Renewed regulation for service providers based on Decree no. 26/2020. (VIII. 25.) of MNB

KPMG Legal Tóásó Law Firm

9 October 2020

Renewed regulation for service providers

Decree no. 26/2020. (VIII. 25.) of MNB

- The previous **Decree no. 45/2018. (XII.17.) of MNB** expired
- The decree shall be applied by **service providers**: credit institutions, financial services institutions, institutions for occupational retirement provision, voluntary mutual insurance funds, operators accepting and delivering international postal money orders and fiduciary managers.
- **General date of entry into force:** 1 October 2020
- **Special date of entry into force regarding new mandatory filtering cases** (*see p. 9*): 1 January 2021

Reasons for the revised regulation

- Keeping up with changes occured due to the comprehensive **amendment of the Hungarian AML Act** effective as of 10 January 2020
- Putting into practice the **supervisory experience of MNB**
- Supporting the development of **IT technologies / innovative operation** of service providers

Recent practice of MNB

During the summer of 2020, MNB has imposed **penalties** amounting to a total of **HUF 124.2 million** to six credit institutions due to failure to comply with the rules on prevention and combating of money laundering and terrorist financing. Typical **reasons for penalties** were that the banks:

- have not reported a number of **suspicious transactions**;
- have not operated their **internal monitoring and information systems** appropriately;
- have filtered **suspicious cash transactions** inaccurately;
- have not obtained the necessary **manager approvals** for significant transactions.

Fundamental shift in approach

Rules-based approach

Risk-based approach

!

- ✓ Service providers gain **greater autonomy in identifying their risks**;
- ✓ **Internal risk assessment systems** come to the fore;
- ✓ Previously **exhaustive lists of cases** prescribed by law are no longer applicable;
- ✓ Service providers may **identify new cases or ignore previous cases**;
- ✓ There are **fewer cases subject to the decision of the service providers' managers**;
- ✓ The **supervisory approval** is no longer necessary in a number of cases (e.g., in case of simplified or enhanced customer authentication)

Strong Customer Authentication (SCA)

Two-factor authentication

The Decree introduces the definition of **strong customer authentication** as the material requirement of the two-factor authentication, which provides that the customer authentication should be carried out based on **at least two factors out of the following three categories**:

SOMETHING THE CUSTOMER KNOWS

= information known by the customer (e.g., password)

SOMETHING THE CUSTOMER HAS

= an object in the exclusive possession of the customer (e.g., phone, messages delivered to the phone no.)

SOMETHING THE CUSTOMER IS

= biometric characteristics of the customer (e.g.: fingerprint, face recognition)

→ The categories are **independent from each other**, which ensures that cracking one of them would not affect the reliability of the others.

→ The **confidentiality of identification data** is ensured by the set procedure.

Example: *A traveler would like to buy her flight ticket online. Therefore, she should provide the airplane company with (1) her bank account details (‚knowledge') and (2) the code sent to her mobile in a message (‚possession') in order to have her online payment accepted.*

Video-based customer authentication methods

Simple **'selfie-based'** customer authentication

Customer authenication through the **KAÜ system**

NEW

Customer authentication with the **E-ID ePASS** function

Subject to certain <u>restrictions</u> applicable to the customer

→ The customer's domicile / residence is <u>not</u> in a third-country of special risk;

→ It is not a cash transaction;

→ It is not a transfer to a non-EU country;

→ The transaction value is less than HUF 10 million.

Service providers may apply these authentication methods <u>irrespective of the customer's risk classification</u> as both methods involve sufficient security controls

Example for the selfie-based authentication: *Someone would like to open a Revolut account. First, she would need to download the service provider's application, then she could initiate the opening of the account by providing her personal identification data + attaching the pictures taken of her ID card and her face. The service provider would check the incoming data and open the account if the data is appropriately verified.*

Further specifications

„Liveness test”

It must be **possible to establish** through the audited electronic means of communication, that:

- ✓ the person who is subject to the authentication procedure is **a real, living person;**
- ✓ the person who is subject to the authentication procedure uses the electronic means of communication **personally in real time**;
- ✓ the live record is **not manipulated**.

Accepted documents for identification

The person subject to the authentication through audited electronic means of communication may identify herself by her

- ✓ personal identification card;
- ✓ **passport;**
- ✓ driving license (card format only).

Mandatory check of documents’ expiry date

Service providers are obliged to check the expiry date of ID documents. However, they are free to choose the means of it, therefore, they are not required to inquire with the authority which issued the document concerned.

Simplified and enhanced customer authentication

Simplified authentication

→ There are **no mandatory cases** of simplified authentication fixed by law.

→ Service providers may apply the simplified authentication method in case of **low-risk customers** which is established based on their internal risk assessment system.

Enhanced authentication

→ Service providers are **obliged to apply** the enhanced authentication in cases set by law.

→ Service providers may only be **exempted from this obligation,** if it is reasonable due to the customer's unusually complex ownership structure and it is also supported by appropriate risk-sensitivity considerations.

Cases where the supervisory authority's approval was required are no longer applicable.

Cases of strengthened procedure

- Previous cases are supplemented by the activities of **transit accounts and transactions of clients already notified before**.

- **Service providers may…**
  - ✓ Identify new cases, or
  - ✓ Neglect to apply previously prescribed cases.

- In case of filtering obligation, service providers shall determine and apply **transaction thresholds in addition to** fixing a maximum threshold.

Example of a new case of strengthened procedure: *The service provider shall resort to the strengthened procedure, if the service provider applies due diligence measures for long-time customers due to transactions amounting to HUF 50 million or more. The strengthened procedure shall be applied for one year starting from the last transaction reaching the amount of HUF 50 million.*

Rules on internal regulation 1.

Requirements of internal policies

Service providers shall **modify their internal policies,** provided that the internal policies set the applicable rules to be followed when **identifying risks** and **determining measures** to be taken to mitigate such risks.

Business continuity requirement

- Service providers must report if their **filtering system fails to operate** for more than 24 hours.
- Such **reports** must be made electronically to the MNB without delay through the ERA system of MNB.

Rules on internal regulation 2.

Internal monitoring systems

- ✓ Possibility to apply **alternative filtering options.**
- ✓ **The deadline for assessing and analyzing the filtering results** has been extended by 20 days (the day of the filtering shall not be counted falling within this period).
- ✓ Even in case of **manual filtering**, service providers shall apply a filtering system.

Transactions to be filtered

Transactions which are subject to mandatory filtering are to be expanded by the following cases from **1 January 2021:**

- ✓ **Money transfer in the amount of HUF 25 million or more** received / transferred by a customer which is a legal entity / entity without legal personality and has no tax number;
- ✓ **Money transfer in the amount of HUF 50 million or more** received / transferred by a customer which is a legal entity / entity without legal personality and has a foreign tax number;

Trainings

Service providers are obliged to hold at least a **prevention training**. Requirements of such trainings are as follows:

Fixed dates of trainings:
→ Date of employees' entry;
→ Date of another session held at least once a year.

Training programs matched with job positions

Exam requirements for employees

Training requirements in light of group-level policies and procedures

Employing persons who are well aware of the respective regulation and are capable to identify risks and to properly handle them

Personal liability

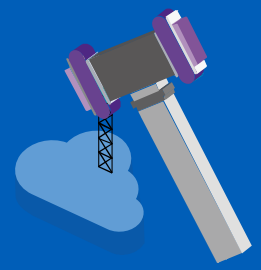
Service providers' managers and employees are subject to…

- Strict personal liability rules, and
- Sanctions of the MNB, which are directly applicable to them.

Sanctions

- **Notification**

- **Fines**
  → managers: HUF 100.000 – 500.000.000
  → other employees: HUF 20.000 – 20.000.000



It is important to note that the service provider cannot pay the fines instead of the employees!

Example: *An employee of a bank's branch office may be held personally liable if she failed to report money transfers of unusually large amounts.*

Please let us know of any questions!

dr. Bálint Tóásó MSc LL.M (Vienna)
Partner, Attorney-at-Law
T: +36 30 663-6245
E: balint.toaso@kpmg.hu

dr. Boglárka Kricskovics-Béli
Attorney-at-Law
T:+36 70 520 4507
E: boglarka.kricskovics-beli@kpmg.hu

dr. Zsóka Erdősy
Associate
T: +36 70 520 4433
E: zsoka.erdosy@kpmg.hu

kpmg.com/socialmedia

kpmg.com/app