, record the data specified in Section 7(2)(a)(aa) and (ad) or (af), or – for customers who are legal persons or organisations without legal personality – the data specified in Section 7(2)(b)(ba) and (bb) and Section 14/A(2)(a), and may request that the instruments specified in Section 7(3) be presented.

(4) When executing a transaction order with an amount of HUF 300,000 or more, for the purpose of fulfilling the obligation specified in Section 6(2), the service providers specified in Section 1(1)(e-h), (j-k) and (m) shall record the data specified in Section 7(2)(a)(aa) and (ad) for natural person customers, or the data specified in Section 7(2)(b)(ba) and (bb) and Section 14/A(2)(a) for customers who are legal persons or organisations without legal personality, and may request that the instruments specified in Section 7(3) be presented.

Section 14/A (1) In the case of executing a transaction order specified in Section 6 (1)(b)-(d) and (i), the service provider shall identify the customer, the customer's proxy, the person with right of disposal and the representative in regards to all data specified in Section 7(2), shall perform the verification of their identity, make a copy of the customer's instrument provided in Section 7(3), and further, shall take the customer due diligence measures specified in Sections 8-9/A.

(2) In the case specified in Section 6(1), the service provider shall record the following data regarding the transaction:

a) the subject matter and amount of the order,

b) the circumstances of performance (location, time, manner).

(3) In addition to the data specified in Subsection (2), the service provider shall – based on a risk sensitivity approach – request disclosure of the information relating to the source of the funds and, in order for the verification of these information, the presentation of the documents relating to the source of the funds.

(4) The service provider shall, based on a risk sensitivity approach, make execution of the transaction order subject to the approval of the executive officer of the service providerspecified in the internal rule specified in Section 65.

(5) If the service provider is unable to perform the customer due diligence measures specified in Subsections (1)-(3), it shall refuse to execute transaction orders regarding the customer in question.

(6) The service provider shall comply with its monitoring obligation relating to customers regularly placing transaction orders as provided in Section 11 for business relationships. The service provider shall determine the scope of customers qualifying as "customers regularly placing transaction orders" in its internal rule based on its own risk assessment as provided in Section 65.

(7) In the event of a change in the data, the service provider shall perform only that customer due diligence measure which is necessary for recording the changed data, if the service provider's customer due diligence obligation provided in Section 6(1)(g) does not prevail.

5. Simplified customer due diligence

Section 15 (1) The service provider shall perform the following customer due diligence measures in the cases described by low risk level in its internal rule based on its own risk assessment as provided in Section 65:

a) shall record the data determined in Section 7(2);

b) shall obtain a copy of instruments specified in Section 7(3) for the purpose of verification of identity;

c) shall conduct the procedures prescribed in Section 8 and 9 concerning the identity of the beneficial owner;

d) shall conduct the procedures prescribed in Sections 9/A and 9/B concerning the determination of the nature of a politically exposed person;

e) shall fulfil the monitoring obligations provided in Sections 11 and 12.

(2) The service provider shall immediately perform the customer due diligence corresponding to the higher risk level, if any data referring to a different risk level of the customer was obtained on the basis of the measures specified in Paragraphs *c)-e)* of Subsection (1).

(3) The service provider may also perform the measures specified in Subsection (1)

a) via a secure, protected electronic communications equipment operated by the service provider and preliminarily audited in the manner specified by the supervisory body provided in Section 5, or

b) based on the copy of documents and declarations sent by the customer by post, if the customer fails to appear in person.

(4) By derogation from Subsection (1), the institution operating the Post Settlement Centre shall record the data specified in Section 7(2), and may, for the purpose of verification of identity, request that the instruments specified in Section 7(3) be presented when executing transaction orders which jointly fulfil the following conditions:

a) its customer has no residential address or registered office in a high-risk third country with strategic deficiencies;

b) the amount of the transaction order exceeds HUF 300,000, but is less than HUF 3,000,000; and

c) the transaction order is aimed to serve as an exchange for the provision of goods or services initiated and to be performed in Hungary.

6. Enhanced customer due diligence

Section 16 (1) The service provider shall perform enhanced customer due diligence measures, if the customer is described by high risk. The customer shall be considered as high-risk in the following cases:

a) the customer is from a high-risk third countries with strategic deficiencies,

b) in the cases set out in the internal rule based on its own risk assessment specified in Section 65,

c) in the case of remote identification specified in Section 17,

d) the customer or its beneficial owner is a politically exposed person, or a close relative of a politically exposed person, or a person in close relation with a politically exposed person, and

e) in other cases set out in the guide issued by the supervisory body specified in Section 5.

(2) In the cases specified in Paragraphs *b)-e)* of Subsection (1), in addition to the customer due diligence measures specified in Sections 7-12, the service provider shall also perform the following customer due diligence measures:

a) business relationships may be established only following the approval of the executive officer of the service provider set out in its internal rule specified in Section 65,

b) shall perform the continuous monitoring of the business relationship as specified in Section 11(1) in an enhanced procedure set out in the internal rule specified in Section 65.

(3) In the cases specified in Paragraph *b)-e)* of Subsection (1), in addition to the customer due diligence measures specified in Subsection (2), the service provider may perform the following customer due diligence measures:

a) may obtain information on the source of the customer's wealth,

b) may perform the measures aimed at the verification of identity specified in Sections 7(3) and 8 personally or via a secure, protected electronic communications equipment operated by the service provider and preliminarily audited, or by means of remote identification specified in Section 17(2) in collaboration with a notary public, foreign representation or the authority of the state of issue of instrument authorised to make certified copy,

c) may perform the enhanced customer due diligence measures set out in the internal rule specified in Section 65.

Section 16/A (1) The service provider shall, prior to establishing a business relationship with or executing a transaction order for a customer from a high-risk third country with strategic deficiencies, act as follows in addition to the customer due diligence measures specified in Sections 7-12:

a) shall request the further information set out in the internal rule specified in Section 65 be made available with regard to the

aa) customer and the beneficial owner,

ab) business relationship,

ac) source of funds and wealth of the customer and the beneficial owner, and

ad) the reasons of the transactions to be executed and already executed,

b) shall make establishment of the business relationship or execution of the transaction order subject to the approval of the executive officer provided in the internal rule specified by Section 65, and

c) shall perform the continuous monitoring of the business relationship specified in Section 11(1) in an enhanced procedure set out in the internal rule specified in Section 65.

(2) The service provider may, prior to establishing a business relationship with or executing a transaction order for a customer from a high-risk third country with strategic deficiencies, apply the following measures:

c) may perform the enhanced customer due diligence measures set out in the internal rule specified in Section 65,

b) may introduce a reporting obligation, or

c) may apply limitations provided in the internal rule specified by Section 65.

(3) The service provider specified in Section 1(1)(a) and (b) shall review and modify as appropriate its correspondent relationship with the service provider established in a high-risk third country with strategic deficiencies.

(4) The minister shall inform the Commission of the measures specified in Subsections (2) and (3).

Section 17 (1) For the purposes of the identification and the verification of identity, if the customer, the person with right of disposal, the representative or the proxy failed to appear in person for identification and the verification of identity, the service provider shall require filing of an authentic copy of the instrument specified in Section 7(3) containing the data specified in Section 7(2) in cases where the identification was not carried out via a secure, protected electronic communications equipment operated by the service provider and preliminarily audited.

(2) The authentic copy of the instrument specified in Subsection (1) may be accepted for performance of the identification and the verification of identity if

a) it was authenticated by a notary public or a Hungarian foreign representation authority in accordance with the provisions of Act XLI of 1991 on Notaries Public (hereinafter referred to as: "Notaries Public Act") relating to the authentication of copies, or

b) the copy was made by an authority of the state where the instrument was issued that is entitled to issue authentic copies and – unless an international convention provides otherwise – the Hungarian foreign representation authority endorsed the authority's signature and stamp indicated on the copy.

(3) For opening a customer account specified in Paragraph 130 of Section 5(1) of the Capital Market Act, a securities account specified in Paragraph 46 of Section 5(1) of the same, or a securities deposit account, the customer may, in order for the verification of identity, submit the instruments specified in Section 7(3) and the declaration specified in Sections 8-9/A electronically – in particular in a scanned format, via email – or via fax if no data, facts or circumstances indicating money laundering or terrorist financing arise. In this case, for the purpose of opening the account, the customer may also certify the existence of his/her payment account to and from which a payment is credited to or charged from the customer account (hereinafter referred to as: "certified payment account") electronically or via fax, as specified in this Subsection. Only accounts managed by the service providers specified in Section 22(1) may be accepted as certified payment accounts. Until the customer's personal appearance for the purpose of identification and the verification of identity or until submission of the instruments specified in Subsections (1) and (2), except for the settlement of transactions concerning a customer account, securities account or securities deposit account, only payments of funds via simple transfer concerning the customer account opened in accordance with this Subsection may be performed, in a manner so that deposits may be made only from the customer's certified payment account and withdrawals may be made only to the customer's same certified payment account.

(4) The service provider managing customer accounts, securities accounts or securities deposit accounts shall, in order to check the data recorded by it in accordance with Subsection (3) identifying the customer, request data – sending the customer's data identifying him/her as a natural person – from the service provider managing the certified payment account regarding whether the customer was identified in regards to the certified payment account and whether the data provided by the customer regarding the customer account, securities account and securities deposit account are correct The contacted service provider shall perform the data request within 8 days. If the contacted service provider does not manage a payment account for the customer, it shall delete the data sent by the service provider managing a customer account, securities account or securities deposit account in the course of the data request without delay after performing the data request.

Sections 18-21

7. Customer due diligence measures performed by other service providers

Section 22 (1) The service provider shall be entitled to accept the result of the customer due diligence specified in Sections 7-10 if the customer due diligence

a) was performed by a service provider established or having a branch or place of business in Hungary or another Member State of the European Union, or

b) was performed by a service provider established or having a branch or place of business in a third country that meets the requirements set out in Subsection (3).

(1a) Accepting the result of the customer due diligence specified in Subsection (1) shall not be prevented by the fact that the scope of instruments and data serving as a basis for the requirements do not correspond to those provided in this Act.

(2) In the case specified in Subsection (1), the service provider accepting the result of the customer due diligence performed by another service provider shall be responsible for fulfilment of the requirements specified in Sections 7-10.

(3) If the customer due diligence was performed by a service provider established or having a branch of place of business in a third country, the result thereof may be accepted in accordance with Subsection (1) if

a) the service provider applies the requirements regarding the customer due diligence set out in this Act or equivalent requirements, and is supervised in accordance with the requirements set out in this Act or equivalent requirements, or

b) the service provider's registered office, branch or place of business is in a country that stipulates requirements equivalent to those set out in this Act.

(4) The service provider shall not be entitled to accept the result of the customer due diligence specified in Sections 7-10 if the customer due diligence was performed by a service provider established or having a branch or place of business in a third country qualifying as a high-risk third country with strategic deficiencies.

(5) The prohibition set out in Subsection (4) shall not apply to accepting the result of the customer due diligence specified in Sections 7-10 from the branch or subsidiary of a service provider established in Hungary or another Member State of the European Union located in a third country qualifying as a high-risk third country with strategic deficiencies, if the branch or subsidiary meets the group-level policies and procedures established against money laundering and terrorist financing specified in Section 62.

(6) The service provider shall be entitled to accept the result of the customer due diligence from the service provider belonging to the same group if

a) the members of the group – in accordance with the group-level policies and procedures specified in Sections 60-62 – apply the customer due diligence and record-keeping requirements provided in this Act or other requirements equivalent to those, and

b) the competent authority of the Member State of establishment or the third country shall supervise on a group level.

Section 23 (1) In the case specified in Section 22(1), the service provider shall be entitled to make available to another service provider the data requested for the purpose of performing the customer due diligence specified in Sections 7-10 if the customer concerned consents to this.

(2) In the case specified in Section 22(1), provided that the requirements set out in Section 22(3) are met, if the service provider performing the customer due diligence and the service provider accepting the result of the customer due diligence agreed on making the result of the customer due diligence available, the service provider performing the customer due diligence shall, upon written request by the service provider accepting the result of the customer due diligence, make available without delay to the service provider accepting the result of the customer due diligence a copy of the data recorded for the purpose of the identification and verification of identity of the customer or the beneficial owner and any other documentation relating to the identity thereof, provided that the customer concerned consents to this.

Section 24 The provisions of Sections 22 and 23 do not need to be applied for outsourcing based on contractual relationships and agency activities.

7/A. Special customer due diligence measures

Section 24/A (1) The service provider specified in Section 1(1)(a) and (b) shall, prior to establishing a correspondent relationship with a service provider established abroad which includes the settlement of amounts and the execution of transactions aimed at the settlement of amounts,

a) perform an assessing analysis for assessing and evaluating the set of tools used by the service provider established abroad for preventing money laundering and terrorist financing;

b) set out the scope of its own responsibility and that of the service provider established abroad with regard to the correspondent relationship;

c) ensure that the service provider established abroad has performed the verification of the identity of the customer with direct access to the correspondence account and that it continuously monitors direct access to the correspondence account; and

d) ensure that the service provider established in Hungary is able to provide the relevant customer due diligence data upon request.

(2) The service provider specified in Section 1(1)(a) and (b) shall, on a risk sensitivity basis, regularly examine the risk money laundering entailed by the given correspondent relationship.

(3) Correspondent relationships may be established with service providers established abroad only subject to approval of the executive officer set out in the internal rule specified in Section 65 of the service provider specified in Section 1(1)(a) and (b).

(4) The service provider specified in Section 1(1)(a) and (b) may not establish or maintain correspondent relationships with fictive banks or any service provider who maintains a correspondent relationship with a fictive bank.

(5) The service provider specified in Section 1(1)(a) and (b) shall be entitled to determine based on a risk sensitivity approach whether it intends to apply the customer due diligence measures specified in Subsections (1)-(3) prior to establishing a correspondent relationship with a service provider established in a Member State of the European Union.

Section 24/B In the course of establishing complex business relationships which include more than one customers concerned by customer due diligence at the same time, the service provider shall perform the customer due diligence per each customer, and shall take account of the overall risk represented by them for risk classification.

Section 24/C (1) When issuing electronic money, the service provider shall perform the customer due diligence measure set out in Section 11(1) and may, for the purpose of identifying the customer or the business relationship or transaction order in order for preventing and combating money laundering and terrorist financing, record the data specified in Section 7(2), and may request presentation of the instruments specified in Section 7(3) for the verification of identity where

a) the payment instrument used for storing electronic money is not rechargeable or is rechargeable but has an upper limit of HUF 45,000 or less per month for payment operations and can only be used in Hungary;

b) the current amount of electronic money stored electronically does not exceed HUF 45,000;

c) the electronic money can be used only for purchasing goods or services;

d) the amount stored on the electronic money cannot be recharged from electronic money in regards to which the customer was not identified; and

e) the issuer of electronic money checks the transaction or business relationship appropriately in order to screen out uncommon transactions and data, facts or circumstances indicating money laundering or terrorist financing.

(2) The service provider shall perform all customer due diligence measures specified in Sections 7-10 where

a) the amount withdrawn in cash or redeemed for cash from the amount issued to it by the electronic card's holder exceeds HUF 15,000, or

b) the paid amount exceeds HUF 15,000 per operation in the case of remote payment operation.

(3) Where the payment instrument for storing unregistered electronic money was issued by a service provider established or having a branch or place of business in a third country, any payment from this payment instrument may be accepted if it meets the requirements specified in Subsections (1)-(2) or other requirements equivalent to those.

8. Central records of information on beneficial owners

Section 25 (1) The customer who is a legal person or an organisation without legal personality shall report the data of its beneficial owner as specified in Section 9(1) to the central records established for storing such data not later than within 5 business days from the commencement of its activity, and shall subsequently report any change concerning the beneficial owner within 5 business days.

(1a) The service provider and the supervisory body shall report to the body keeping central records specified in Subsection (1) if it detects any difference between the beneficial owner data stored in the central records and those available to it. The body keeping records, after considering the content of the report, shall either rectify or maintain the data stored in the central records within 15 days from the receipt of the report.

(2) The supervisory body specified in Section 5, the financial intelligence unit, the investigative authority, the internal affairs division of the police that investigates professional misconduct and criminal acts, the counter-terrorist body, the national security services, the prosecutor's office, the court and the state tax authority shall be entitled to request data from the central records specified in Subsection (1) for the purpose of fulfilling its tasks set out in this Act without limitation, while the service provider shall be entitled to the same by means of direct access for the purpose of performing the customer due diligence measures specified in Sections 7-12.

(3) Third parties may request data from the central records specified in Subsection (1) – except for the data relating to the beneficial owners in the case of trust agreements as specified in this Act – in the scope of an individual data service, only to the extent that is strictly necessary for the purpose of use.

(3a) Third parties may request data from the central records specified in Subsection (1) in the scope of an individual data service with regard a person qualifying as beneficial owner in the case of trust agreements, if the given third person

a) proves its legitimate interest in accessing such data, or

b) submits a written request in regards to a trust in which legal person or organisation without legal personality it has a majority influence either directly or indirectly.

(3b) The person submitting request for data under Subsections (3) and (3a) shall be entitled to learn the name, date of birth, citizenship and country of residence of the legal person, organisation without legal personality, or of the person qualifying as the beneficial owner in the case of trust agreement, as well as the type and extent of the beneficial ownership interest as provided in Section 3(38).

(4) Disclosure of the data shall not violate the personality rights and privacy rights of the person concerned by the data request.

(5) By derogation from Subsections (2) and (3), the access of service providers – except for the service providers specified in Section 1(1)(a-e) and (l) – and third parties to the central records specified in Subsection (1) may be partially or fully restricted exceptionally and on a case-by-case basis if:

a) access to the data of the beneficial owner would incur the risk of the commitment of a criminal offence against the person or property of the beneficial owner;

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

(5a) In the case specified in Subsection (5), an appeal against the decision restricting the access may be submitted.

(6) The detailed rules relating to the recording of the data and information specified in Section 9 relating to the beneficial owners of customers who are legal persons or organisations without legal personality are set out in the Act on the Central Records of the Data of Beneficial Owners.

8/A Central records of bank accounts and safes

Section 25/A (1) The service provider keeping the bank account shall inform the authority keeping the central records of bank accounts and safes of the following data of payment accounts identified by an international bank account number specified in Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009:

a) first and last name of the account holder, in the case of a non-natural person, the name of the holder organisation;

b) first and last name of the person(s) with right of disposal over the account;

c) first and last name of the beneficial owner of the account holder as specified in Section 9;

d) account number;

e) date of opening or termination of the account.

(2) The data reporting specified in Subsection (1) shall be performed not later than within 5 business days from concluding the payment account contract, while any subsequent change to the data shall be reported within 5 business days.

Section 25/B (1) The service provider which provides safe service shall inform the authority keeping central records of bank accounts and safes of the following data of safe service contracts:

a) first and last name of the person who rents the safe, in the case of a non-natural person, the name of the owner organisation;

b) first and last name of the person(s) with right of disposal over the safe;

c) term of the safe service contract.

(2) The data reporting specified in Subsection (1) shall be performed not later than within 5 business days from concluding the safe service contract, while any subsequent change to the data shall be reported within 5 business days.

9. Data accompanying fund transfers

Section 26 (1) The competent authority responsible for monitoring conformity with the provisions against money laundering and terrorist financing specified in Articles 8 and 12 of the Regulation is the Supervisory Body, while in regards to the MNB, the financial intelligence unit.

(2) The Member State's authority competent in the field of combating money laundering and terrorist financing specified in Article 14 of the Regulation are the Supervisory Body and the financial intelligence unit.

(3) At the request of the bodies specified in Subsection (2) acting in their scope of competence specified in Article 14 of the Regulation, the service provider shall disclose to them the data relating to the paying party and the beneficiary specified in Article 4 of the Regulation.

(4) The service provider shall retain the data relating to the paying party and the beneficiary specified in Article 4 of the Regulation in accordance with Sections 57 and 58.

(5) The competent authority specified in Article 17(4) and (7) and Articles 19-22 of the Regulation is the Supervisory Body, while in regards to the MNB, the financial intelligence unit.

(6) In the course of the audit, the Supervisory Body shall act in accordance with the provisions of the Act on the General Rules of Administrative Proceedings and Service, by applying the deviations provided in Act CXXXIX of 2013 on the National Bank of Hungary (hereinafter referred to as: "National Bank Act"), while the financial intelligence unit shall act in accordance with the provisions of the Act on the General Rules of Administrative Proceedings and Service.

(7) In the case of a violation of the Regulation's provisions or the inappropriate performance of the obligations set out in the Regulation, the Supervisory Body shall apply the measures set out in Section 69(1) in proportion to the severity of the violation, and shall prohibit the service provider from conducting fund payment activities until the unlawful situation is remedied.

(8) The penalty specified in Section 69(1)(h) may be imposed on the service provider that omits to perform or performs late or deficiently those set out in the Regulation and the Supervisory Body's decision.

(9) In the case of a violation of the Regulation's provisions or the inappropriate performance of the obligations set out in the Regulation, the financial intelligence unit shall apply the measures set out in Section 69(1)(a) and (b) in proportion to the severity of the violation.

(10) In the case of a violation of the Regulation's provisions or the inappropriate performance of the obligations set out in the Regulation, the Supervisory Body and the financial intelligence unit shall act in accordance with Section 69(5) and (6) in regards to legal persons and organisations without legal personality.

(11) In the case of a violation of the Regulation's provisions or the inappropriate performance of the obligations set out in the Regulation, the service provider shall make a report to the Supervisory Body and the financial intelligence unit in accordance with Section 72.

(12) In the cases specified in Articles 2(5), 5(2), 6(2) and 7(3) and (4) of the Regulation, the official exchange rate published by the MNB on the day of receipt of the transaction order for fund transfer or, for currencies not included in the MNB's exchange rate list, the exchange rate of such currencies converted into EUR included in the MNB's communication valid on the day of receipt of the transaction order for transfer shall be applied for calculating the EUR value of the sum transferred.

(13) The service provider shall not be obliged to apply the provisions of the Regulation to fund transfers within Hungary complying with the requirements set out in Article 2(5) of the Regulation.

10. Risk assessment

Section 27 (1) For the purpose of performing the tasks falling into the scope of the duties specified in this Act, the service provider shall prepare an internal risk assessment – proportionate to the nature and size of the service provider – based on the nature and amount of the business relationship or transaction order and the circumstances of the customer, the product, the service and the equipment used.

(2) For the purpose of preparing the internal risk assessment specified in Subsection (1), the service provider shall identify and evaluate the risk factors related to the nature and amount of the business relationships relationship or transaction order, the customer, the product, the service, the geographic area and the equipment used in order to determine and evaluate the risks.

(3) The service provider shall record in writing, update and make available to the competent authorities – in the course of the authorising and supervisory activity – the risk assessment specified in Subsection (1).

(4) The internal risk assessment does not need to be prepared if the supervisory body specified in Section 5 provides option for this in the guide provided to the service provider.

(5) Based on the internal risk assessment specified in Subsection (1), the service provider shall, in order to mitigate and manage the risks, establish its internal rules of procedure in the internal rule specified in Section 65 based on the nature and amount of the business relationship or transaction order and the circumstances of the customer, the product, the service and the equipment used, and – where justified by the its nature and size – the

service provider shall operate an external control function to control the compliance of the internal rules of procedure.

(6) The service provider shall take into consideration the result of the national risk assessment for preparing the internal risk assessment specified in Subsection (1) and in order to mitigate and manage the risks.

(7) Application of the internal risk assessment specified in Subsection (1) and the internal rules of procedure specified in Subsection (5) shall be subject to the approval of the service provider's executive officer set out in the internal rule specified in Section 65.

(8) The service provider obliged to prepare an internal risk assessment shall monitor the risks of money laundering and terrorist financing, review the internal rules of procedure as necessary, and shall modify them subject to the approval of the service provider's executive officer set out in the internal rule specified in Section 65.

Section 28 (1) For exercising the supervisory activity specified in Section 66, the supervisory body specified in Section 5 shall prepare a supervisory risk assessment – proportionate to the nature and size of the service provider – based on the nature and size of the service provider or the sector and the circumstances of the customer, product, service and equipment used that is typical to the service provider or sector.

(2) The supervisory body specified in Section 5 shall identify the risks of money laundering and terrorist financing existing based on the circumstances of the customer, product, service and equipment used that is typical to the service provider or sector, utilising all information available under Section 27 therefor.

(3) The supervisory body specified in Section 5 shall consider the result of the national risk assessment for preparing the supervisory risk assessment specified in Subsection (1).

(4) For exercising the supervisory activity specified in Section 66, the supervisory body specified in Section 5 shall, taking into consideration the supervisory risk assessment, prepare the supervisory rules of procedure – proportionate to the nature and size of the service provider – based on the nature and size of the service provider or the sector and the circumstances of the customer, product, service and equipment used that is typical to the service provider or sector.

(5) The supervisory body specified in Section 5 shall monitor the changes of risks of money laundering and terrorist financing concerning the sector supervised by it already identified in the risk assessment, shall identify the risks that have not been identified yet, and shall update its risk assessment based on the foregoing.

Section 29 (1) The minister shall inform the Commission and the Member States of the result of the coordinated national risk assessment at all times.

(2) The minister shall disclose a summary of the results of the coordinated national risk assessment as updated at all times, in a version which does not include any classified information.

(3) The bodies contributing to the preparation of the coordinated national risk assessment may – in a manner that also conforms to the provisions governing their international cooperation – provide information for the risk assessment prepared by the Member States of the European Union.

11. Reporting obligation

Section 30 (1) Executive officers, employees and assisting family members of the service provider shall promptly make a report in writing to the person specified in Section 31(1) (hereinafter referred to as: "report") of any arising data, fact or circumstance indicating

a) money laundering,

b) terrorist financing or

c) that a *res* originates from a punishable act

(hereinafter referred to as: "data, fact or circumstance constituting grounds for reporting").

(2) The report specified in Subsection (1) shall include

a) the data recorded by the service provider under Sections 7-14/A,

b) the detailed presentation of the data, fact or circumstance constituting grounds for reporting, and

c) the documents supporting the data, fact or circumstance constituting grounds for reporting (where available).

(3) The service provider's executive officers, employee or assisting family member shall inspect the arising of data, facts and circumstances indicating money laundering, terrorist financing and that a *res* originates from a punishable act also with respect to executed transactions, transactions to be executed and transactions initiated by the customer not executed, as well as in the case specified in Section 13(8).

Section 31 (1) The service provider shall designate – depending on the characteristics of the organisation, and in particular its size and number of management levels – one or two persons (hereinafter referred to as: "designated person"), who shall promptly forward any report received from the executive officer, employee or assisting family

member of the service provider to the financial intelligence unit. The designated person must be the service provider's executive officer, employee or assisting family member.

(2) The service provider shall inform the financial intelligence unit of the designated person's name, position, contact details and date of start of activity, as well as any change in the foregoing, within five business days.

(3) The designated person shall forward the report on behalf of the service provider to the financial intelligence unit via a protected electronic message, regarding the receipt of which the financial intelligence unit shall inform the service provider sending the report via an electronic message without delay.

Section 32 (1) Until the forwarding of the report specified in Section 31(1) in accordance with Section 31(3), the service provider shall not execute the transaction.

(2) If non-performance of the transaction in accordance with Subsection (1) is not possible or performance of the reporting prior to execution of the transaction would threaten the monitoring of the beneficiary, the designated person shall forward the report on behalf of the service provider in accordance with Section 31(3) after execution of the transaction.

Section 33 (1) In regards to the service provider's executive officer, employee and assisting family member – including the designated person – (hereinafter collectively referred to as: "reporting person"), the central contact point and the service provider, if the foregoing acted in good faith, making the report shall not qualify as a violation of any restriction posed by any law or contract in regards to data disclosure, and shall not result in civil law or criminal liability even if the report subsequently proves to be unfounded.

(2) Any measure adverse to the reporting person – including the service provider's employees and representatives – that was adopted in consequence of a report made based on the internal rule or to the financial intelligence unit on the ground of alleged money laundering or terrorist financing shall be deemed as illegal, thus in particular the employer's measures which are adverse to or discriminative towards the employees.

(3) The reporting person – including the service provider's employees and representatives – may raise a complaint to or submit an appeal against the measure specified in Subsection (2) adversely affecting him or her.

Section 34 (1) The service provider shall suspend execution of the transaction if any data, fact or circumstance constituting grounds for reporting arises in relation to such a transaction, for the investigation of which the service provider deems that immediate measures by the financial intelligence unit are required. In this case, the service provider shall promptly make a report to the financial intelligence unit in order for it to be able to check the well-foundedness thereof.

(2) The service provider may suspend the transaction specified in Subsection (1) also by suspending all transactions concerning the service engaged by the customer decreasing the customer's wealth. In this case, the service provider shall call the financial intelligence unit's attention to this in its report specified in Subsection (1).

(3) Upon the request of the authority specified in Section 48(1) instructing the financial intelligence unit thereto, the financial intelligence unit may obligate the service provider in writing – referring to crime prevention, crime detection and investigation purposes – to execute the transactions specified by the financial intelligence unit during the term of the suspension.

(4) The service provider shall execute the suspended transaction if the financial intelligence unit notifies it in accordance with Section 35(4)(b) or if after the suspension, the term specified in Section 35(2) and (3) passed without notification from the financial intelligence unit.

(5) In regards to suspending the transaction, the service provider shall comply with those set out in the guide issued by the supervisory body specified in Section 5.

Section 35 (1) The service provider shall suspend execution of the transaction in accordance with the financial intelligence unit's instruction if the financial intelligence unit notifies the service provider in writing regarding a fact, data or circumstance constituting grounds for reporting in connection with the transaction or the service provider's customer.

(2) The financial intelligence unit shall inspect the data, fact or circumstance that is the basis of the report and the necessity of the information forwarding specified in Section 48(1) within four business days as of the reporting specified in Section 34 and the notification specified in Subsection (1).

(3) The financial intelligence unit shall be entitled to extend its inspection specified in Subsection (2) for a further three business days if this is necessary for the information forwarding specified in Section 48(1).

(4) The financial intelligence unit shall notify the service provider within the deadline specified in Subsection (2) if

a) it extends the term of the inspection pursuant to Subsection (3),

b) the transaction can be performed prior to the completion of the financial intelligence unit's inspection.

Section 36 The service provider and the financial intelligence unit shall – provided it acted in good faith – not have any civil law or criminal liability for suspending execution of the transactions in accordance with Sections 34(1) or 35(1) even if they can be executed later pursuant to Section 34(4).

Section 37 (1) If the supervisory body specified in Section 5 becomes aware in the course of its supervisory activity of any data, fact or circumstance constituting grounds for reporting, it shall promptly inform the financial intelligence unit thereof.

(2) If the customs authority becomes aware in the course of the monitoring of the traffic of goods and persons at the customs border of any data, fact or circumstance constituting grounds for reporting, it shall promptly inform the financial intelligence unit thereof.

12. The financial intelligence unit

Section 38 (1) The financial intelligence unit shall conduct an analysing-evaluating activity in order to promote the combating of money laundering and terrorist financing, as well as the prevention, detection and investigation of crimes, in the course of which it conducts operative and strategic analysis.

(2) The financial intelligence unit shall operate within the organisation of the National Tax and Customs Administration (Nemzeti Adó- és Vámhivatal), but independently in its scope of duties specified in this Act.

Section 39 In the event a fact, data or circumstance constituting grounds for reporting arises, the financial intelligence unit shall perform an operative analysis in order to perform the information forwarding specified in Sections 48(1) and 49(1). The financial intelligence unit shall, in the course of its operative analysis:

a) compare the information received in accordance with Section 40 with the data managed for the purpose of the analysing-evaluating activity – considering the risks specified in the national risk assessment –, and perform an automated risk assessment;

b) compare the information it became aware of pursuant to Act XLVIII of 2007 Implementing Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community (hereinafter referred to as: "Cash Control Act"), the data of databases it has direct access to, public data, data accessible to anyone and the data that can be obtained pursuant to this Act, and shall identify and interpret the connections between them;

c) monitor the financial transactions and processes related to the data specified in Paragraph *a)*, and shall inspect the business relationships and transaction orders;

d) decide regarding the necessity of performance of those set out in Sections 34(3), 35(4), 42-44 and 46;

e) decide on the measures applicable in the scope of the international exchange of information and cooperation specified in Section 49;

f) makes declarations and draws conclusions for the purpose of the forwarding of information specified in Section 48(1).

Section 40 The operative analysis shall be initiated based on

a) the service provider's report;

b) the service provider's report related to the suspension of the transaction specified in Section 34(1);

c) the information of the supervisory body specified in Section 5 or of the customs authority specified in Section 37(2);

d) the request for the disclosure of the information specified in Section 48(4) by the authorities specified in Section 48(1);

e) the information forwarded by the customs authority pursuant to Section 4(3) of the Cash Control Act;

f) the data request of or information made in relation to a data, fact or circumstance constituting grounds for reporting by the body responsible for implementing financial and asset-related restrictive measures specified in the Act on the Implementation of Financial and Asset-related Restrictive Measures Ordered by the European Union and the UN Security Council or the body responsible for implementing restrictive measures relating to transfer of funds;

g) the various forms of international exchange of information and cooperation with the foreign financial intelligence unit specified in Section 49(1).

Section 41 (1) In the course of its strategic analysis, the financial intelligence unit shall examine the processes and characteristics related to money laundering and terrorist financing.

(2) The financial intelligence unit may inform the bodies specified in Section 48(1) regarding the result of the strategic analysis and the supervisory bodies specified in Section 5, provided that the body is entitled to disclose the data pursuant to law, and this is necessary for it to exercise its powers and fulfil its duties.

Section 42 (1) In the scope of its analysing-evaluating activity, the financial intelligence unit shall be entitled to learn and process – to the extent necessary for fulfilling its duties – any data processed by the service provider, including payment, insurance, bank, securities, fund and occupational pension secrets and business secrets.

(2) In the scope of its analysing-evaluating activity, the financial intelligence unit may, to the extent necessary for fulfilling its duties, request the service provider to disclose to it the data and secrets specified in Subsection (1), in which case the service provider shall send the data and/or secrets specified in the request to the financial intelligence unit.

(3) The service provider shall ensure that the request of the financial intelligence unit be performed fully, quickly and via secure channels.

Section 43 (1) In the scope of its analysing-evaluating activity, the financial intelligence unit shall, to the extent necessary for fulfilling its duties, be entitled to learn and process data processed by a central administrative body, a court or the supervisory body specified in Section 5, including data qualifying as tax secret or customs secret.

(2) The central administrative body, the court or the supervisory body specified in Section 5 shall make available to the financial intelligence unit the data and/or secret specified in Subsection (1) requested in the scope of the analysing-operative activity of the financial intelligence unit.

Section 44 (1) In the scope of its analysing-evaluating activity, the financial intelligence unit shall, to the extent necessary for fulfilling its duties, be entitled to learn and process data processed by investigative authorities, the prosecutor, the national security services, the internal affairs division that investigates professional misconduct and criminal acts as defined by the Act on the Police, and to anti-terrorist organisations.

(2) In the scope of its analysing-evaluating activity, the financial intelligence unit may request the bodies specified in Subsection (1) to disclose data to it, which request this body shall not refuse except for the case specified in Subsection (4).

(3) In addition to requesting the data service specified in Subsection (2), in the scope of its analysing-evaluating activity, the financial intelligence unit shall, to the extent necessary for fulfilling its duties, obtain data from the database of the investigative body with direct access. Direct access shall be provided by the investigative authority.

(4) The head of the body requested in accordance with Subsection (2) may refuse the data service or exclude the direct access provided pursuant to Subsection (3) if:

a) the data service or the provision of direct access

aa) would be harmful in relation to an investigation, information interception or data interception;

ab) would harm national security;

b) the data disclosure would be in breach of an international convention;

c) in regards to data originating from a foreign secret service, the foreign secret service providing the data does not consent to the data disclosure; or

d) a Member State participating in a joint investigation team or crime detection team does not consent to the data disclosure.

(5) The head of the body requested pursuant to Subsection (2) may

a) prohibit;

b) restrict;

c) make subject to its prior consent the forwarding of the disclosed data to the bodies specified in Sections 48(1) and 49(1).

Section 45 (1) The deadline set by the financial intelligence unit for providing the data specified in Sections 42, 43 and 44(2) shall be eight days at minimum and thirty days at maximum. The requested body shall perform the data service or communicate the factors obstructing of the performance thereof within the deadline provided.

(2) The financial intelligence unit shall, in justified cases, be entitled to set shorter deadlines than those specified in Subsection (1) for the data services specified in Sections 42, 43 and 44(2) during the term of the suspension specified in Section 34(1) and 35(1).

(3) The financial intelligence unit shall indicate in the request specified in Sections 42, 43 and 44(2) the exact purpose of the data processing and the scope of data requested.

(4) If the request of the financial intelligence unit relates to the disclosure of personal data, it may relate only to such an amount and type of personal data that is absolutely necessary for the purpose of the request.

Section 46 (1) In the scope of its operative analysis, the financial intelligence unit may make a proposal for the performance of a procedure falling into the competence of a central administrative body, sending the data necessary for initiating and conducting the procedure that may be processed by the body conducting the procedure. The central administrative body requested to conduct the procedure shall promptly inform the financial intelligence unit regarding the outcome of utilisation of the information and – provided that the proposed procedure was performed –, after the final and binding completion of the procedure, the result of the procedure.

(2) In the scope of its operative analysis, the financial intelligence unit may send information, sending the data required for conducting the procedure falling into the competence of the supervisory body specified in Section 5 or the company registry court that may be processed by the body conducting the procedure.

(3) The supervisory body specified in Section 5 or the company registry court shall inform the financial intelligence unit regarding the outcome of utilisation of the data sent in the scope of the information by 31 March of the year after the year concerned.

Section 47 (1) The financial intelligence unit may use the data or secret it becomes aware of pursuant to Sections 42-44 and 75(1)-(2) only for the purpose of conducting its strategic analysis activity specified in Section 41(1) and for the purposes specified in Sections 48(1) and 49(1), in order for the performance of the operative analysis specified in Section 39.

(2) The financial intelligence unit may use the data or secret it becomes aware of pursuant to Section 46 only for the purposes specified in Sections 48(1) and 49(1), in order for the performance of the operative analysis specified in Section 39.

Section 48 (1) The financial intelligence unit may forward the results of its operative analysis – only for the purpose of combating money laundering and terrorist financing, as well as for the prevention, detection and investigation of crimes – to:

a) investigative authorities;

b) prosecutors;

c) courts;

d) national security services;

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

(2) The financial intelligence unit shall be entitled to provide data to the body responsible for implementing restrictive measures relating to transfer of funds in order for the performance of its tasks set out in the Act on the Implementation of Financial and Asset-related Restrictive Measures Ordered by the European Union and the UN Security Council.

(3) The financial intelligence unit shall keep records of data forwarding for the purpose of verifying the lawfulness of data forwarding and informing the data subject, which contain the date and time of forwarding of data processed, the ground and addressee of data forwarding, the scope of personal data forwarded, as well as other data specified in the law prescribing such processing. The financial intelligence unit shall retain the data recorded in the records of data forwarding for a period of twenty years from the date of forwarding of the data.

(4) The authorities specified in Subsection (1) may, for the purpose of fulfilling their tasks set out in law, send requests – indicating the purpose thereof – from the data processing system of the financial intelligence unit, to the extent necessary for the performance of their tasks.

(5) The bodies specified in Subsections (1) and (2) shall send feedback to the financial intelligence unit regarding utilisation of the results of the operative analysis and the manner of concluding the procedure conducted based on the results mentioned above, as well as the name of the underlying criminally punishable act (where applicable).

(6) The financial intelligence unit may, in order to ensure those set out in Section 53(1),

a) prohibit;

b) restrict;

c) make subject to its prior consent the use of data it became aware of under Section 49(1) and forwarded under Subsection (1).

(7) For the purpose of its analysing-evaluating activity specified in Section 38 and data forwarding under Section 48(1), the financial intelligence unit shall be entitled to enter into cooperation agreements with supervisory bodies specified in Section 5 and authorities specified in Section 48(1).

Section 49 (1) The financial intelligence unit shall be entitled to independently engage in international exchange of information and cooperation with foreign financial intelligence units and – in accordance with the provisions of the Act on the International Cooperation Between Law Enforcement Bodies – Europol for the purpose of combating money laundering and terrorist financing, as well as for the prevention, detection and investigation of crimes.

(2) The international exchange of information and cooperation specified in Subsection (1) shall cover the cases where legal classification of the underlying alleged criminally punishable act related to money laundering is not known at the time of the exchange of information.

(3) The financial intelligence unit shall use secure electronic channels – in conformity with the guidelines of the Financial Action Task Force and the Egmont Group – in the course of the international exchange of information and cooperation.

(4) The financial intelligence unit shall take into consideration the recommendations of the Financial Action Task Force and the guidelines of the Egmont Group in the course of the international exchange of information and cooperation.

(5) The financial intelligence unit shall be entitled to enter into a cooperation agreement with a foreign financial intelligence unit if the latter facilitates performance of the exchange of information and the cooperation in accordance with Subsection (1).

(6) The financial intelligence unit shall appoint a contact person in charge of receiving data requests from the foreign financial intelligence units.

Section 50 (1) In the scope of its analysing-evaluating activity, the financial intelligence unit may send a request to foreign financial intelligence units and Europol in accordance with Section 49.

(2) The request shall include all facts, information relevant in regards to combating money laundering and terrorist financing – relating to the natural or legal person or organisation without legal personality connected thereto – that are absolutely necessary for the activity of the foreign financial intelligence unit and for successfully responding to the request. The request shall indicate the reason thereof, as well as the manner of utilisation of the requested information.

(3) If the financial intelligence intends to send a request as per Section 42 to a service provider who provides services in Hungary but is not established and has no place of business and branch in Hungary, the financial intelligence unit shall send the request to the financial intelligence unit of the Member State where the service provider is established or has a place of business or branch.

Section 51 (1) In the scope of its analysing-evaluating activity, the financial intelligence unit may send information to foreign financial intelligence units and Europol in accordance with Section 49.

(2) The information shall include the data specified in Section 50(2) appropriately. The information shall indicate the reason thereof, as well as the manner of utilisation of the forwarded information.

(3) If the financial intelligence unit receives – pursuant to this Act or the Cash Control Act – a report or information concerning another Member State of the European Union, the financial intelligence unit shall promptly inform the financial intelligence unit of the Member State concerned.

Section 52 (1) The financial intelligence unit may forward the information obtained in the scope of international exchange of information and cooperation under this Act or the Act on Implementing 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 to the foreign financial intelligence unit and Europol, irrespective of the type of the underlying crime.

(2) The financial intelligence unit shall refuse to reply to the foreign financial intelligence unit's request for exchange of information and the related information provision where

a) the performance thereof would harm Hungary's fundamental national security and law enforcement interests;

b) the performance thereof would be in breach of the Hungarian laws;

c) the information can be disclosed only with the consent of the holder thereof, and no such consent has been given,

d) the information can be disclosed only with the consent of the foreign financial intelligence unit or Europol, and no such consent has been given.

(3) The financial intelligence unit shall not be entitled to refuse the international exchange of information or cooperation on the grounds that

a) the legal rules governing the taxation aspects of money laundering and the corresponding underlying crimes in the law of another Member State of the European Union or in a third country differ from the law of Hungary;

b) the national law prescribes a confidentiality obligation or an obligation to keep the data confidential for the service providers, save the cases specified in Section 73(3) and (4);

c) an inspection or a criminal procedure is ongoing in the case concerned by the request, except if the international exchange of information or cooperation would hinder the mentioned inspection or criminal procedure;

d) the nature or legal status of the contacting competent authority with similar competence differs from that of the contacted competent authority.

(4) The financial intelligence unit may restrict or make subject to requirements the utilisation of the information forwarded by it to a foreign financial intelligence unit. The restriction shall not be based on the fact that the legal rules governing the taxation aspects of money laundering or the corresponding underlying crimes in the law of the country of the foreign intelligence unit differ from the law of Hungary.

(5) The financial intelligence unit shall promptly give its broadest possible consent to the forwarding of the sent information to the foreign competent authorities by the foreign financial intelligence unit, irrespective of the type of the underlying crime. The financial intelligence unit may refuse to give its consent only where

a) it is outside the scope of application of this Act;

b) it would endanger the successful conduct of the investigation;

c) it may be given only with the consent of the foreign financial intelligence unit, and no such consent has been given;

d) the refusal specified in Subsection (2) would be possible but this was not known at the time of disclosure of the information;

e) it would severely harm a legitimate interest.

(6) The financial intelligence unit shall appropriately justify refusal of the consent.

Section 53 (1) The financial intelligence unit shall use the information obtained in the scope of the international exchange of information and cooperation solely for the purpose for which it previously requested and received it or for which the foreign financial intelligence unit disclosed it in its information. Any utilisation and information forwarding not previously approved shall be subject to the prior consent of the foreign financial intelligence unit sending the information.

(2) The financial intelligence unit may use the information obtained in the international exchange of information and cooperation only for the purposes set out in this Act.

(3) The financial intelligence unit may, in regards to the financial intelligence units of other Member States of the European Union, use a mechanism for the exchange of information that is different from the forms specified in Sections 50 and 51 but is in accordance with Section 49(4), provided that the purpose of such mechanism is to accelerate or prepare for the international exchange of information.

(4) Technologies providing for the complete protection and encryption of personal data and the comparison of personal data processed by the financial intelligence units of other Member States of the European Union in an encrypted manner shall qualify as usable technologies.

13. Prohibition of disclosure

Section 54 (1) The reporting person, the financial intelligence unit, the service provider requested pursuant to Sections 42(2) and 75(2), the authority requested pursuant to Section 43(2), the body responsible for implementing financial and property restricting measures and the body requested pursuant to Sections 44 and 46 shall not provide information to the customer or any third person or organisation regarding performance of the reporting or data service, the contents thereof, the analysing-evaluating activity, suspension of execution of the transaction as per Sections 34 and 35, the reporting person's identity or whether criminal proceedings have been initiated against the customer, and shall ensure that the reporting, the content thereof and the identity of the reporting person remain in secret.

(2) The prohibition set out in Subsection (1) shall not apply to the information provided by the reporting person to the supervisory body specified in Section 5, the service provider's request as per Sections 42(2) and 75(2), the request of the body specified in Sections 43(2), 44 and 46, the information specified in Section 41(2) and the information forwarding specified in Sections 48 and 49.

(3) The prohibition set out in Subsection (1) shall not apply to the disclosure of information taking place between Member State credit institutions and financial institutions belonging to the same group and between their branches and majority-owned subsidiaries established in third countries, provided that such branches and majority-owned subsidiaries are in full compliance with the group-level policies and procedures specified in Section 62 – including the procedures governing the sharing of information within the group –, and that the group-level policies and procedures comply with the requirements provided in this Act.

(4) The prohibition set out in Subsection (1) shall not apply to disclosure of information between the service providers Specified in Section 1(1)(g), (h) and (l) located in a Member State or a third country where requirements equivalent to those set out in this Act apply, when the persons concerned conduct their professional activity within the same legal person or network.

(5) In regards to the service provider specified in Section 1(1)(a)-(e), (g), (h) and (l), the prohibition specified in Subsection (1) shall not apply to the disclosure of information between the two or more concerned service providers, provided that

a) the information relate to the same customer and the same transaction concerning two or more obliged service providers,

b) at least one of the two or more concerned service providers conduct an activity that falls under the scope of this Act, and the other service providers are residents of a Member State or a third country where requirements equivalent to those set out in this Act apply,

c) the concerned service providers conduct the same activity specified in the Paragraphs of Section 1(1), and

d) in regards to professional confidentiality and the protection of personal data, requirements equivalent to those applicable in Hungary apply to the service providers.

(6) In regards to the service provider specified in Section 1(1)(g)-(h) and (l), the prohibition specified in Subsection (1) shall not apply to the provision of information to the customer that the transaction to be executed or already executed by the customer results in the violation of legal provisions.

Section 55 The scope of the restriction specified in Section 54 shall apply also to performance of the customer's access to his/her personal data recorded under Sections 7-11 and request for information regarding the processing of his/her personal data.

14. Data protection, records, statistics

Section 56 (1) The service provider's executive officer, assisting family member and employee participating in the performance of its task specified in this Act, solely for the purpose of its tasks to be performed for preventing and combating money laundering and terrorist financing and to the extent necessary thereto, learn and process the personal data – including information on the source of funds and wealth – he/she obtains in the course of performing the obligation specified in this Act and in the law based on the authorisation of this Act.

(2) The service provider shall be entitled to process the personal data it obtains in the course of performing the obligation specified in this Act and in the law based on the authorisation of this Act for eight years as of termination of the business relationship or execution of the transaction order.

Section 57 (1) The service provider shall retain in the records kept by it the data it obtains in the course of performing the obligation specified in this Act and in the law based on the authorisation of this Act not qualifying as personal data – including data obtained in the course of electronic identification and any other data generated in relation to the business relationship – for eight years as of termination of the business relationship or execution of the transaction order.

(2) The service provider shall retain in the records kept by it the instrument it obtains in the course of performing the obligation specified in this Act and in the law based on the authorisation of this Act, the copy thereof and the instrument it obtains in the course of electronic identification, the document certifying performance of the reporting and the data service specified in Section 42 or suspension of execution of the transaction as per Sections 34 and 35 and the copy thereof, as well as any other document created in relation to the business relationship and the copy thereof, for eight years as of termination of the business relationship or execution of the transaction order.

(3) The service provider specified in Section 1(1)(a)-(e) and (l) shall record in the records specified in Subsections (1) and (2) also the transaction orders executed in cash (HUF or domestic currency) with a value of HUF 4,500,000 or more, and shall retain such information for eight years.

(4) The service provider shall delete or destroy the data, instrument and copies thereof specified in Section 56 and Subsections (1)-(3) without delay after lapse of the retention period.

Section 58 (1) The service provider shall, by derogation from Sections 56(2) and 57(1)-(3), retain the data and instruments specified in the foregoing Sections upon the request of the supervisory body specified in Section 5, the financial intelligence unit, the investigative authority, the prosecutor or the court for the period specified in the request, but at maximum for ten years as of termination of the business relationship or execution of the transaction order.

(2) The data retention period may be extended based on the request specified in Subsection (1) only where the data or instrument specified therein is required for the purposes of a procedure in progress or to be initiated.

(3) The service provider shall delete the data or instrument from its records after the final and binding closing of the procedure or failure of the planned procedure specified in Subsection (2). The body specified in Subsection (1) shall promptly notify the service provider regarding final and binding closing of the procedure or failure of the planned procedure specified in Subsection (2).

(4) The financial intelligence unit and the supervisory body specified in Section 5 shall retain the data and instruments it becomes aware of under this Act for ten years as of becoming aware of or obtaining them.

Section 59 (1) The financial intelligence unit shall – in cooperation with the supervisory bodies specified in Section 5, the investigative authorities, the Prosecutor General's Office ("Legfőbb Ügyészség") and the National Judicial Office ("Országos Bírói Hivatal") – keep statistics allowing for monitoring of the effectiveness of the Hungarian system for combating money laundering and terrorist financing.

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

a) the number of reports;

b) pursuant to Sections 34 and 35, the number of suspended transactions, the number of successful suspensions and the amounts secured by currency;

c) the number of initiated attachments that may be ordered pursuant to the Act on the Implementation of Financial and Asset-related Restrictive Measures Ordered by the European Union and the UN Security Council and the number of attachments ordered by the court in relation to terrorist financing, as well as the value of the funds or economic resources in HUF and EUR;

d) the number of reports forwarded by the financial intelligence unit pursuant to Sections 48(1) and 49(1), as well as their proportion to all reports received by the financial intelligence unit;

e) the data relating to the number of requests and information sent by the financial intelligence unit to foreign financial intelligence units pursuant to Section 49 and the performance of the requests of foreign financial intelligence units, in breakdown by country;

f) the number of criminal proceedings launched on suspicion of antimoney laundering, terrorist acts under Section 261 of Act IV of 1978 and terrorist acts under Sections 314-316 of the Criminal Code, failure to report a terrorist act (Section 317 of the Criminal Code) and terrorist financing (Section 318 of the Criminal Code), by separately indicating the number of criminal proceedings initiated based on information forwarded by the financial intelligence unit and the number of criminal proceedings in which the information forwarded by the financial intelligence unit was utilised, as well as the name of the underlying criminally punishable acts and the manner of closing the proceedings;

g) in the criminal proceedings specified in Paragraph *f)*:

ga) the number of indictments and accused persons;

gb) the number of final and binding decisions and persons convicted in final and binding decisions;

h) the number of seizures imposed in the course of the criminal proceedings specified in Paragraph *f)*, the value of the seized object, the value of the seized property in HUF and EUR, the number of sequestrations and the value of the sequestrations in HUF and EUR, the number of confiscations, the value of the confiscated object, the value of the confiscated property in HUF and EUR, and the value of the property made subject to confiscation of property in HUF and EUR;

i) the data relating to the size and economic significance of sectors falling under the scope of this Act recorded by the supervisory bodies specified in Section 5;

j) the number of employees ensured for the supervisory body specified in Section 5 to conduct its supervisory activity under this Act, and for the financial intelligence unit to perform its duties specified in Sections 38-53;

k) the number of on-site and off-site inspections, the number of infringements identified as a result of supervisory procedures and the measures and administrative measures applied by the supervisory body specified in Section 5.

(3) The investigative authority shall send the data specified in Subsection (2)(f) and (h), the Prosecutor General's Office the data specified in Subsection (2)(f), (g)(ga) and (h), the National Judicial Office the data of final or already definitive court decisions relating to the number of attachments specified in Subsection (2)(c) ordered and the HUF value of attached funds or economic resources and the data specified in Subsection (2)(g)(gb), and the supervisory body specified in Section 5 the data specified in Subsection (2)(i)-(k) quarterly to the financial intelligence unit. The investigative authority, the Prosecutor General's Office, the National Judicial Office and the supervisory body specified in Section 5 may perform the data disclosure also by electronic means.

(4) The data specified in Paragraph *i)* of Subsection (2) shall be recorded in a breakdown by profession.

(5) The financial intelligence unit shall publish the comprehensive statistics compiled from the data available to it pursuant to Subsection (2) annually.

(6) Upon request of the Commission, the financial intelligence unit shall provide – via the minister – detailed information regarding the statistics specified in Subsection (2) annually.

(7) The financial intelligence unit shall inform the service providers, the supervisory bodies specified in Section 5 and the minister regarding the successfulness of the reports and its proposals facilitating the successfulness thereof regularly, but at least once a year.

Section 59/A The procedure applied and the records kept by the service provider shall ensure the fulfilment of requirements provided in this Act and in the law based on the authorisation of this Act, including consistency, the ability of continuous monitoring and verifiability.

15. Group-level policies, procedures and measures for branches and subsidiaries located in other Member States of the European Union or in third countries

Section 60 (1) The service provider belonging to the same group shall apply group-level policies and procedures.

(2) The group-level policies and procedures shall – for the purpose of comprehensively implementing group-level policies and procedures, efficient conduct of supervisory activity, as well as for preventing and combating money laundering and terrorist financing – cover, in particular

a) the intra-group sharing of data obtained in the course of performing the customer identification measures which either qualify as personal data or not – including data obtained during the electronic identification –, and the protection of data either qualifying as personal data or not, recorded by the service provider,

(2) the intra-group sharing of information relating to the performance of reports and the data service specified in Section 42, the contents thereof, the suspension of transactions as per Sections 34 and 35, the identity of the reporting person, and to any criminal proceedings in progress or subsequently initiated against the customer,

c) the ensuring of the appointment of the executive officer in Section 63(5)-(6),

d) the training specified in Section 64,

e) the determination of the external control function specified in Section 27(5), and

f) the preparation of the internal rule in accordance with the group-level risk assessment and the provisions of Section 65.

Section 61 (1) The service provider shall ensure that its branches, subsidiaries and places of business located in another Member State of the European Union also apply the provisions against money laundering and terrorist financing applicable in the given Member State.

(2) The service provider issuing electronic money and payment service provider having a place of business in Hungary but established in another Member State shall designate a Hungarian central contact point, which ensures that the service provider's operation is in compliance with regulations against money laundering and terrorist financing, and which facilitates the implementation of supervisory measures prescribed under Section 69, if any of the following conditions prevail:

a) the number of places of business in Hungary reaches at least 10;

b) the volume of electronic money distributed and redeemed by the places of business, or the aggregate value of payment transactions executed by them in a financial year is expected to exceed HUF 900,000,000, or exceeded HUF 900,000,000 in the preceding financial year, or

c) the information necessary for assessing whether the criteria provided in Paragraphs *a)* or *b)* were met are not made available to the Supervisory Body, upon request and in due time.

(3) In order to comply with criteria provided in Subsection (2), the central contact point shall be responsible for performing the reporting under Sections 30 and 32 and the data service under Section 42, the suspension of executing the transaction as specified in Sections 34 and 35, as well as for complying with the legal requirements applicable to reporting under Section of Act on the Implementation of Financial and Asset-related Restrictive Measures Ordered by the European Union and the UN Security Council.

(4) The service provider shall apply measures fitting the group-level policies and procedures specified in Section 60(2) also in its branches and subsidiaries located in other Member States of the European Union.

Section 62 (1) Where the service providers have branches, majority-owned subsidiaries or places of business in a third country which applies less strict minimum criteria for combating money laundering and terrorist financing compared to the requirements provided in this Act, the branches, majority-owned subsidiaries or places of business in the given third country shall implement the requirements prescribed in this Act, including, among others, those governing privacy, to the extent enabled by the law of the given third country.

(2) The service provider shall apply measures which comfort to the group-level policies and procedures specified in Section 60(2) also in its branches, subsidiaries and places of business located in third countries.

(3) If the legal regulations of the third country – in particular those governing confidentiality, privacy and the performance of data service – do not enable the application of measures comforting to those set out in Subsection (2), the service provider shall promptly notify the minister thereof through the supervisory body.

(4) The minister shall inform the Commission and the Member States of all cases where the legal regulations of a third country – in particular those governing confidentiality, privacy and the performance of data service – do not enable the application of measures comforting to those set out in Subsection (1).

(5) Where the legal regulations of a third country do not enable the application of measures comforting to those specified in Subsection (2), the service provider shall apply additional measures in its branches, subsidiaries or places of business located in the given third country – in accordance with Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries, developed by the European supervisory and adopted by the Commission –, and, where justified, the supervisory body specified in Section 5 may decide on the application of further supervisory measures.

16. Internal control and information system, training programme

Section 63 (1) In regards to its employees participating in its activity under this Act, the service provider shall provide for the following for the purpose of preventing any business relationship or transaction giving ground to or resulting in money laundering or terrorist financing:

operation of an internal control and information system which enables the anonymous reporting within the service provider, concerning the violation of

a) record-keeping obligation (customer due diligence),

b) the obligation to support effective reporting (screening), and

c) any obligation arising from this Act.

(2) The system specified in Subsection (1) shall ensure that the service provider is able to fully and quickly perform requests or data requests received from the financial intelligence unit, the supervisory body specified in Section 5 and the crime prevention and law enforcement bodies.

(3) The internal control and information system specified in Subsection (1)(c) shall also cover the operation of an internal system established – having regard for the service provider's type and size – for the performance of notifications that may be sent by the service provider's executive officer, employee and assisting family member in the case of the service provider's breach of the provisions of this Act, which system shall ensure anonymity.

(4) The supervisory body specified in Section 5 may issue a guide for the fulfilment of the obligation specified in Subsection (1) to the service providers under its supervision.

(5) The service provider shall designate within five business days as of the start of its activity – depending on the characteristics of the organisation, and in particular its size and the number of management levels – one or more executive officers specified in its internal rule, who shall be responsible for the fulfilment of the obligations arising from this Act by the service provider's employees.

(6) In regards to service providers specified in Section 1(1)(a)-(d), the executive officer specified in Subsection (5) shall possess appropriate knowledge for the performance of duties arising from this Act and the law based on the authorisation of this Act, as well as shall have an obligation to directly report to the body responsible for the management function. With regard to service providers specified in Section 1(1)(a), the executive officer specified in Subsection (5) may – in addition to its duties provided in Subsection (5) – perform solely such duties which relate to compliance with the law and security.

Section 64 (1) The service provider shall, in accordance with its identified risks, ensure that its employees participating in its activity specified in this Act familiarise themselves with the statutory provisions relating to preventing and combating money laundering and terrorist financing, that they recognise business relationships and transactions allowing for or constituting money laundering or terrorist financing, and that they are able to act in accordance with this Act in the event that data, facts or circumstances relating to money laundering or terrorist financing arise.

(2) The service provider shall ensure that its employees participating in its activity specified in this Act familiarise themselves with the international and Hungarian statutory provisions relating to the financial and asset-related restrictive measures ordered by the European Union and the UN Security Council and act in accordance with the obligations set out therein.

(3) In order to ensure fulfilment of the obligation specified in Subsection (1) and (2), the service provider specified in Section 1(1) shall ensure that its employees participating in its activity specified in this Act participate in training programmes.

(4) The supervisory body specified in Section 5 may issue a guide for the fulfilment of the obligation specified in Subsection (3) to the service providers under its supervision.

17. Internal rule

Section 65 (1) The service provider shall prepare an internal rule for the performance of tasks belonging in the scope of responsibilities specified in this Act.

(2) The supervisory body specified in Section 5 shall approve the internal rule if it is in conformity with the mandatory substantive elements specified in this Act and the Decree implementing it, provided that it is not in conflict with any law or the purpose of this Act.

(3) The supervisory body specified in Section 5 shall issue a mandatory guide to the service provider under its supervision for developing the internal rule.

(4) The service provider shall review and, if necessary, modify its internal rule within thirty days as of any change in the law, in the guide issued by the supervisory body specified in Section 5 or its internal order, including the internal risk assessment specified in Section 27.

(5) The supervisory body specified in Section 5 shall check the internal rule reviewed under Subsection (4) within the scope of its supervisory activity aimed at checking the service provider's compliance with the provisions of this Act – in accordance with the supervisory risk assessment –, and shall apply measures under this Act as appropriate in order to ensure that the internal rule complies with the laws and this Act.

(6) Persons trading in goods may commit to fulfil the obligations arising from this Act by submitting its internal rule to the trade licensing authority. The trade licensing authority shall register the service provider concurrently with approving the internal rule. Only registered persons trading in goods may accept cash payments with an amount of HUF 3,000,000 or more.

(7) The Office shall prepare a consolidated rule for trusts for the performance of the tasks falling under the scope of the duties specified in this Act, which rule shall qualify as the internal rule – as per this Section – of service providers engaged in trust activity. The Office shall review and modify as appropriate the consolidated rule upon any amendment of this Act or any change in the risk assessment specified in Section 27.

(8) Authorisation of the service provider specified in Section 1(1)(a)-(e) and (i) shall, in addition to the conditions specified in this Act, also be subject to that it submits for approval its internal rule to the supervisory body specified in Section 5, along with its application for the license.

(9) The service provider specified in Section 1(1)(f)-(h), (j) and (n)-(q) shall prepare and submit for approval to the supervisory body specified in Section 5 an internal rule within forty-five days as of it starting its activity.

(10) Service providers in operation at the time of entry into force of this Act shall prepare and submit for approval to the supervisory body specified in Section 5 an internal rule in connection with its activity falling under the scope of this Act within 45 days as of this Act's entry into force.

(11) The trade licensing authority shall register the service provider engaged in the trade of works of art, antiques concurrently with approving its internal rule.

18. Supervision, measures

Section 66 (1) The supervisory body specified in Section 5 shall ensure the service provider's compliance with the provisions of this Act by conducting its supervisory activity specified in this Act pursuant to the laws governing the supervisory body's activity and in accordance with Subsection (3).

(2) The supervisory body's supervisory activity specified in Section 5 shall also cover ensuring compliance with the international and Hungarian statutory provisions concerning financial and asset-related restrictive measures ordered by the European Union and the UN Security Council.

(3) In the course of its supervisory activity, the supervisory body specified in Section 5(e) and (f) of this Act shall act in accordance with the Act on the General Rules of Administrative Proceedings and Service – with the differences set out in this Act –, the supervisory body specified in Section 5(a) and (g) of this Act shall act in accordance with the Act on the General Rules of Administrative Proceedings and Service and the National Bank Act, the supervisory body specified in Section 5(b) of this Act shall act in accordance with the Act on the General Rules of Administrative Proceedings and Service and the Act on Organising Gambling, and the supervisory body specified in Section 5(c) of this Act shall act in accordance of the Act on the Hungarian Chamber of Auditors, Auditory Activities and Public Auditory Supervision and the Act on the General Rules of Administrative Proceedings and Service. In the course of their authority proceedings initiated based on the applications specified in this Act, the supervisory bodies specified in Section 5(e)-(g) shall not apply the provisions of the Act on the General Rules of Administrative Proceedings and Service relating to conditional decisions.

(4) During the performance of supervision, the supervisory body specified in Section 5(d)(da) shall proceed in accordance with Act LXXVIII of 2017 on Attorneys at Law (hereinafter referred to as: "Attorneys Act"), whereas the supervisory body specified in Section 5(d)(db) shall proceed in accordance with the provisions of the Notaries Public Act.

(5) The supervisory body specified in Section 5 shall send a written information to Commission along with the concurrent information of the minister of its contact details at all times and any change thereto.

Section 67 (1) During the performance of its supervisory activity, the supervisory body specified in Section 5 shall proceed according to the result of the supervisory risk assessment specified in Section 28 and shall adjust the frequency and scope of the supervisory procedure prescribed by this Act to the observed risks.

(2) The supervisory activity of the supervisory body specified in Section 66 and this Section also covers the controlling of the internal risk assessment and internal rules of procedure of the service provider prescribed by Section 27.

Section 68 (1) During the performance of its supervisory activity set out herein, the supervisory body specified in Section 5 shall ensure also that the Hungarian branches, subsidiaries and places of business of a service provider established in another Member State of the European Union comply with the provisions of this Act.

(1a) In regards to credit institutions and financial institution belonging to the same group, the supervisory body specified by Section 5 shall cooperate with the supervisory body of the Member State where the place of business of the given group is located.

(1b) The supervisory body specified in Section 5 shall supervise the effective implementation and conduct of the group-level policies and procedures with regard to Section 61(1).

(2) During its supervisory activity, the supervisory body specified in Section 5 may – with regard to the central contact point provided in Section 61(2), in exceptional cases, in particular in the event of a serious infringement that requires immediate remedy – apply the measures specified in Section 69 for a transitional period.

(3) During the implementation of the supervisory measure specified in Subsections (1) and (2), the supervisory body specified in Section 5 shall cooperate with the supervisory body of the other concerned state and the European supervisory bodies.

Section 69 (1) In the cases where the provisions of this Act are violated or the obligations set out herein are not duly performed, any other law issued based on the authorisation of this Act is violated, or where the provisions of the supervisory body's decision are violated or ignored, the supervisory body specified in Section 5(a-c) and (e-g) may apply the following measures proportional to the severity of infringement:

a) it notifies the service provider;

b) it orders the service provider to cease the infringement by setting a deadline;

c) it orders the service provider to review the internal rule in line with the requirements and until the deadline appointed by the supervisory body and to present the reviewed rule to the supervisory body;

d) in the case of service providers specified in Section (1)(1)(a)-(e), (g), (i) and (m) – with the restrictions set out by law – the supervisory body withdraws the issued activity or operating license or suspends it until cessation of the infringement;

e) in the case of service providers specified in Section 1(1)(j), (k) and (p)-(r), the supervisory body removes the service provider from the records, whereas in the case of service providers specified in Section 1(1)(f) and (h) it initiates the removal of such service provider from the records with the body keeping those records;

f) it initiates determination of the responsibility of the executive officer of service provider or the employee or assisting family member of the entity responsible for the infringement;

g) it initiates the suspension or withdrawal of the executive powers of the executive officer of the service provider until cessation of the infringement;

h) in addition to or independent of the measures listed above in Paragraphs *a)-g)* and *i)-l)*,

ha) in the case of service providers specified in Section 1(1)(a-c) and (e), it may impose a fine of an amount ranging from HUF 400,000 to 10% of the annual net sales revenue indicated in the annual financial statement or the annual consolidated financial statement accepted by the body authorised to approve the statement, or 10% of the revenue corresponding to the net sales revenue in line with the applicable accounting laws, but not exceeding HUF 2,000,000,000,

hb) in the case of service providers specified in Section 1(1)(d), it may impose a fine of an amount ranging from HUF 400,000 to 10% of the total amount of membership fees and supports of the year preceding the reporting year, but not exceeding HUF 2,000,000,000,

hc) in the case of service providers specified in Section 1(1)(f)-(k), (m) and (p)-(r), it may impose a fine of an amount ranging from HUF 100,000 to HUF 400,000,000;

i) in the case of service providers specified in Section 1(1)(a)-(e), it may appoint a supervisory commissioner;

j) it orders the service provider by setting a deadline to ensure the professional training of employees (executive officers), or to hire employees (executive officers) in possession of appropriate professional knowledge;

k) in the case of service providers specified in Section 1(1)(a)-(e), it may prescribe the performance of an extraordinary data service obligation;

l) in the case of service providers specified in Section 1(1)(a)-(e), it may

la) address a warning to the service provider's executive officer, employee or assisting family member,

lb) impose a fine on the service provider's executive officer ranging from HUF 100,000 to HUF 500,000,000 that shall not be undertaken by the service provider, whereas on the service provider's employee or assisting family member, ranging from HUF 20,000 to HUF 20,000,000 that shall not be undertaken the service provider either.

(2) In the course of its procedure, the supervisory body practicing supervision over the service providers specified in Section 1(1)(a)-(e) and (m) – in addition to the scope of cases provided in the National Bank Act – shall apply the measures listed in Subsection (1) – except for Paragraphs *h)* and *l)* – which it is entitled to take in the form of an order unappealable by means of an independent appeal as extraordinary measures as well, if this is urgently necessary for protecting the interest of society in the efficient enforcement of the prohibition of money laundering and terrorist financing.

(3) If the financial advantage resulting from the infringement can be determined in the case specified in Subsection 1(h)(hc) and double the amount thereof exceeds HUF 400,000,000, then the maximum amount of the imposable fine is double the amount of the financial advantage.

(4) When applying the measures, the supervisory body specified in Section 5(a-c) and (e-g) takes into account the following aspects:

a) the severity of the infringement,

b) the wilful or negligent conduct of the persons responsible for the infringement,

c) the market share of the infringing entity if relevant with regard to the given service provider category,

d) the impact of the infringement on the service provider or its customers,

e) the responsible persons' cooperation with the supervisory body,

f) the duration, recurrence and frequency of infringement.

(5) In addition to the measure specified in Subsection (1)(l), the measure provided in Subsection (1) shall be applied against the service provider even if the service provider qualifies as a legal person or an organisation without legal personality, and the executive officer of the service provider violates the provisions of this Act for the benefit of the service provider.

(6) In addition to the measure specified in Subsection 1(l), the measure provided in Subsection (1) shall be applied against the service provider even if the service provider qualifies as a legal person or an organisation without legal personality, and the employee or the assisting family member of the service provider violates the provisions of this Act for the benefit of the service provider, in a manner that the performance of the supervisory and controlling obligation of the executive officer of the service provider could have prevented the infringement.

(7) The fine imposed pursuant to Subsection 1(h) shall be paid within thirty days from the communication thereof. Upon the request of the service provider, the supervisory body may enable deferral or payment in instalments for the performance of payment obligation (hereinafter referred to as: "facilities for payment"). The service provider ordered to pay the fine may request the authorisation of facilities for payment in its application submitted within five days from the communication of the decision, if any reason beyond its control hinders the performance by deadline or would cause disproportionate difficulty for the service provider. Meeting the requirements must be reasonably proved with documents.

Section 70 During the performance of supervisory activity, the supervisory bodies specified in Section 5 closely cooperate with each other, the financial intelligence unit, the investigative authority, the prosecutor's office and the court and other supervisory bodies of the Member States or third countries.

Section 71 The supervisory body specified in Section 5(a)-(c) and (e)-(g) shall immediately disclose on its website the decisions which became definitive or those declared enforceable irrespective of appeals that were made in the supervisory procedure under this Act; the disclosed information shall include at least the nature of the violation of the rule or the deficiency and shall ensure that the data, information on the person of the infringing entity can be learned.

(2) The supervisory body specified in Section 5(a)-(c) and (e)-(g) may postpone the performance of the disclosure obligation provided in Subsection (1) until the reasons constituting grounds thereto prevail, if

a) disclosing the data and information on the infringing entity – also taking into account the severity of infringement – would cause disproportionate disadvantage for the concerned entity; or

b) disclosing such data and information would endanger the stable, uninterrupted operation of the service provider sector specified in Section 1(1)(a)-(e) or

c) endanger the performance of any ongoing or future procedure.

(3) The supervisory body specified in Section 5(a)-(c) and (e)-(g) may be exempted from the performance of the disclosure obligation provided in Subsection (1), if

a) postponement of the disclosure for the reasons set out in Subsection (2) is not sufficient; or

b) it would be disproportionate having regard to the severity of the infringement.

(4) Until the cessation of the reason specified in Subsection 2(a), the disclosure obligation may be performed also without disclosing any data or information on the person of the infringing entity, in a form ensuring anonymity if decided so by the supervisory body specified in Section 5(a)-(c) and (e)-(g).

(5) In the case of disclosing a decision declared enforceable irrespective of remedies as specified by Subsection (1), the supervisory body specified in Section 5(a)-(c) and (e)-(g) shall also disclose the information on the result of appeal – simultaneously with the decision's becoming final – on its website.

(6) The supervisory body specified in Section 5(a)-(c) and (e)-(g) shall ensure the availability of the information disclosed pursuant to Subsection (1) for five years from the disclosure thereof.

Section 72 (1) The executive officer, employee, assisting family member of the service provider and the customer of the service provider (hereinafter referred to as: "person submitting notification") may notify – by providing his/her name and residential address – the supervisory body specified in Section 5 of any circumstance regarding the violation of the provisions of this Act by the service provider (executive officer, employee or assisting family member of the service provider) (hereinafter referred to as: "notification").

(2) The supervisory body specified in Section 5 shall examine the notification and decide regarding the necessity of launching the supervisory procedure specified in this Act *ex officio*, the form of control and non-initiation of the supervisory procedure within thirty days from the receipt thereof. If the person submitting notification did not submit the notification to the supervisory body authorised to proceed, the supervisory body specified in Section 5 transfers the notification to the body having competence and jurisdiction for the conduct of procedure without delay.

(3) The supervisory body specified in Section 5 shall notify the person submitting the notification of

a) the decision taken under Subsection (2) without delay and

b) the transferring of the notification simultaneously with the transfer.

(4) The substantive examination of the notification may be omitted, if:

a) the same person submitted a notification identical to a previous one;

b) the person submitting the notification informed the supervisory body about the circumstance specified in Subsection (1) within six months from obtaining knowledge thereof;

c) the person submitting the notification did not verify his involvement as specified by Subsection (1);

d) the notification is clearly groundless;

e) the examination of the notification does not fall under the scope of this Act;

f) the supervisory body does not have competence and jurisdiction for the examination of the notification.

(5) The supervisory body specified in Section 5 omits the examination of the notification sent by an unidentifiable person, unless the notification is based on material infringement according to the information available.

(6) The person submitting the notification in good faith shall not suffer any disadvantage for submitting the notification.

(6a) Any adverse measure taken for the person submitting notification shall qualify as unlawful, thus in particular the employer's measures which are adverse to or discriminative towards the employees.

(6b) The person submitting notification may raise a complaint to or submit an appeal against the measure specified in Subsection (6a) adversely affecting him or her.

(7) The personal data of the person submitting the notification and the alleged infringing entity may be processed in order for the performance of the obligations set out in this Section only by the body having competence for conducting the supervisory procedure specified in this Act. The personal data of the data subject – without its written consent – shall not be transferred to third parties or disclosed to the public.

(8) The data related to the notification, the investigation conducted on the basis of the notification and the measures taken shall be retained for five years from the completion of the last investigative action or measure.

Section 18/A Professional confidentiality, cooperation between the Supervisory Body and other authorities

Section 72/A (1) Any person who is or was an employee of the Supervisory Body with respect to fulfilling the obligations under this Act shall keep any business secret, banking secrets, securities secret, payment secret or insurance secret it becomes aware of in the course of his/her work (hereinafter collectively referred to as for the purpose of this Section: "professional secret"). The persons acting on behalf of the Supervisory Body as non-employees shall be bound by a confidentiality obligation.

(2) The persons specified in Subsection (1) may disclose the professional secret obtained by them in the course of fulfilling their obligations under this Act solely in a summarised or aggregate form in a manner that the specific credit institutions and financial service providers remain unidentifiable.

(3) The confidentiality obligation concerning professional secrets shall not prevail in the course of a criminal procedure towards the Supervisory Body, the prosecutor's office, the investigative authority or the body conducting the preparatory procedure.

(4) Without prejudice to the provisions of Subsections (1) and (2), the Supervisory Body shall be entitled to exchange information with the supervisory bodies supervising credit institutions and financial service providers in other Member States of the European Union, including the European Central Bank.

(5) The Supervisory Body may use the professional secrets specified in Subsection (1) solely for the following purposes:

a) for the purpose of performing their duties under this Act and the laws governing the combating of money laundering and terrorist financing, prudential regulations and the supervision of credit institutions and financial service providers, also including the application of any such measures;

b) for the purpose of remedy procedure against the Supervisory Body's decision;

c) for the purpose of court procedures initiated for violating this Act and the EU laws governing the combating of money laundering and terrorist financing, prudential regulations and the supervision of credit institutions and financial service providers.

(6) In order to support the combating of money laundering and terrorist financing, the Supervisory Body shall conduct international exchange of information independently with the supervisory bodies supervising credit institutions and financial service providers in other Member States of the European Union, including the European Central Bank. Within the framework of this international cooperation and its own scope of competence, the Supervisory Body shall initiate an inspection on behalf of the contacting supervisory body, and shall hand over the information obtained in the course of the inspection to the contacting supervisory body with the conditions specified in Subsections (1)-(5).

(7) For the purpose of supporting the combating of money laundering and terrorist financing, the Supervisory Body shall be entitled to enter into a cooperation agreement with the supervisory body of a third country with a similar scope of competence, on a reciprocal basis. For the purpose of protecting professional secrets, the cooperation agreements shall include privacy provisions which at least provide an equivalent level of protection as those in Subsections (1)-(5). The information obtained under the cooperation agreements shall be used solely for the purposes provided in this Act.

19. Specific provisions applicable to attorneys, registered in-house legal counsels and notaries public

Section 73 (1) The attorney shall be subject to the customer due diligence and reporting obligations set out herein – with the exception specified in Subsection (3) – if he/she conducts an activity specified in Section 3(1)(i) of the Attorneys Act, or holds in custody cash and valuables, or conducts the attorney's activities specified in Section 2(1) of the Attorneys Act in relation to the preparation and execution of the following legal transactions:

a) transfer of ownership of assets (share) held in business associations or other business organisations,

b) transfer of ownership of real property,

c) foundation, operation, termination of business association or other business organisation,

d) unilateral legal statement on the establishment of trust agreements or trust activity,

e) transfer of movable property – in particular funds and financial instruments – without any compensation.

(1a) The registered in-house legal counsel shall subject to the customer due diligence and reporting obligations set out herein – with the exception specified in Subsection (1b) and (3) – if he/she conducts the attorney's activities specified in Section 2(1) of the Attorneys Act in relation to the preparation and execution of the following legal transactions:

a) transfer of ownership of assets (share) held in business associations or other business organisations,

b) transfer of ownership of real property,

c) foundation, operation, termination of business association or other business organisation,

d) unilateral legal statement on the establishment of trust agreements or trust activity.

(1b) The customer of the registered in-house legal counsel – as a service provider – shall fulfil the obligations binding the registered in-house legal counsel based on the attorney's activities conducted under this Act for his/her customer qualifying as a service provider under the same, in accordance with the rules applicable to service providers.

(1c) The attorney and the registered in-house legal counsel shall be bound by a customer due diligence under this Act, if the conditions provided in either Subsection (1) or in Subsection (1a) and Section 6(1) prevail together. In regards to registered in-house legal counsels, transaction order shall mean the conduct of activity for the customer not belonging under Subsection (1b).

(1d) The customer due diligence and reporting obligation of the attorney and the registered in-house legal counsel shall cover the persons entering into a contract with his/her customer and the customer's representatives, as well.

(2) The notary public is subject to the customer due diligence and reporting obligations set out herein – with the exception specified in Subsection (4) – if he/she performs trust custody or conducts any other non-contentious civil procedure specified in the Notaries Public Act in relation to the preparation and execution of the following legal transactions:

a) transfer of ownership of assets (share) held in business associations or other business organisations,

b) transfer of ownership of real property,

c) foundation, operation, termination of business association or other business organisation;

d) unilateral legal statement on the establishment of trust agreements or trust activity.

(3) The attorney and the registered in-house legal counsel are not subject to the reporting obligation set out herein and the obligation to respond specified in Section 75(3) regarding the inquiries from the financial intelligence unit, if

a) he/she obtained knowledge of the data, fact or circumstance which the report is based on during the preparation or performance or following the performance of defense in criminal proceedings or representation before court – with the exception of providing representation in proceedings before company registry courts –,

b) he/she obtained knowledge of the data, fact or circumstance which the report is based on during the provision of legal advice in relation to the representation or performance of defense specified in Paragraph (a) above or to the necessity of launching the procedure.

(4) The notary public is not subject to the reporting obligation set out herein and the obligation to respond specified in Section 75(3) regarding the inquiries from the financial intelligence unit, if

a) he/she obtained knowledge of the data, fact or circumstance which the report is based on during the provision of instructions for the parties in relation to the necessity of launching the procedure,

b) the notary public conducts a non-contentious procedure that falls outside the scope of non-contentious civil procedures regulated in the Notaries Public Act.

Section 74 (1) The attorney, the registered in-house legal counsel and the notary public shall perform the reports at the regional association/chamber. The employee of the attorney or notary public – also including the employed attorney – shall perform the reports at the attorney or notary public exercising the employer's rights. The attorney or notary public exercising the employer's rights shall forward the report to the regional association/chamber without delay. The employee of the law office shall submit the reports to the person designated by the assembly of members, who shall forward it without delay to the chamber having registered the concerned law office.

(1a) The junior in-house legal counsel shall make the report with the registered in-house legal counsel with whose direction he/she conducts the attorney's activity as specified in Section 73(1a). The registered in-house legal counsel shall forward the report to the regional association/chamber without delay.

(2) The president of the regional bar association/chamber of notaries public designates the person who forwards the reports received from the persons specified in Subsection (1) to the financial intelligence unit without delay. The regional bar association/chamber of notaries public shall provide information on the designated person and any change therein for the financial intelligence unit without delay.

(3) In the case of law offices, the assembly of members may decide whether the obligations specified in Sections 30(1), 63 and 64 shall be performed by the office or the members.

Section 75 (1) Within the scope of its analysing-evaluating activity, the financial intelligence unit – to the extent necessary for the performance of its tasks – shall be entitled to learn and process the data processed by the attorney, the registered in-house legal counsel and the notary public, as well as the privileged information obtained by the attorney or notary public.

(2) Within the scope of its analysing-evaluating activity, the financial intelligence unit may inquire at the attorney, the registered in-house legal counsel and the notary public regarding the data and privileged information specified in Subsection (1) above. The inquiry of the financial intelligence unit is sent through the designated person specified in Section 74(2), who forwards it to the contacted attorney, registered in-house legal counsel or notary public without delay.

(3) If the contacted attorney, registered in-house legal counsel or notary public processes the data and/or secrets indicated in the inquiry in the scope of the performance of the attorney or notary public activity specified in Section 73(1)-(2) or as a result of such activity, he/she shall send the data and/or secrets indicated in the inquiry to the designated person within the deadline specified in Section 45, who shall forward the reply to the financial intelligence unit without delay.

(4) Where the attorney, the registered in-house legal counsel or the notary public does not process the data and/or secrets indicated in the inquiry in the scope of the performance of the attorney or notary public activity specified in Section 73(1)-(2) or as a result of such activity or processes them so but a ground for exemption specified in Section

73(3)-(5) prevails, then the attorney, the registered in-house legal counsel or the notary public shall become entitled to refuse to reply. The attorney or the notary public shall notify the financial intelligence unit of the fact of refusing to reply in a manner specified in Subsection (3) without delay.

(5) The performance of the reporting obligation of the attorney, the registered in-house legal counsel or the notary public and the performance of the inquiry of the financial intelligence unit shall not qualify as a breach of the statutory confidentiality obligation.

(6) For the purposes of this Act, the notary public is not subject to the obligation specified in Section 3(2) of the Notaries Public Act.

Section 76 (1) With regard to

a) the supervisory rules of procedure, the supervisory risk assessment and the supervisory body's guide applicable by the regional bar associations,

b) minimum requirements of the audited electronic telecommunications equipment and its operation, the method of auditing this equipment, as well as the performance of customer due diligence by using this equipment, and

c) the performance of duties belonging to the scope of obligations under this Act in relation to the activity of individual attorneys, the single-member law office as specified in Section 73(1), and the activity of the registered in-house legal counsel as specified in Section 73(1a),

the Hungarian Bar Association prepares a uniform rule, which shall qualify as an internal rule and risk assessment as provided in Section 65 in relation to the activity of individual attorneys, the single-member law office as specified in Section 73(1), and the activity of the registered in-house legal counsel as specified in Section 73(1a).

(2)

(3) For the performance of the tasks falling under the scope of obligations set out in this Act, the Hungarian Chamber of Notaries Public prepares a guide for the notaries public; this guide qualifies as an internal rule as specified in Section 65 for notaries public.

(4) The Hungarian Bar Association shall revise and amend the rule specified in Subsections (1), whereas the Hungarian Chamber of Notaries Public shall revise and amend the guide specified in Subsection (3) if necessary following the amendments to this Act, as well as in the case when the risk assessment provided in Section 27 changes.

Section 76/A Based on the data service by the Hungarian Chamber of Auditors, the regional chambers of notaries public, the Hungarian Chamber of Notaries Public and based on the regional bar associations, the Hungarian Bar Association shall publish an annual report anonymously until the 30th day of June following the year concerned, which includes information regarding the following:

a) the measures adopted in connection with holding liable the service providers supervised by the Hungarian Chamber of Auditors, the regional chambers of notaries public and the regional bar associations on the ground of the material and/or recurrent and/or regular breach of the provisions of this Act;

b) the number of notifications on the potential or actual breaches of the provisions of this Act under Section 72(1);

c) the number of reports received by the Hungarian Chamber of Auditors, the regional chambers of notaries public and the regional bar associations, and the number of reports forwarded to the financial intelligence unit;

d) the number and description of measures which – under Sections 66-72 – were executed with a view to monitoring whether the obliged

service providers comply with their obligations specified in Sections 6-24, 30-37, 56-59 and 63-64.

Section 19/A Rules for registering specific service providers

Section 76/B (1) The registered office service provider shall report its intention to conduct such activity to the supervisory body specified in Section 5 (hereinafter referred to as for the purpose of this Subchapter: "supervisory body"); the activity may be continued after being reported.

(2) The registered office service provider shall report any change to the data provided upon registration and to the conditions of being registered – including the termination of its activity – within 15 business days to the supervisory body.

(3) The reports shall be made in writing.

Section 76/C (1) The person shall be excluded from the possibility to qualify as natural person registered office service provider

a) who was condemned until relieved from the detrimental consequences which are attached by law to any prior conviction, for committing any of the following crimes:

aa) under Act IV of 1978 on the Criminal Code (in effect until 30 June 2013): crimes against public justice (Title VII, Chapter XV), crimes against international justice (Title VIII, Chapter XV), terrorist act, violation of

international economic restrictions, seizure of aircraft, any means of railway, water or road transport or any means of freight transport, affiliation with organised crime, taking the law into one's own hands, forgery of public documents, misuse of a document, economic crimes (Chapter XVII), crimes against property (Chapter XVIII),

ab) under Act C of 2012 on the Criminal Code: crimes of corruption (Chapter XXVII), terrorist act, terrorist financing, seizure of a vehicle, affiliation with organised crime, violation of international economic restrictions, forgery of public documents, use of a forged private document, misuse of a document, crimes under Chapter XXXV-XLIII, or

b) who fails to meet the conditions specified in the decree on the provision of registered office service.

(2) A legal person or an organisation without legal personality may not conduct registered office service activities, if

a) a ground for exclusion specified in Subsection (1) prevails against any of its executive officers, natural person members or beneficial owners (hereinafter collectively referred to as for the purpose of this Subchapter: "persons concerned"), or

b) it fails to meet the conditions specified in the decree on the provision of registered office service.

(3) The report shall include the following data of the registered office service provider

a) if a legal person or an organisation without legal personality:

aa) name,

ab) registered office,

ac) company registration number or registration number,

ad) official contact details;

b) if a natural person:

ba) name, name at birth,

bb) mother's name,

bc) residential address,

bd) place and date of birth.

(4) The following shall be attached to the report:

a) the internal rule as specified herein and in Act on the Implementation of Financial and Asset-related Restrictive Measures Ordered by the European Union and the UN Security Council,

b) with regard to Subsection (1)(a) or Subsection (2)(a), the certificate of clean criminal record of the persons concerned, not older than 30 days, and

c) the documents which prove compliance with the requirements provided in the decree on the provision of registered office service.

Section 76/D The records shall contain:

a) the data listed in Section 76/C(3),

b) the date of reporting and the date of registration,

c) the fact, ground and date of removal from the records,

d) the circumstances relating to the examination of the conditions of registration.

Section 76/E (1) Where it can established based on the report that the registered office service provider meets the conditions, and the report contains the data, certificates required under Section 76/C(3) and (4), the supervisory body shall register the registered office service provider.

(2) The supervisory body has a 60-day period to perform its administrative duties.

(3) The supervisory body may examine annually whether the conditions of registration still prevail for the registered office service providers kept in the records. In order for the successful conduct of the examination, the registered office service provider kept in the records shall prove in writing until 31 December of the year concerned that the conditions provided in the decree on the provision of registered office service are met. The supervisory body shall examine whether a data giving ground for exclusion under Section 76/C(1)(a) or (2)(a) arises with regard to a natural person registered office service provider, the executive officer, natural person member or beneficial owner of a legal person or an organisation without legal personality by means of a data request as specified in Section 71(2) of Act XLVII of 2009 on the criminal database, the registration of verdicts brought against Hungarian nationals in the courts of European Union Member States and the registration of criminal and biometric data (hereinafter referred to as: "Criminal Records Act") by providing the data specified in Section 69(2) of the Criminal Records Act.

(4) If the supervisory body finds that the conditions of registration are not met, it shall call the registered office service provider to eliminate the obstacle and certify this in writing within 30 days from the receipt of the notification. Following the unsuccessful lapse of the deadline, the supervisory body shall remove the registered office service provider from the records, and shall notify the national tax and customs administration.

(5) The national tax and customs administration shall examine the scope of taxpayers for whom the given registered office service provider performs registered office service, and shall call the taxpayer(s) concerned to ensure a regular registered office.

20. Closing Provisions

Section 77 (1) The minister is authorised to determine the mandatory substantive elements of the internal rule and the declaration on the source of wealth in the form of a decree.

(2) The minister is authorised to determine in a decree the detailed rules governing the following for the service providers specified in Section 1(1)(f), (h)-(k) and (n)-(r):

a) set of regulations applicable to the preparation of the internal risk assessment,

b) operating the internal control and information system,

c) cases of simplified and enhanced customer due diligence and the related rules of supervisory approval,

d) minimum requirements of the audited electronic telecommunications equipment and its operation, the method of auditing this equipment, as well as the performance of customer due diligence by using this equipment,

e) cases and set of requirements of the enhanced procedure,

f) specification of cases requiring managerial decision for the establishment of business relationships based on a risk sensitivity approach and the execution of transaction orders,

g) training programme,

h) suspension of transactions.

(3) The president of the MNB is authorised to determine the detailed rules governing the following for the service providers specified in Section 1(1)(a)-(e) and (m) in the form of a decree:

a) set of regulations applicable to the preparation of the internal risk assessment,

b) operating the internal control and information system,

c) cases of simplified and enhanced customer due diligence and the related rules of supervisory approval,

d) minimum requirements of the audited electronic telecommunications equipment and its operation, the method of auditing this equipment, as well as the performance of customer due diligence by using this equipment,

e) cases and set of requirements of the enhanced procedure,

f) specification of cases requiring managerial decision for the establishment of business relationships based on a risk sensitivity approach and the execution of transaction orders,

g) training programme,

h) suspension of transactions.

(4) The Government is authorised to adopt decrees in order to

a) determine the detailed rules for the operation of the central records created for storing the data of beneficial owners, and of the central records of bank accounts and safes,

b) designate the bodies responsible for operating the database and records specified in Paragraph *a)*.

Section 78 (1) This Act – with the exception provided in Subsection (2) – enters into force on 26 June 2017.

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

(3) Section 3(28)(m) enters into force on 3 January 2018.

Section 79

Section 80 (1) The service provider operating upon the entry into force of Act CXIX of 2019 on the Amendment of Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing and Certain Related Acts (hereinafter referred to as: "Amending Act") shall modify its internal rule in accordance with the provisions provided by the Amending Act within 90 days from the entry into force of the same.

(2) Regarding the individual attorneys and single-member law offices and the notaries public, the Hungarian Bar Association and the Hungarian Chamber of Notaries Public shall modify the internal rule as specified herein within sixty days from the entry into force of the Amending Act.

(3) The Hungarian Bar Association shall modify the rule specifying the content of the guide to be issued by the regional bar association within thirty days from the entry into force of the Amending Act

(4) The Office shall modify the uniform rule specified in this Act for the trusts within sixty days from the entry into force of this Amending Act.

(5) The service provider operating upon the entry into force of the Amending Act shall comply with the data service obligation under Section 25(1) of the Anti Money Laundering Act by not later than 1 March 2021.

(6) With regard to the payment accounts active and the safe service contracts in effect upon the entry into force of the Amending Act, the data service obligation under Sections 25/A and 25/B shall be complied with by not later than 21 March 2021.

(7) The service provider shall eliminate the restrictive measure enforced under Section 12(5) in force until the day preceding the entry into force of the Amending Act, if the customer fulfils its obligation to disclose the identification data.

Section 81 If the service provider informed the authority operating as financial intelligence unit about a person designated according to Section 23(3) of Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter referred to as: "Act CXXXVI of 2007"), the service provider shall provide information as prescribed by Section 31(2) in the case of any change in the designated person or his data specified in Section 31(2). In this case the tasks of the designated person shall be performed by the person designated under Section 23(3) of Act CXXXVI of 2007 until a change occurs in the designated person.

21. Conformity with the legislation of the European Union

Section 82 (1) This Act serves for establishing conformity with

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

b) Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU

.

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

22. Amending provisions

Sections 83-92
Sections 93-94
Section 95