REGISTRATION OF THE ACTIVITY
OF ENTERPRISES PROVIDING SOLELY ACCOUNT INFORMATION SERVICES

Pursuant to the provisions in sub-paragraph aa) of paragraph a) and paragraph b) of Section 9 (1) of Act CCXXII of 2015 on the general rules of trust services and electronic transactions, Sections 17 (1) and 19 (1) of Government Decree 451/2016. (XII. 19.) on the detailed rules of electronic services, and Section 3 (1) of MNB Decree 36/2017. (XII. 27.) on the rules of electronic communication in official matters in progress before the Magyar Nemzeti Bank ("Decree"), on grounds of Section 58 (2) of Act CXXXIX of 2013 on the Magyar Nemzeti Bank ("**MNB Act**"), the legal representative of an **economic operator or an applicant (client)** obliged to apply electronic communication must submit his application, notification or other petition by using the prescribed form available in the information system ensuring the electronic transactions of the Magyar Nemzeti Bank (**MNB**) ("ERA System") and introduced for the procedure related to the petition in question, in the manner and with content specified therein, simultaneously uploading the attachments specified by the law and other documents required by the MNB.

In the licensing procedures, the applications and notifications must be submitted by using the prescribed electronic form available in the *E-administration / Licensing* service on the ERA interface available on the MNB's website, attaching the certified electronic copies of the appendices. The resolutions, requests for clarification, notices and other communications of the MNB are delivered to the financial institutions or their legal representatives by sending them to the delivery storage space.

The website of the MNB contains information materials on electronic transactions and the submission of appendices to be attached in licensing procedures (electronic documents):
https://www.mnb.hu/letoltes/tajekoztatas-az-e-ugyintezesrol-az-mnb-elotti-engedelyezesi-eljarasokban-1.pdf

Further information related to certain aspects of the licensing procedures is available under the following menu item: https://www.mnb.hu/letoltes/tajekoztato-az-egyes-engedelyezesi-illetve-nyilvantartasba-veteli-eljarasok-soran-leggyakrabban-felmerulo-a-ma-gyar-nemzeti-bank-mnb-gyakorlatat-erinto-kerdesekkel-kapcsolatban-1.pdf

In addition to the provisions stipulated in *Act CXXXV of 2013 on Certain Payment Providers* (**Payment Service Providers Act**), the licensing guide also contains the provisions included in the guidelines issued by the European Banking Authority (**EBA**) entitled *"Guidelines, based on Article 5 (5) of Directive 2015/2366/EU, on the information to be provided for the licensing of payment institutions and e-money institutions and for the registration of the services consolidating account information"* (**Guidelines**), and the MNB – integrating it in its supervisory practice – expects the institutions to comply with those during its proceeding.

I. GENERAL RULES

Payment institution is an enterprise that holds a licence, as prescribed by the law, to provide payment services – including also the enterprises that of the payment services provide solely account information services (based on prior registration) – ,but it is not licensed to issue e-money. *(Section 5 (1a) of the Payment Service Providers Act)*

1.1. Organisational rules

Payment institutions may operate as joint stock company, limited liability company, cooperative society or as the branch office of a payment institution with its registered seat in another EEA state. *(Section 10 (1) of the Payment Service Providers Act)*

- payment institutions operating in the form of joint stock company and limited liability company shall be subject to the provisions of Act V of 2013 on the Civil Code (**Civil Code**) applicable to business associations, limited liability companies and joint stock companies.
- payment institutions operating in the form of cooperative society shall be subject to the provisions of the Civil Code applicable to cooperative societies,

- the payment institutions operating in the form of branch office shall be subject to the provisions of Act CXXXII of 1997 on Hungarian Branch Offices and Commercial Representative Offices of Foreign Companies, with the derogations specified in this Act. *(Section 10 (3) of the Payment Service Providers Act)*

1.2. Personal and material conditions

Payment institutions, which of the payment services provide solely account information services, may commence and pursue the financial services activity only upon the existence of

- internal regulations complying with prudent operations,
- personal conditions necessary for the performance of financial services activity and financial auxiliary services activity,
- IT, technical and security equipment and premises, audit procedures and systems,
- information and control systems for reducing operational risks, and
- transparent organisational structure (**personal and material conditions**).

(Section 2 (3), sub-paragraphs b)-e) and g)-h) of the Payment Service Providers Act)

The personal and material conditions must be also satisfied upon the changing of the registered office or the business location as well as upon amending the financial services activity or the supplementary financial services activity. *(Section 12 (2) of the Payment Service Providers Act)*

II. REGISTRATION RELATED TO PROVISION OF ACCOUNT INFORMATION SERVICES SOLELY

The payment institution providing solely account information services shall register – through an electronic form – the commencement and termination of its activity with the MNB. *(Section 20/A (1) of Payment Service Providers Act)*

The enterprise intending to provide solely account information services shall submit true, complete, accurate and up-to-date information and comply with all provisions prescribed in the relevant guidelines. The details of the information provided by the enterprise intending to provide solely account information services shall be proportionate with the size and internal organisation of the applicant as well as with the nature, range, complexity and risks of the specific services that the applicant intends to provide. *(Paragraph 1.2. of Part 4.2. of the Guidelines)*

When the application contains information or is based on information that is available to the MNB, but the respective piece of information is no longer valid, accurate or complete, the applicant shall forthwith submit the updated version of the application to the MNB. Such application shall indicate the respective information, the place thereof in the original application, explain why the information is no longer valid, accurate or complete, provide the up-to-date information and confirm that the rest of the information included in the original application remains valid, accurate and complete. *(Paragraph 1.5. of Part 4.4. of the Guidelines)*

Pursuant to Directive 2015/2366/EU (**PSD2**), the senior officers and the persons responsible for the management of the payment institution must have good business reputation and possess appropriate knowledge and experience to perform payment services, regardless of the institution's size, internal organisation and the nature, scope, complexity and risks of its activities and the rights and responsibilities of the specific position. *(Paragraph 1.2. of Part 4.2. of the Guidelines)*

All data submitted by the enterprise intending to provide solely account information services are necessary for the assessment of the application; the MNB will treat these in accordance with the professional secrecy obligations set out in the PSD2, without prejudice to the applicable EU laws and the national requirements and procedures on the exercise of the right to access, rectify, cancel or oppose. *(Paragraph 1.5. of Part 4.2. of the Guidelines)*

III. CONTENT OF THE APPLICATION FOR REGISTRATION

The application for registration of the commencement of account information services shall contain, as a minimum

a) the applicant's programme of operations,
b) the medium-term business plan, related to the first three years, also containing a preliminary budget and the facts related to the fulfilment of the personal and material conditions necessary for the operation,
c) the description of the corporate governance and internal audit systems, including the administrative, risk management and accounting procedures, presenting the proportionality, appropriateness and reliability of such corporate governance and audit procedures,
d) the description of the procedures used for the monitoring, management and follow-up of security incidents and security-related customer complaints, including the incident reporting procedure elaborated in accordance with the notification obligation stipulated in Section 55/B of *Act LXXXV of 2009 on the Pursuit of the Business of Payment Services* (**Payment Services Act**),
e) the description of the procedure used for registering, monitoring, tracking and limiting access to sensitive payment data,
f) the description of measures to ensure business continuity, which contains the clear identification of the critical operations, efficient standby plans, and the procedures for the regular testing and review of the suitability and efficiency of such plans,
g) the description of the security principles, and particularly the detailed risk assessment related to the consolidation of account information, and the security check and risk mitigation measures that serve the proper protection of customers against the identified risks, including fraud and the illegal use of sensitive and personal data,
h) the presentation of the applicant's organisational structure and scope of responsibilities, organisational and operational rules as well as the regulations containing the general terms and conditions,
i) if the applicant intends to commission an agent to consolidate the account information, plans to establish branch offices or outsource the operation of its activity, the presentation of this, including the applicant's commitment to inspect the agent, branch office and the entity performing the outsourced activity at least annually,
j) the data of the applicant's senior officer specified in Annex 1, and the following documents confirming the fulfilment of the conditions stipulated in Section 29,
    - the declaration of the candidate related to the non-existence of any disqualifying reasons specified in Section 29 (5)-(6) of the Payment Service Providers Act,
    - curriculum vitae to confirm that he or she has minimum three years' management experience gained in bank or corporate management or in the financial or economic area of public administration, *(Section 29 (5e) of the Payment Service Providers Act)*
    - original, or certified copy of the certificate of clean record – issued in relation the entirety of the data included in the criminal records – with enhanced content (no criminal record, is not banned from exercising civil rights, not disqualified from occupation or activity), not older than 90 (ninety) days, issued by the authority of the country of citizenship or, in the absence thereof, of the country of abode, *(Section 29 (5c) of the Payment Service Providers Act)*
    - in order to prove the good business reputation for the purposes of Section 30 of the Payment Service Providers Act, the questionnaire published on the MNB's website, fully filled in by the candidate.
k) the applicant's Articles of Association, and
l) declaration that the governance of the applicant takes place in its principal office established in the territory of Hungary. *(Section 20 (1) of Payment Service Providers Act)*

The identification data of the applicant intending to provide solely account information services must be also attached to the application.

IV. GUIDANCE WITH REGARD TO THE DOCUMENTS DEFINED IN SECTION III IN ACCORDANCE WITH THE GUIDELINES

4.1 Identification data

Pursuant to Section 2 of Part 4.2 of the Guidelines, the applicant shall provide the following identification data.

a) the applicant's corporate name and, if different, trade name;
b) an indication whether the applicant is already incorporated or is in the process of incorporation;
c) the applicant's national identification number;
d) the applicant's legal status and (draft) articles of association and/or constitutional documents evidencing the applicant's legal status;
e) the address of the applicant's registered office and business site;
f) the applicant's electronic address and website, if available;
g) the name(s) of the person(s) in charge of submitting the application, and their contact details;
h) an indication whether or not the applicant has ever been, or is currently being subject to the supervision of the competent authority in the financial services sector;
i) the registered certificate of incorporation or, if applicable, negative certificate of the commercial register that the name used by the company is available;

4.2. Applicant's programme of operations

Pursuant to Section 3 of Part 4.2 of the Guidelines, the applicant's programme of operations shall contain the following data.

a) step-by-step description of the types of the account information consolidation services, including an explanation how the applicant decided that its activity complies with the account information consolidation services specified in Article 4(16) of PSD2;
b) declaration to the effect that the applicant will never possess the funds;
c) description of the provision of account information consolidation services, including the following:
i. the draft contract between the involved parties, if applicable;
ii. the terms and conditions applicable to the provision of account information consolidation services;
iii. the processing times;
d) the number of different business locations where the applicant intends to provide the payment services, if applicable;
e) description of the ancillary services related to the consolidation of account information services, if applicable;
f) a declaration whether or not the applicant plans to provide account information consolidation services in other EU Member States or third countries after receiving the licence;
g) an indication whether or not the applicant intends, in the next three years, to provide or already provides business activities other than the consolidation of account information as referred to in Article 18 of Directive 2015/2366/EU, including a description of the type and expected volume of the activities;
h) the information specified in the EBA Guidelines (EBA /GL/2017/08) on the criteria of how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5 (4) of Directive (EU) 2015/2366 where the applicant intends to provide solely the services stipulated in Section 8.

4.3. Business plan of the applicant

Pursuant to Section 4 of Part 4.2 of the Guidelines, the business plan shall contain the following data.

a) marketing plan containing the following information:
    i. analysis of the company's competitive position;
    ii. description of the users of the account information consolidation services in the respective segment of the account information consolidation market, and of the marketing materials and distribution channels;

b) audited annual accounts of the previous three years, if available, or a summary of the financial situation of the companies that have not yet produced annual accounts;
c) forecast budget calculation for the first three financial years that demonstrates that the applicant is able to apply appropriate and proportionate systems, resources and procedures necessary for its reliable operation.

The planned budget shall include:

i. an income statement and balance-sheet forecast, including target scenarios and stress scenarios as well as their benchmark assumptions, such as volume and value of transactions, number of clients, pricing, average amount per transaction, expected increase in profitability threshold;
ii. explanations of the main components of income and expenses, the financial debts and the capital assets;
iii. diagram and detailed breakdown of the estimated cash flows for the next three years.

4.4. Organisational structure

Pursuant to Section 5 of Part 4.2 of the Guidelines, the presentation of applicant's organisational structure shall cover the following.

a) detailed organisational chart, showing each division, department or similar structural unit, including the name of the person(s) responsible, in particular those in charge of internal audit functions; the chart shall be accompanied by descriptions of the functions and responsibilities of each division, department or similar structural unit;
b) an overall forecast of the number of employees for the next three years;
c) description of the relevant outsourcing schemes, particularly:
i. the identification data and geographical location of the outsourcing provider;
ii. identification data of the persons responsible, within the account information consolidation provider, for the individual outsourced activities;
iii. clear description of the outsourced activities and their main characteristics;

d) copy of each draft outsourcing contract;
e) description of the use of branches and agents, where applicable, including:
i. statement of the offsite and onsite inspections that the applicant intends to perform in the branches and at the agents;
ii. the IT systems, processes and infrastructure used by the applicant's agents to perform activities on behalf of the applicant;
iii. in the case of agents, the selection policy, monitoring procedures and agents' training and, where applicable, the draft terms of engagement;

f) list of all natural persons and legal entities that have close relation with the applicant, indicating their identification data and the nature of the relation.

4.5. Corporate governance and internal audit mechanisms

Pursuant to Section 6 of Part 4.2 of the Guidelines, the applicant shall describe the Corporate governance and internal audit mechanisms, in particular:

a) a statement of the risks identified by the applicant, including the type of risks, and the procedures applied by the applicant for the assessment and prevention of the risks;
b) the procedures supporting the execution of the planned periodic and ongoing audits, including the frequency of the audits and the allocated human resources;
c) the accounting procedures applied for the recording and reporting of the applicant's financial information;

d) the identity of the person(s) in charge of the internal control functions, including the persons responsible for the periodic and ongoing control and for ensuring compliance, and the up-to-date curriculum vitae of such persons;
e) the name of any auditor that is not a statutory auditor within the meaning of Directive 2006/43/EC;
f) the composition of the management body and, if applicable, of any other supervisory body or committee;
g) description of the method applied by the payment institution for the monitoring and audit of outsourced functions to ensure that the quality of its internal audit does not deteriorate;
h) description of the method applied by the applicant for the monitoring and audit of the agents and branches within the framework of its internal audit;
i) if the applicant is the subsidiary of a regulated entity in another EU Member State, the description of the group governance.

4.6. Procedures used for the monitoring, management and follow-up of the security incidents and the customer complaints related to security

Pursuant to Section 7 of Part 4.2 of the Guidelines, applicant shall describe the procedures used for the monitoring, management and follow-up of the security incidents and the customer complaints related to security:

a) organisational measures and tools for the prevention of fraud;
b) detailed data of the persons and bodies responsible for providing assistance to clients in the event of fraud, technical issues and/or claim management;
c) reporting line in cases of fraud;
d) contact point for clients, including a name and email address;
e) procedures for the reporting of incidents, including the communication of these notifications to internal or external bodies, including notification of major incidents to national competent authorities under Article 96 of PSD2, and in line with the EBA Guidelines on incident reporting stipulated in the aforementioned article.
f) the monitoring tools used and the follow-up measures and procedures in place to mitigate security risks.

4.7. Access to sensitive payment data

Pursuant to Section 8 of Part 4.2 of the Guidelines, the applicant shall provide a description of the processes in place to register, monitor, track and restrict access to sensitive payment data, in particular:

a) description of the data flows classified as sensitive payment data in the context of the business model related to the account information consolidation services;
b) the procedures in place to authorise access to sensitive payment data;
c) description of the monitoring tool;
d) access right policy, detailing access to all relevant infrastructure components and systems, including databases and back-up infrastructures;
e) description of the method of filing the collected data;
f) the expected internal and/or external use of the collected data, e.g. by the contracting parties;
g) the IT system and the implemented technical security measures, including encryption and/or tokenisation;
h) identification of the individuals, bodies and/or committees with access to the sensitive payment data;
i) an explanation of how breaches will be detected and addressed;
j) the annual internal audit plan related to the safety of the IT systems.

4.8. Presentation of business continuity measures

Pursuant to Section 9 of Part 4.2 of the Guidelines, the applicant shall describe the business continuity measures by providing the following information:

a) business impact analysis, including the business processes and recovery objectives, such as recovery time objectives and recovery point objectives and protected assets;
b) identification data of the back-up site, access to IT infrastructure, and the critical/key software and data necessary for recovery in the event of a disaster or disruption;
c) an explanation of how the applicant will deal with significant continuity events and disruptions, such as the failure of critical/key systems; the loss of critical/key data; the inaccessibility of the premises; and the loss of key persons;
d) how often does the applicant intend to verify its business continuity and disaster recovery plans, including the manner of recording the results of the verification.

4.9. Description of the security principles

Pursuant to Section 10 of Part 4.2 of the Guidelines, the applicant shall describe its security regulation by providing the following information:

a) detailed assessment of the risks related to the payment services the applicant intends to provide, including the risk of fraud and the security control and risk mitigating measures introduced by the applicant to provide the users of the payment services with proper protection against the identified risks;
b) description of the IT systems in accordance with the following content:
    i. architecture and network elements of the systems;
    ii. the business IT systems supporting the business activities provided (e.g. the applicant's website, wallets, the payment engine, the risk and fraud management engine, and customer accounting);
    iii. IT systems supporting the organisation and administration of the applicant (e.g. accounting, legal reporting systems, human resource management, customer relationship management, e-mail servers and internal file servers);
    iv. information on whether the applicant or the applicant's group already uses these systems; if the systems are not in use yet, the estimated date of implementation;
c) type of authorised external connections (e.g. connection with counterparties, service providers, other legal entities of the group and employees working remotely), including the justification for these connections;
d) for each of the connections listed under point c), the logical security measures and mechanisms in place, specifying the control the payment institution will have over such access as well as the nature and frequency of each control, such as technical versus organisational; preventive or detective; and real-time monitoring or regular reviews, (e.g. use of an active directory separated from the group, the opening/closing of communication lines, security equipment configuration, generation of keys or client authentication certificates, system monitoring, authentication, confidentiality of communication, intrusion detection, antivirus systems and logs);
e) logical security measures and mechanisms controlling internal access to IT systems, with the following content:
    i. technical or organisational nature and frequency of the individual measures, i.e. indicating whether the measure is preventive or detective, and whether or not it is carried out in real time;
    ii. how the issue of client environment segregation is dealt with when the applicant's IT resources are shared;
f) measures and mechanisms ensuring the physical security of the applicant's premises and data centre, such as access controls and environmental security;
g) security of the IT systems in accordance with the following content:
    i. customer authentication procedure used for both consultative and transactional access,
    ii. explanation of how safe delivery to the legitimate payment service user and the integrity of the authentication factors at the time of both initial enrolment and renewal,
    iii. description of the systems and procedures introduced by the applicant to analyse transactions and identify suspicious or unusual transactions.
h) detailed risk assessment related to the applicant's payment services (e.g. fraud, with reference to the control and mitigation measures explained in the application file, demonstrating that the risks are addressed);

i) list of the main written procedures in relation to the applicant's IT systems or, for procedures that have not yet been formalised, an estimated date for their finalisation.

4.10. Identity and suitability assessment of senior executives and officers responsible for management

Pursuant to Section 11 of Part 4.2 of the Guidelines the applicant shall provide the following information with regard to the identity of its senior executives and officers in charge of the management and to the assessment of their suitability:

a) personal data with the following content:
   i. full name, gender, place and date of birth, address and nationality, and personal identification number or copy of ID card or equivalent;
   ii. details of the position for which the assessment is sought, and indication whether or not the position in the management body is executive or non-executive; the information shall cover the following details:
      - letter of appointment, contract, offer of employment or relevant drafts, as applicable;
      - planned start date and duration of the mandate;
      - description of the individual's key duties and responsibilities;

b) where applicable, information on the suitability assessment carried out by the applicant, which shall include details of the result of any assessment of the suitability of the individual performed by the institution, such as relevant board minutes or suitability assessment reports or other documents;

c) evidence of knowledge, skills and experience, which shall include a curriculum vitae containing details of education and professional experience, including academic qualifications, other relevant training, the name and nature of all organisations for which the individual works or has worked, and the nature and duration of the functions performed, in particular highlighting any activities within the scope of the position sought;

d) evidence of good reputation, honesty and integrity, which shall include:
   i. criminal records and relevant information on criminal investigations and proceedings, relevant civil and administrative cases, and disciplinary actions, including disqualification as a company director, bankruptcy, insolvency and similar procedures, confirmed by an extract from the judicial record or equivalent instrument concerning the absence of criminal conviction, investigations and proceedings, such as third-party investigations and testimonies made by a lawyer or a notary established in the European Union;
   ii. statement as to whether criminal proceedings are pending or the person or any organisation managed by him or her has been involved as a debtor in insolvency proceedings or comparable proceedings;
   iii. information on the following; - investigations, enforcement proceedings or sanctions by a supervisory authority that the individual has been directly or indirectly involved in; - refusal of registration, authorisation, membership or licence to carry out a trade, business or profession; or withdrawal, revocation or termination of registration, authorisation, membership or licence; or expulsion by a regulatory or government body or by a professional body or association; dismissal from employment or a position of trust, fiduciary relationship, or having been asked to resign from employment in such a position, excluding redundancies; whether or not an assessment of the reputation of the individual as an acquirer or a person who directs the business of an institution has already been conducted by another competent authority, including the identity of that authority, the date of the assessment and evidence of the outcome of this assessment, and the consent of the individual, where required, to seek and process such information and use the provided information for the suitability assessment; whether or not any previous assessment of the individual, commissioned by another, non-financial sector authority, has already been conducted, including the identity of that authority and evidence of the outcome of such an assessment.

4.11. Professional indemnity insurance or a comparable guarantee

The payment institution providing account information services shall have professional indemnity insurance covering the territories in which they offer services, or some other comparable guarantee against their liability vis-à-vis the account servicing payment service provider or the payment service user resulting from non-authorised or fraudulent access to or non-authorised or fraudulent use of payment account information. *(Section 13/A (2) of Payment Service Providers Act)*

Pursuant to Section 12 of Part 4.2 of the Guidelines, as an evidence of a professional liability insurance or comparable guarantee complying with the provisions of Article 5 (2) and 5 (3) of PSD2, the applicant shall provide the following information:

a) an insurance contractor other equivalent document confirming the existence of professional indemnity insurance or a comparable guarantee, with a cover amount that is compliant with the aforementioned EBA Guidelines;
b) documentation that the method used by the applicant to calculate the minimum amount complies with the aforementioned EBA Guidelines, including all applicable components of the formula specified therein.

V. PERSONAL REQUIREMENTS

The personnel at the payment institutions, named specifically by the Payment Providers Act, include the senior executive, the internal auditor and the auditor.

5.1. Senior executives of the payment institution

Pursuant to the provisions of Section 3 (40) of the Payment Service Providers Act, the following persons shall qualify as senior executives of the payment institution:

- the person in charge of managing the payment services business of the payment institution, including all deputies
- the managing director.

5.2. Internal auditor

The payment institution shall employ at least one internal auditor. *(Section 32 (2) of the Payment Service Providers Act)*

Only such person may be appointed as the head of the internal audit unit, or – if the payment institution employs only one internal auditor – only such person may be entrusted with the internal audit duties, who

- has a university-level degree in the relevant field or is a certified chartered accountant,
- has at least three years of professional experience, and
- has clean criminal record. *(Sub-paragraphs a)-c) of Section 32 (5) of the Payment Service Providers Act)*

With a view to ascertaining that the internal auditor satisfies the relevant requirements, the payment institution shall ask the candidate to submit the following documents:

- original instrument or notarised copy of the document confirming the university-level degree in the relevant field /certified chartered accountant qualification,
- employer's certificate(s) to confirm the professional experience of at least three years,
- certificate of clean criminal record with enhanced content not older than 90 days

Pursuant to the provisions of sub-paragraphs a)-d) Section 32 (6) of the Payment Service Providers Act, the following shall be recognized as a university-level degree in the relevant field:

- a university or college diploma in economics under Act LXXX of 1993 on Higher Education, or a degree in economics obtained in basic and masters training within the framework of economic sciences in accordance with Act XXXXIX of 2005 on Higher Education,
- a law degree,
- a diploma in accountancy; or a diploma in higher education or post graduate qualification in the banking profession.

5.3. Rules applicable to the auditor

In the case of payment institutions the auditor commissioned for auditing services shall be a certified auditor or registered statutory auditor (audit firm) holding a valid authorization for auditing, if

- the auditor (audit firm) is certified to audit financial institutions,
- the auditor do not have any, direct or indirect, ownership interest in the payment institution,
- the auditor has no loan debt towards the payment institution,
- neither of the members with a qualifying holding in the payment institution has any, direct or indirect, ownership interest in the audit firm. *(Sub-paragraphs a)-d) of Section 35 (1) of the Payment Service Providers Act)*

The restrictions specified in sub-paragraphs c)-d) of paragraph (1) shall also apply to the close relative of the auditor. *(Section 35 (2) of the Payment Service Providers Act)*

VI. SPECIAL PROVISIONS APPLICABLE TO THE ACTIVITY OF PAYMENT INSTITUTIONS PROVIDING SOLELY ACCOUNT INFORMATION SERVICES

A payment service user has the right to make use of services enabling access to the account information services, if his payment account is accessible online. *(Section 38/C (1) of the Payment Services Act)*
The use of the account information services shall not be conditional on the existence of a contractual relationship between the account information service provider and the payment account servicing payment service provider for that purpose. *(Section 38/C (2) of the Payment Services Act)*

The payment service provider providing account information services

a) shall provide services solely on the basis of the payment service user's explicit consent,
b) shall ensure that the personalized security credentials of the payment service user are not, with the exception of the user and the issuer of the personalized security credentials, accessible to other parties and that they are transmitted through safe and efficient channels,
c) for establishing and maintaining each communication session, it shall identify itself towards the payment account servicing payment service provider of the payment service user and securely communicate with the payment account servicing payment service provider and the payment service user,
d) shall access only the information from payment accounts designated by the payment service user and from associated payment transactions,
e) shall not request sensitive payment data linked to the payment account, and
f) shall not use, access and store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with the data processing and data protection requirements set out by legislation and directly applicable acts of the European Union. *(Section 38/C (3) of the Payment Services Act)*

With a view to making use of account information services, the payment account servicing payment service provider

a) shall communicate securely with the account information service provider, and
b) treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons. *(Section 38/C (4) of the Payment Services Act)*

***

Institutions existing on 12 January 2018, which are not authorized to provide payment services, engaged in providing either payment initiation services or account information services, or both, shall fulfill the obligation for the submission of an application for authorization under the Payment Service Providers Act, or the obligation of notification after 13 January 2018 without delay, and may pursue such activities until the evaluation of the application according to the provisions in effect on 12 January 2018. *(Section 92 (6) of Payment Service Providers Act)*

Pursuant to Section 3(4) of MNB Decree 32/2023. (VII. 19.) on the administrative service fees of the Magyar Nemzeti Bank applied in certain licensing and registration procedures in the context of the supervision of the financial intermediary system and with respect to trustee enterprises, the conduct of the notification procedure is subject to the payment of administrative service fee by the payment institution providing solely account information services in the amount of HUF 1.400.000.

Further information about the administrative service fee is available in the following link:
https://www.mnb.hu/letoltes/tajekoztatas-a-magyar-nemzeti-bank-altal-egyes-engedelyezesi-es-nyilvantartasba-veteli-eljarasokban-alkalmazott-igazgatasi-szolgaltatasi-dijrol.pdf

Should, after carefully reading this guide, any further question – related to the respective, individual case, not possible to answer in the form of consultation over the phone or in writing – arise, the MNB provides the applicant with the possibility of personal consultation. For the possibility of personal consultation, contact the secretariat of the Money and Capital Markets Licensing Department (telephone number: (Telephone: +361-489-9731 or +361-489-9381; Email: ptef@mnb.hu).

If the questions are solely of IT nature, you may also contact the Information Technology Supervision Department directly for the purpose of personal consultation (Telephone: +361-489-9321; Email: iff@mnb.hu).

Last amendment: August 2023