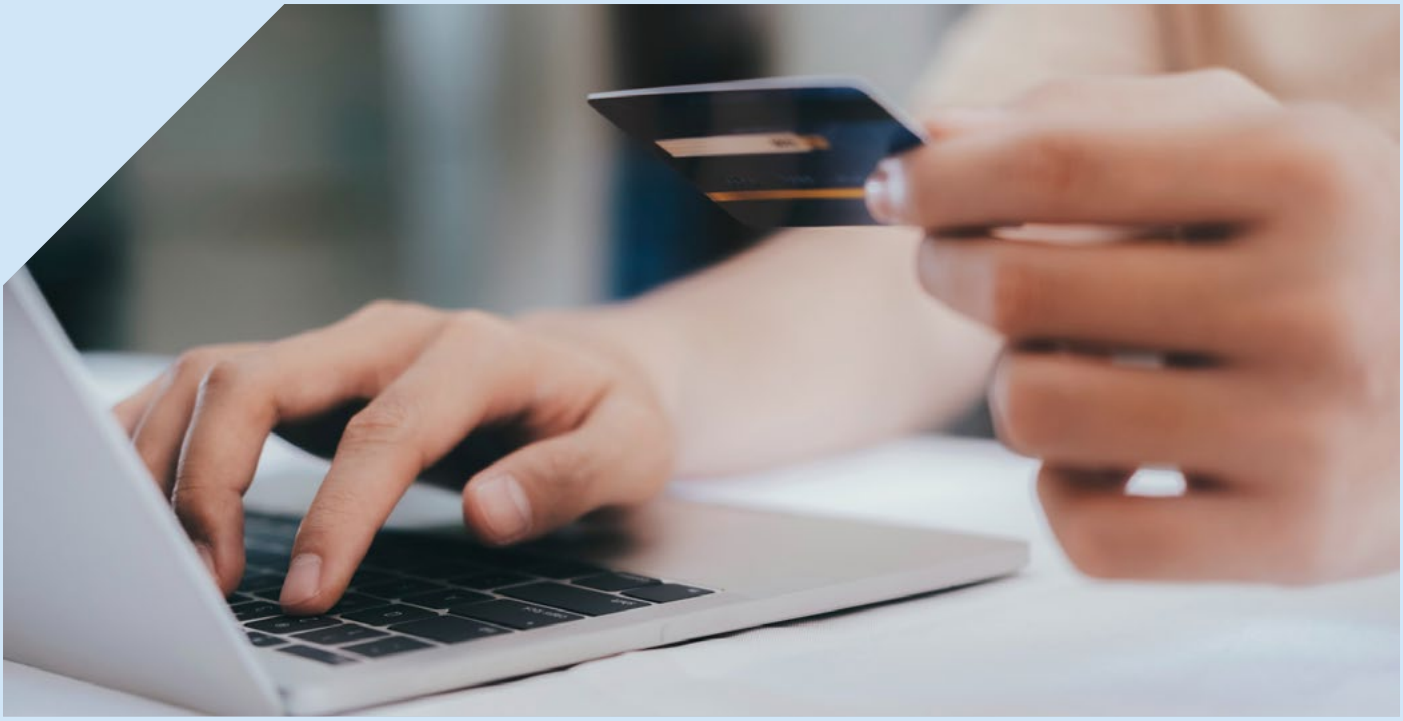
TEGOS

BANKING AND FINANCE NEWS

CONTENT



Procedure for restricting payments for online lotteries and gambling

On 3 May 2025, the Order of the Director of the Gaming Control Authority "On the Approval of the Description of the Procedure for the Restriction of Payments for Participation in Remote Gambling and Lotteries Organised by Operators of Unlawful Gambling Activities, the Tickets of which are Distributed Online through Payment Service Providers Operating in the Republic of Lithuania" (**Description**) came into force.

Based on Description:

- operations initiated with a payment card related to remote gambling (acceptance of bet amounts and payout of winnings) may only be carried out with service providers that are included in the list of the Gambling Supervisory Authority (hereinafter – the **Supervisory Authority**) and are authorized to conduct such activities in Lithuania;
- similarly, operations initiated with a payment card related to lotteries (acceptance of ticket payments and payout of winnings) are allowed only with entities included in the Supervisory Authority's list and authorized to conduct lottery activities, or with their designated ticket distributors.

In addition, the Description confirms the following **restrictions on illegal gambling**: it sets out the procedure for the termination of all payment transactions with unlawful gambling operators for payment service providers (**PSPs**).

Key provisions:

- Lists of gambling operators and operators distributing lottery tickets online are maintained and published by the Supervisory Authority on its website http://lpt.lrv.lt in accordance with the Law on Gaming and the Law on Lotteries.

- The Supervisory Authority informs the PSPs of the update of the lists by means of electronic communications immediately, but no later than two business days after their update.
- The PSPs must integrate the new data into their systems no later than 5 business days after receiving the information.
- The PSPs must use technical means that:
  - identify payment transactions related to non-listed entities;
  - refuse payment transactions if the payee or payer is not on the lists.
- Payment transactions must be automatically declined in the following cases:
  - funds are sent to an entity that is not on the list;
  - funds are received from an entity that is not on the list.
- The details of the payer or payee in the payment transactions must match the details in the lists.

TEGOS comment: From now on, the PSPs will have to pay even more attention to payments related to gambling and lotteries. All payment transactions by illegal gambling operators should be stopped, and transactions initiated by card payments can only be made with the entities listed by the Supervisory Authority.

More information here →

The EBA's conclusion on the compliance of non-bank payment service providers with the safeguarding requirements in PSD2

On 8 May 2025, the European Banking Authority (**EBA**) published a response on the compliance of non-bank payment service providers (**NB PSPs**) with the requirements for safeguarding client funds under the Payment Services Directive (**PSD2**).

On 18 July 2024, the European Central Bank (**ECB**) published a policy (**Policy**) governing the access of NB PSPs, in particular payment institutions (PIs) and electronic money institutions (EMIs), to central-bank operated payment systems. The policy defines the conditions under which the NB PSPs can participate directly in these systems and stipulates that settlement accounts will be offered for the sole purpose of processing payment transactions. The ECB also indicated that safeguard accounts used to protect the funds of payment service users in accordance with the relevant requirements of the Payment Service Directive 2 (**PSD2**) will not be provided in Eurosystem central-bank operated payment systems.

In accordance with Article 10(1) of the PSD2, the NB PSPs are required to safeguard payment service users' funds in either of the following ways:

1. Funds shall not be commingled with the own funds of the NB PSPs. If they are not transferred to the payee or another payment service provider by the end of the business day following the day when the funds have been received, they shall be:
   - deposited in a separate account in a credit institution or a central bank (if allowed),
   - invested in secure, liquid, low-risk assets.

2. Funds shall be covered by an insurance policy or some other comparable guarantee from an insurance company or a credit institution, which does not belong to the same group as the payment institution itself, for an amount equivalent to that which must be separated.

In order to clarify how non-bank PSPs with direct access to central-bank operated payment systems should adequately implement the requirements for safeguarding client funds under the restrictions set out in the Policy, on 8 August 2024, the EBA was asked whether non-bank PSPs with direct access to central-bank operated payment systems for settling payment transactions would comply with the safeguarding requirements of Article 10 of the PSD2 if the settlement balance of the account were held at a central bank/payment system without the central bank managing the non-bank PSP's safeguarding account.

The EBA has clarified that if a central bank does not provide accounts for safeguarding funds, the holding of client funds in a settlement account at the end of the business day following the receipt of the funds does not constitute an adequate means of safeguarding client funds within the meaning of Article 10(1) of the PSD2. Only when the central bank offers safeguarding accounts, the NB PSPs with direct access to the central-bank operated payment system may deposit funds into a safeguarding account and be considered to be adequately fulfilling the requirements for safeguarding client funds under Article 10(1) of the PSD2.

TEGOS komentaras: The EBA's response awaited by the NB PSPs did not provide a different interpretation of the aspects of compliance with the requirements of Article 10 of the PSD2. The NB PSPs that have held client funds in accounts opened in the Eurosystem central-bank operated payment system must, as from 9 April 2025, find other operational ways to meet the liquidity needs of the central bank payment system and to comply with the requirements for safeguarding client funds. As an alternative, the Bank of Lithuania encourages market participants to make more active use of insurance as a way to protect client funds, especially if NB PSPs make payments through the payment system of CENTROlink or another central bank.

More information here →

The Parliament adopts amendments to the Law on Markets in Crypto-assets

On 19 June 2025, the Parliament adopted the Law (No. XV-308) amending Articles 3, 10, 12, 13, 14, 15 of, and the Annex to, the Law on Markets in Crypto-assets (No. XIV-2879) (**MCAL**).

Main amendments:

- Issuers of asset-referenced tokens and crypto-asset service providers are obliged to comply not only with the provisions of Regulation (EU) 2023/1114 (**MiCAR**) and the MCAL, but also with the provisions of any other legislation, the supervision of which falls under the competence of the supervisory authority.
- It provides that sanctions may also be imposed in cases of breaches of the requirements of Regulation (EU) 2022/2554 (**DORA**) and gives the supervisory authority additional powers to impose fines for non-compliance with these requirements, on top of the existing powers to impose sanctions for breaches of the MiCAR and the MCAL.

TEGOS comment: In light of the amendments to the MCAL, issuers of asset-referenced tokens and crypto-asset service providers should perform a careful self-assessment of the compliance of their activities not only with the MiCAR but also with the DORA. This is particularly relevant for service providers that manage information systems related to the provision of critical services to the financial sector.

More information here →

The Council of the European Union adopts the 17th package of sanctions against Russia

The 17th package of sanctions against Russia was adopted on 20 May 2025. The sanctions package aims to further restrict Russia's access to battlefield technology and cut revenues from Russian energy imports by targeting an unprecedented number of vessels from Russia's shadow fleet.

Measures envisaged:

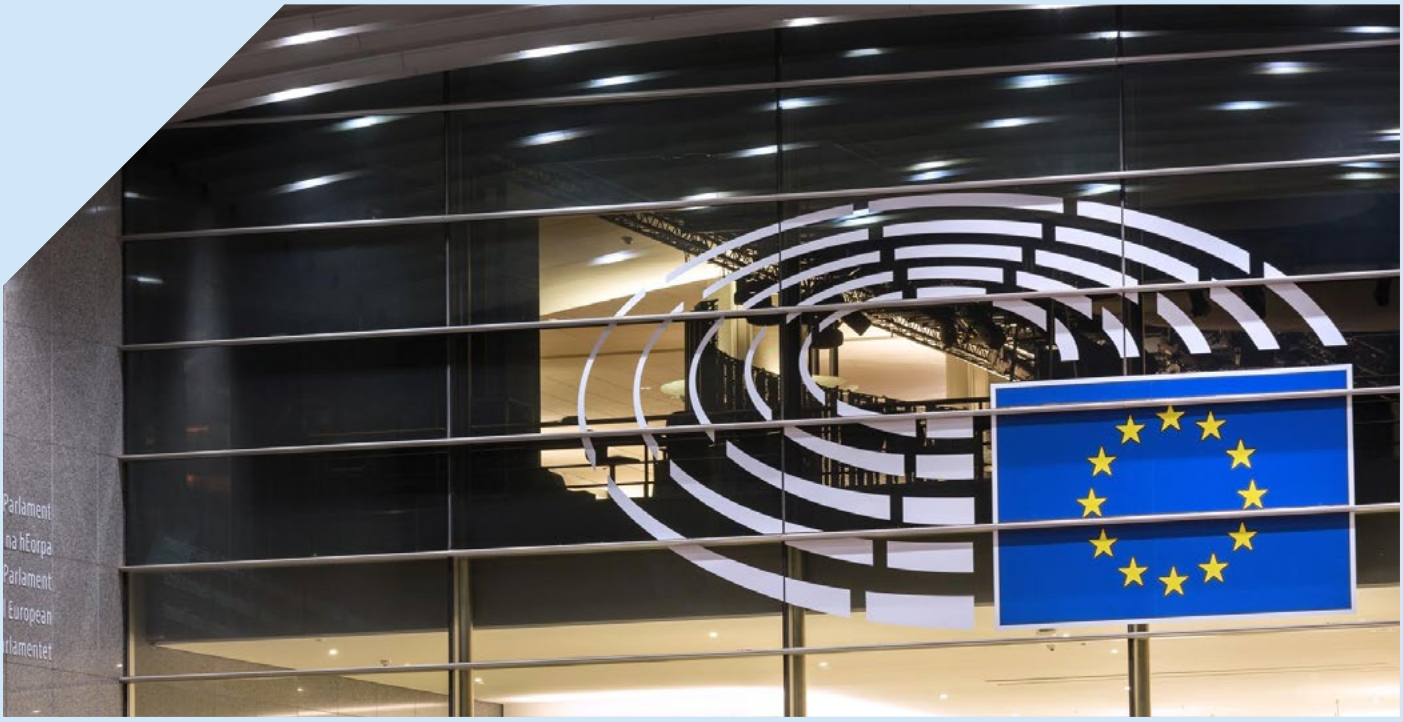
- This package also adds 31 new companies to the list providing direct or indirect support to Russia's military industrial complex, or engaged in sanctions circumvention. This includes 18 companies established in Russia, and 13 established in third countries.
- The list of items that could contribute to Russia's military and technological development or to the development of its defence and security sector is expanded to include items used by Russia in its aggressive war against Ukraine and items contributing to the development or production of its military systems, including chemical precursors to energetic materials and spare parts for machine tools.
- It prolongs an existing exemption from the oil price cap, which allows crude oil produced from the Sakhalin-2 project in Russia to be transported by ship to Japan in view of energy security concerns. The extension is granted for one year until 28 June 2026.
- The list of ships includes 189 additional vessels which are banned from entering Member States' ports and locks, as well as from receiving a wide range of maritime transport-related services.

The 17th package of sanctions includes 75 additional listings, including 17 individuals and 8 entities, responsible for actions undermining the territorial integrity, sovereignty, and independence of Ukraine. They are now subject to asset freezes and prohibition to make economic resources available, and – in the case of individuals – also to travel bans.

Measures envisaged: The EU has extended financial sanctions against third-country entities supporting Russia's military-industrial complex, including entities from China, Belarus, and Israel. In addition, 31 new entities are subject to stricter export restrictions on dual-use goods and technologies, some of which are located in Serbia, UAE, Turkey, Vietnam, and Uzbekistan.

The EU once again condemned Russian aggression and imposed significant shadow fleet sanctions, which are the most significant of the G7 decisions in this area. With 75 additional listings, the EU measures now cover more than 2,400 individuals and entities.

More information here →



The EU has adopted its 18th package of sanctions against Russia

On 18 July 2025, the Council of the European Union (**EU**) adopted the 18th package of sanctions against Russia. This package is designed to restrict exports, reduce Russian revenue streams, and adjust the price cap on Russian oil. According to the EU, these measures are part of efforts to increase pressure on Russia in light of its ongoing war against Ukraine.

Key measures in the banking sector:

- The current ban on using the SWIFT system has been extended to a complete ban on any transactions with Russian entities and financial institutions. Sanctions have also been imposed on 22 Russian banks and financial operators from third countries that are helping to circumvent existing sanctions by financing trade with Russia.

- Expanded sanctions on the Russian Direct Investment Fund, its subsidiaries, and investment projects. This is intended to restrict financing channels for the modernization of the Russian economy and the strengthening of its industrial base.
- Restrictions imposed on third-country financial and credit institutions and crypto-asset service providers that support Russia's war or help circumvent sanctions.
- Any operators from third countries are prohibited from conducting transactions related to circumventing the oil trade ban.
- A ban has been imposed on the sale, supply, or transfer of software management systems and software designed for use in the financial sector to Russia.

Export restrictions:

Additional restrictions are being imposed on exports of so-called "*key technologies and industrial goods*" to Russia. This list includes goods with a total value of over EUR 2.5 billion, such as machinery, metals, plastics, chemicals, and dual-use technologies that could be used in Russia's military-industrial complex.

Energy sector restrictions:

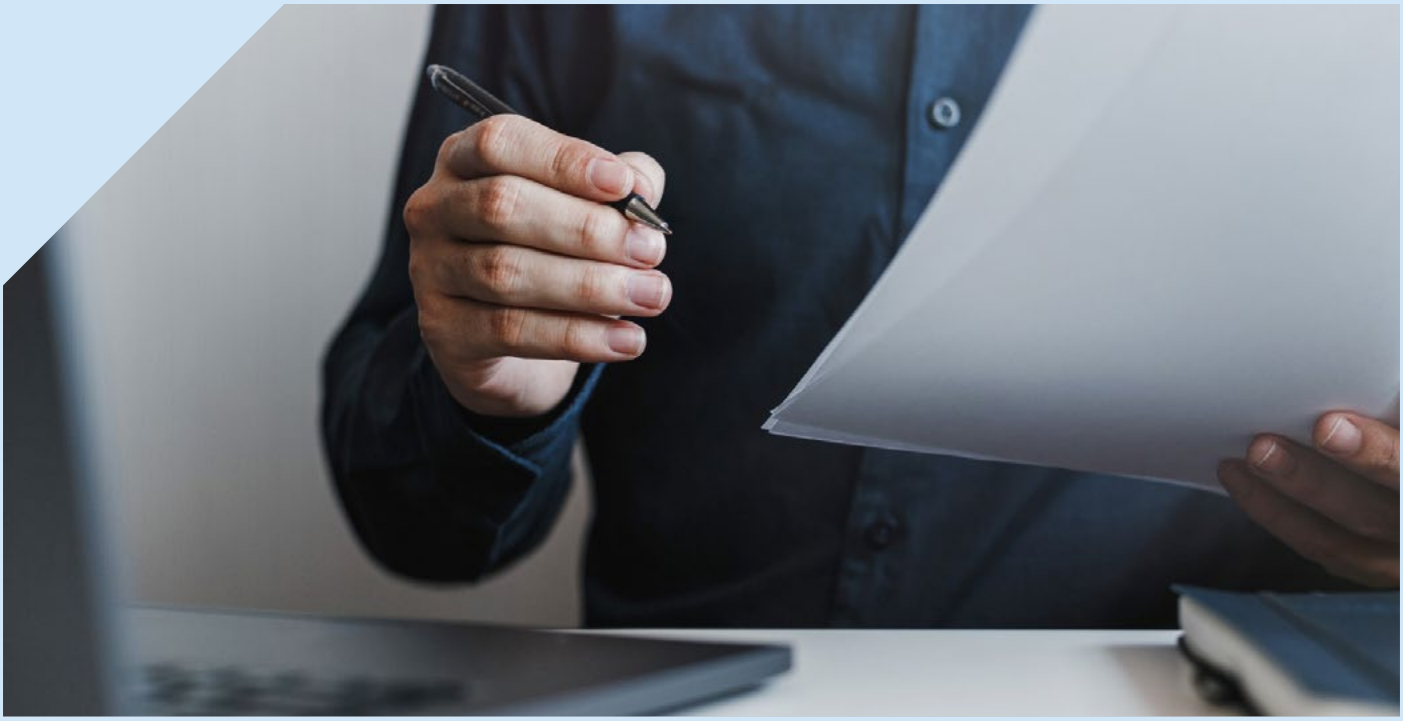
- The oil price cap has been reduced from USD 60 to USD 47.6, with a dynamic review mechanism – the cap will always be 15% lower than the average price of Urals oil over the last six months.
- Prohibition on transactions involving the "Nord Stream 1" and "Nord Stream 2" gas pipelines – no EU entity may enter into transactions involving them.
- A ban on imports of refined petroleum products made from Russian crude oil, even if they are refined in third countries.
- Restrictions on the shadow fleet – 105 more ships have been added to the list (444 in total), prohibiting them from entering EU ports and receiving services.

Expansion of the sanctions list:

The EU Council also agreed to significantly expand the list of sanctioned persons and entities, adding 14 natural persons and 41 legal entities that have contributed to actions threatening Ukraine's sovereignty and territorial integrity. The total number of sanctioned persons and entities now exceeds 2 500.

TEGOS comment: The 18th package of EU sanctions against Russia is one of the toughest yet and includes a bunch of measures to further limit Russia's ability to keep fighting Ukraine. In the context of the 18th package of sanctions, measures against Belarus have also been tightened: a catch-all provision for advanced technologies has been introduced, the list of sanctioned entities has been expanded, and the list of goods prohibited from transit through Belarus has been updated.

More information here →



Mandatory payment services licence for EMT operations

On 10 June 2025, the European Banking Authority (**EBA**) published a No Action letter (**Letter**) on the interplay between the Payment Services Directive 2 (**PSD2**) and the Markets in Crypto-Assets Regulation (**MiCAR**).

The Letter advises the EU institutions to ensure that, in the long term, EU law needs to avoid a dual authorisation for the activity of transacting electronic money tokens (**EMTs**). While the existing Payment Services Directive 2 (**PSD2**) still applies, the Letter advises national competent authorities (**NCAs**) to enforce authorisation of PSD2 for a specified subset only of crypto asset service providers (**CASPs**) that transact EMTs. This requirement will remain in force until 2 March 2026, after which certain PSD2 provisions will be deprioritised.

The Letter advises viewing the transfer of crypto assets as a payment service under PSD2 where:

- operations entail EMTs;
- the payment service is carried out on behalf of the client.

Furthermore, the custody and administration of EMTs on behalf of clients under PSD2 should be regarded as a payment service, and custodial wallets as payment accounts where the wallets allow sending and receiving EMTs to and from third parties. For these services, the Letter advises NCAs to require an authorisation under PSD2 only from 2 March 2026 onwards and, during the authorisation process, to apply streamlined procedures that make maximum use of information that legal entities provide during their CASP authorisation process.

The Letter advises not to consider as payment services under PSD2 the exchange of crypto-assets for funds and exchange of crypto-assets for other crypto-assets where exchange transactions involve EMTs, and, therefore, an PSD2 authorisation should not be required in such cases.

As a result of this recommendation, many EMT transactions will not be subject to PSD2 requirements during the intervening period. The EBA considers such an alternative to be too complex and undesirable, given the burden that dual authorisation would impose on CASPs. However, the EBA does not agree that an authorisation as a CASP under MiCAR is sufficient to address the risks that arise from EMT transactions. The success of the Payment Services Directive 1 (PSD1), PSD2 and the Electronic Money Directive over the past 15 years has shown that the stability and reliability of the retail payments market is essential for consumer protection and confidence.

TEGOS comment: As only entities holding a payment service provider licence will be allowed to provide EMT-related services defined in the Letter, CASPs wishing to provide EMT-related services should assess the need for a licence under PSD2. It should be noted that CASPs seeking a payment institution licence for EMT transactions are subject to a simplified licensing process. Alternatively, CASPs may cooperate with an already licensed payment service provider in order to avoid licensing requirements.

More information here →

FCIS continues the supervision of the VASP sector

On 10 June 2025, the Financial Crime Investigation Service (**FCIS**) issued a notice stating that it will continue the active supervision and control of the sector of custodial wallet providers and virtual currency exchange operators (**VASPs**) to ensure a more effective compliance with anti-money laundering and counter-terrorist financing (**AML/CTF**) requirements.

This decision was taken in view of the extended transitional period for obtaining a crypto-asset service provider licence.

A number of key areas will receive increased attention. In particular, the timeliness and accuracy of reporting and information. The FCIS will assess whether the VASP entities provide timely and correct reporting of all data required by law. It will also assess the effectiveness of risk management systems, i.e. whether they work in practice and not just formally.

The FCIS also highlights the importance of increased cooperation. In order to ensure AML/CTF measures, it is necessary to strengthen the dialogue between the FCIS and the actors in the VASP sector. It is therefore recommended to review and update internal controls, to assess the risks and to prepare for possible inspections in the coming months.

In addition, the FCIS informs that the annual survey conducted via the Strix AML platform has ended. Its objective was to assess the ML/TF risks of each entity. The information provided is currently being analysed, and the survey data will be used to determine the level of risk and to decide on the necessary monitoring actions.

It should be noted that some VASP entities did not submit the mandatory Strix AML questionnaire. The FCIS warns that entities that fail to submit a completed questionnaire will be considered as non-compliant and may be subject to severe sanctions, including restriction or suspension of their activities, imposition of fines, and, as a last resort, removal from the public list of VASPs.

TEGOS comment: Until the MiCA licence is granted, it is important to ensure the proper implementation of AML/CFT requirements during the transitional period, while the activities of custodial wallet providers and virtual currency exchange operators (VASPs) under the supervision of the FCIS are still ongoing. Properly designed and implemented AML/CFT practices can provide a good basis for the implementation of AML/CFT requirements after obtaining a MiCA licence.

More information here →

Changes in access to Eurosystem payment systems for non-bank payment service providers

On 2 June 2025, the Governing Council of the European Central Bank (**ECB**) adopted Decision (EU) 2025/1148 (ECB/2025/18) amending Decision (EU) 2025/222 (ECB/2025/2) on access by non-bank payment service providers (**NB PSPs**) to Eurosystem central bank operated payment systems and central bank accounts.

Main amendments:

- **Date of access to TARGET:** The possibility for NB PSPs to apply for access to TARGET is postponed until **6 October 2025** (the original date was 16 June 2025). The reasons for this postponement are the need to ensure a uniform legal framework in all euro-area Member States and to coordinate technical changes to the system.
- **Transition period:** The transition period is extended from 31 December 2025 to **31 March 2026** to enable the migration of NB PSPs currently registered as addressable business identifier code (BIC) holders or reachable parties on the Eurosystem central banks' own account in order for these NB PSPs to become full participants in TARGET. The decision to extend this period was taken in order to enable a smooth adaptation to the new requirements and to ensure a gradual phasing-out of the existing connection by certain NB PSPs for payment processing.
- **Entry into force:** The new decision entered into force on **3 June 2025**.

TEGOS comment: The extension of the deadlines will ensure a uniform legal framework across euro-area Member States and a smoother transition to direct participation of NB PSPs in TARGET.

More information here →

The Bank of Lithuania publishes new draft legislation updating the supervisory reporting requirements for the FMPs

The Bank of Lithuania has submitted for public consultation a package of draft legal acts aimed at updating the supervisory reporting framework for financial market participants (**FMPs**) and implementing the provisions of Regulations (EU) 2023/1114 (**MiCAR**) and (EU) 2023/1113 of the European Parliament and of the Council, as well as provisions of the Law of the Republic of Lithuania on Markets in Crypto-assets.

These amendments aim to ensure clear, predictable and proportionate regulation for new and existing FMPs and to allow for the effective exercise of supervisory functions. **One of the main changes is the migration of the collection and submission of supervisory reports to the REGATA system (REGulated dATA), moving away from the iAPS system used previously.**

Main changes:

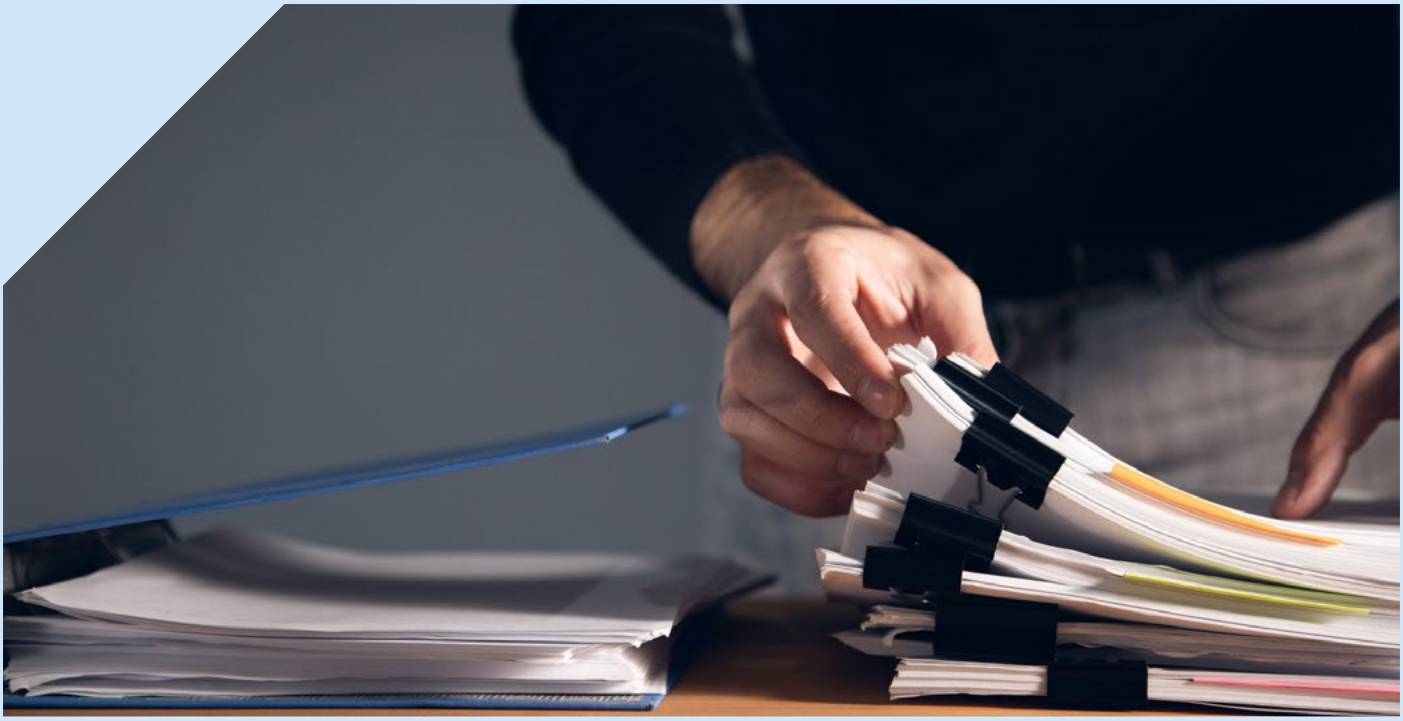
1. **Data submission through REGATA**
   - All numerical data will have to be reported **to the nearest euro or unit**, depending on their nature.
   - **Error thresholds** above which reports will need to be revised and the **procedure for submitting revised** reports are set.
2. **Simplification of supervisory reporting by payment institutions**
   - Some reports are **waived**, e.g., reports on loans, the number of employees, separate reports on complaints.
   - The **service report** will only be submitted after a change in the operation of the institution.

- Two reports on safeguarding customer funds are **merged into one** to reduce the administrative burden.
- The data on liability insurance will be provided in **Excel format according to the European Banking Authority (EBA) tool**.
- A new report on the **investment of client funds in low-risk assets** will enter into force on **1 January 2026**.

3. **New requirements for crypto-asset service providers (CASPs) and ART issuers**
   - CASPs and ART issuers will be required to provide regular **financial, capital adequacy and operational reports** covering the balance sheet, revenues, capital requirements, business volumes and information on crypto-assets.
   - Specific reporting on **cross-border public offerings** and the redemption of **asset-referenced tokens** is introduced.
4. **Additional reporting obligations for financial brokerage firms**
   - Entities providing crypto-asset services under MiCAR will be required to provide additional performance data, such as the **value of crypto-asset units in custody**, the **number of contracts in crypto-asset portfolios**, and the **volume of intermediated transactions**.
5. **Changes in anti-money laundering and counter-terrorist financing (AML/CFT) reporting**
   - A **unified reporting framework** for all supervisory entities is established.
   - The **frequency of reporting** is changed from quarterly to **semi-annually** in order to balance the relevance of information and the administrative burden.
   - **The content of reports is simplified**, introducing **uniform forms** for entities in different sectors and developing **new forms** for CASP entities.

TEGOS comment: The launch of the legislative package for public consultation is an opportune time for market participants to familiarise themselves with the planned changes in the area of supervisory reporting by financial market participants, to assess the changes that will be required for market participants in terms of collecting, processing and transferring the information into reports in their IT systems, and to assess the preparation time and resources. At the same time, this is the right time to comment on draft legislation. Overall, we consider that the planned changes should bring more clarity to regular reporting, simplify reporting by standardising on a single standard for different market participants (in the case of AML/CFT reporting) and reduce the frequency of reporting for some reports (in the case of AML/CFT reporting).

More information here →



The Bank of Lithuania submits changes to the requirements for audit committees for coordination

The Bank of Lithuania has prepared a draft amendment to Resolution No. 03-14 of the Board of the Bank of Lithuania of 24 January 2017 “On Approval of the Description of the Requirements for Audit Committees” and submitted it for coordination **from 19 June 2025 to 5 July 2025**.

The draft amendment has been prepared in accordance with the amendments to the Law of the Republic of Lithuania on Audit of Financial Statements and Other Assurance Services, which transposes Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting into national law.

The draft amendment to the Resolution prepared by the Bank of Lithuania provides for additional duties of audit committees related to the oversight of the sustainability reporting process. In particular, the new provisions will require an audit committee when monitoring and evaluating the sustainability reporting process:

- to **make recommendations to the supervisory body** (or, in the absence of a supervisory body, to the general meeting of shareholders) on the selection, appointment, re-appointment and removal of an independent assurance provider (e.g., an auditor or other service provider), as well as on the terms and conditions of the contract with such a provider, including the selection criteria and the assessment of the qualification and experience of independent assurance providers;
- to **request information** from the independent assurance provider on its internal quality control procedures and carry out an assessment of that information;

- to **ensure independence oversight** by monitoring whether the independent assurance provider has in fact complied with the principles of independence and objectivity;
- to **assess the effectiveness of the sustainability reporting process** by checking that the resources offered are sufficient for the scale of the tasks and that the team carrying out the tasks has the necessary knowledge, skills and experience to perform adequately the tasks set out in the assurance contract;
- to **discuss with the independent assurance provider** the sustainability reporting assurance conclusion to be provided, and analyse difficulties encountered during the assurance process and significant disagreements with members of the governing bodies or senior management.

In addition to these duties, the draft also clarifies the requirements for the accountability of the audit committee and the approval of the regulations of the internal audit service in line with the corporate governance principles of the Organisation for Economic Co-operation and Development (OECD).

TEGOS comment: Although the entry into force of the "sustainability reporting" obligation under Directive (EU) 2022/2464 was delayed by two years by the adoption of the so-called "Stop the Clock" Directive by the European authorities (the provisions of which were transposed into Lithuanian law on 25 June, when the Parliament approved amendments to the Law on Reporting by Enterprises and Groups of Enterprises and the Law on Securities), however, the obligation is a short time away from coming into force and companies should start preparing for the implementation of the obligation from now on, especially given that the "Stop the Clock" Directive itself has been adopted to allow companies to prepare for sustainability reporting in a more meaningful and effective way. Therefore, the draft resolution of the Bank of Lithuania is a good opportunity for companies to start assessing the effectiveness of their internal audit processes to ensure sustainability reporting.

It is worth noting that, like the provisions of Directive (EU) 2022/2464, the Bank of Lithuania's resolution applies only to public-interest entities (including collective investment undertakings).

The new resolution has not yet been adopted following the consultation period.

More information here →

The Parliament approves amendments to the AML/CFT Law: facilitations and changes for financial institutions envisaged

On 25 June 2025, the Parliament adopted amendments to the Law on the Prevention of Money Laundering and Terrorist Financing (**AML/CFT Law**).

Key amendments:

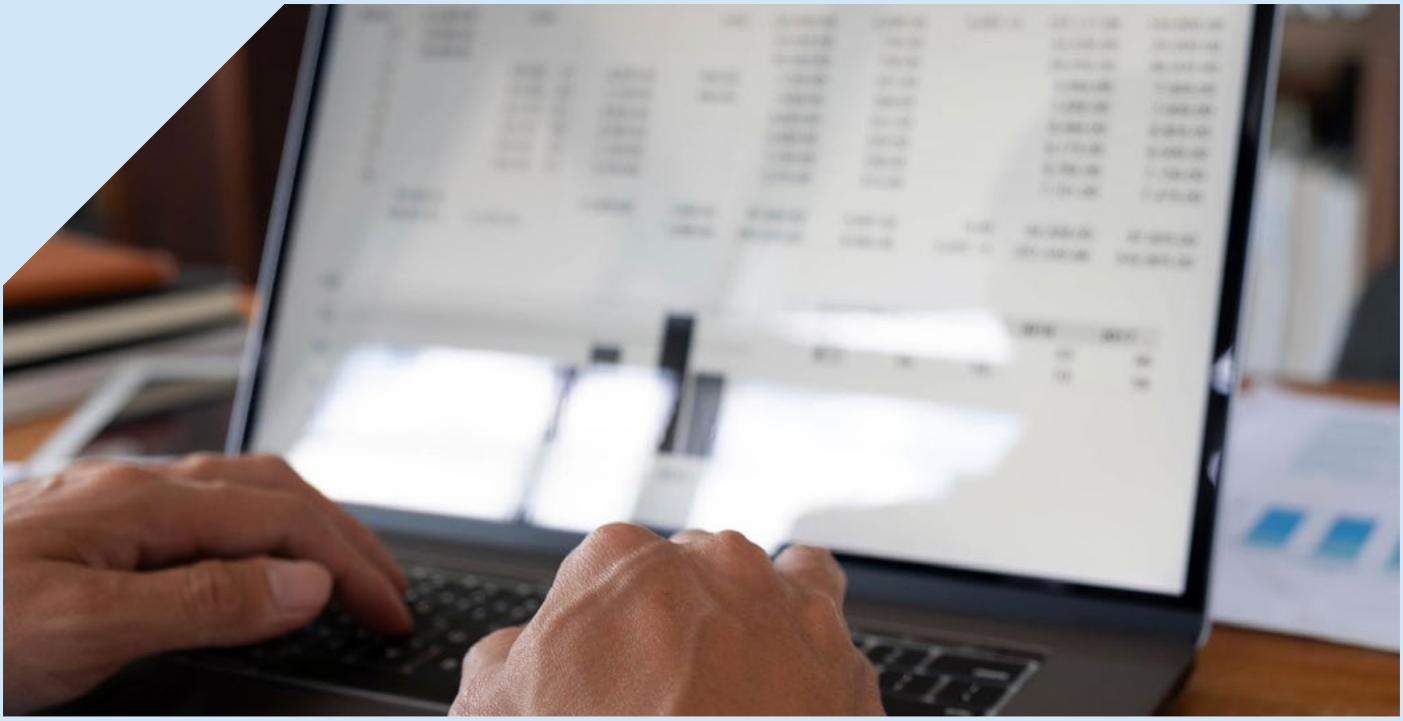
- The new wording provides that **powers of attorney issued in EU Member States will be recognised without the need for legalisation or apostille**. This exemption will not apply to powers of attorney issued in third countries; the former will remain subject to the document authentication requirement.
- An additional **data collection channel**, allowing information on clients and beneficiaries to be obtained not only from **public registers or information systems** but also from other **reliable and independent data sources**, in particular where official registers do not keep the relevant data, is established.
- The previous imperative to **request documents and other data** is abandoned in favour of an obligation to take **reasonable measures**. This concept implies that financial institutions and other obliged entities are required to ensure that they have a sufficient understanding of the control and ownership structure and the nature of the activities of the client, which is a legal person, but that they are free to choose the most appropriate sources of information and forms of assessment in the light of their individual situation and risk profile.

- The amendments substantially revise the procedure of application of **simplified due diligence (SDD)**. Instead of the previous list of closed conditions, there is an obligation to **assess risks according to lower risk factors**, which is now considered to be a non-exhaustive list. In addition, the **EUR 1,000 threshold**, which used to apply in case of electronic money, has been removed.
- From now on, certain financial institutions identified in accordance with Article 77 of Regulation (EU) 2024/1620 will have to pay an **annual supervisory fee** to the European Anti-Money Laundering and Countering the Financing of Terrorism Authority (AMLA).

The amendments entered into force on 1 July 2025.

TEGOS comment: Taking into account the adopted amendments, relevant financial market participants should review and update their internal policies and procedures on money laundering and terrorist financing prevention measures, insofar as they relate to simplified identity verification and the submission of powers of attorney with an apostille.

More information here →



From October, legally binding pre-transfer verification of payee details

On 26 June 2025, the Bank of Lithuania issued a press release informing about a new measure to combat payment fraud–**verification of the payee's account and name prior to the transfer**. This measure will apply from **9 October 2025** throughout the euro area, implementing the requirements of European legislation.

Material changes:

- **Before executing a SEPA or instant payment in euro**, payment service providers (banks, credit unions, payment and electronic money institutions) will be obliged to verify that the **name of the payee** in the payment order corresponds to that of the **owner of the specified IBAN account**.
- **The verification results will be provided to the payer in real time** before the payment is confirmed.
- The **decision to execute the payment will be taken solely by the payer** based on the eligibility information provided. Verification results may be as follows:
  - the name of the payee fully corresponds;
  - the name of the payee almost corresponds (indicate the proposed correction);
  - the name of the payee does not correspond (significant discrepancy, e.g., the account belongs to a different person than the one indicated in the payment order);
  - the verification failed.

Legal liability:

- If the payer still confirms the payment after receiving a notification of a non-compliant payee, **the payer shall be held liable for the incorrect transfer of funds**.
- **In the event that the verification service is not properly provided** and the funds are transferred to the wrong payee, **the liability will be borne by the payment service provider**, who will be obliged to refund the transferred amount.

Important:

- The verification function will only be available at the time of payment initiation in the bank's or other institution's system (e.g., via online banking or mobile app).
- Banks or other payment service providers **will never send emails or SMS messages with active links** asking you to verify the payee's details, which may constitute fraudulent attempts.

TEGOS comment: In order to properly implement the mandatory pre-transfer verification of payee data from 9 October 2025, financial market participants need to prepare their IT systems and processes for the implementation of such verification and for informing the customer about the results of the verification, and to tailor their communication messages to customers accordingly. It is important to remember that if the verification service is not properly provided and the funds are transferred to the wrong payee, the liability will be borne by the payment service provider, who will be obliged to refund the transferred amount. We believe that the application of this additional measure will be an effective anti-fraud measure to reduce the losses suffered by customers and financial market participants as a result of fraud.

More information here →

If you have any questions, the TEGOS BANKING AND FINANCE TEAM is ready to help you

Žygimantas Stankevičius
Partner
zygimantas.stankevicius@tegos.legal
+370 5 251 4444

Lina Mileškevičienė
Chief Expert
lina.mileskveviciene@tegos.legal
+370 5 251 4444

Evelina Tumakova - Kuzmič
Associate Partner
evelina.tumakova@ tegos.legal
+370 5 251 4444

Rasa Blinstrubienė
Associate Partner
rasa.blinstrubiene@tegos.legal
+370 5 251 4444

Paulius Liškauskas
Associate
paulius.liskauskas@tegos.legal
+370 5 251 4444

Samanta Sluoksnaitytė
Legal Assistant
samanta.sluoksnaityte@tegos.legal
+370 5 251 4444

Enrika Gudzevičiūtė
Legal Assistant
enrika.gudzeviciute@tegos.legal
+370 5 251 4444