REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

10.2024

The Bank of Lithuania ML/TF analysis

LINK

The Bank of Lithuania (BoL) conducted an analysis of money laundering and terrorist financing (ML/TF) risks faced by electronic money and payment institutions (EMIs) based on data from January to December 2023. The Bank of Lithuania has issued an official reminder regarding the guidelines on Anti-Money Laundering (AML), fraud prevention, sanctions compliance, and internal controls applicable to financial market participants. Key considerations include:

- Implementation of international sanctions and restrictive measures. Transaction monitoring rules should undergo regular review and testing to maintain effectiveness.
- Strengthening the internal control system regarding ML/TF.
- Fraud prevention - investment scams remain the most prevalent type of fraud within the financial market; thus, financial institutions are encouraged to assess customers for potential connections to fictitious or unlicensed investment platforms.
- Managing the risk of conflict of interest and treatment of related parties. The risk of conflicts of interest is elevated by inadequate separation of duties among employees within financial institutions.
- Periodic training programs should incorporate updated and relevant money laundering (ML) and terrorist financing (TF) typologies.
- Insufficient information-sharing mechanisms increase the risk that management may be inadequately informed about current ML/TF risks.

The Bank of Lithuania analysis

LINK

The BoL conducted an analysis which showed that the customer base of electronic money and payment institutions (EMIs) registered in Lithuania predominantly consists of individuals from the European Economic Area (EEA). However, an interesting trend emerges regarding the average payment transaction values: customers from target territories and third countries exhibit significantly higher average transaction values compared to their EEA counterparts.

Our recommendations:

- Comprehensive Risk Assessment:

Financial institutions should conduct thorough risk assessments to identify potential vulnerabilities related to money laundering, terrorist financing, and fraud. This includes evaluating both geographical and business risks associated with their client base.

- Enhanced Due Diligence (EDD):

For clients categorized as high-risk due to increased geographical or business risks, institutions must implement enhanced due diligence measures. This may include more rigorous customer verification processes, ongoing monitoring of transactions, and detailed scrutiny of client backgrounds.

- Training and Awareness:

Regular training programs should be established to ensure that staff are well-informed about the latest regulatory requirements and best practices in risk management. This will enhance the institution's ability to detect and prevent financial crime effectively.

Financial Crimes Investigation Service under the Ministry of the Interior of the Republic of Lithuania

LINK

Summary of the 3rd National Money Laundering and Terrorist Financing Risk Assessment performed by the FICIS. The latest assessment has identified various business sectors with significant risks related to money laundering (ML) and terrorist financing (TF). Notably, the following findings emerged:

1. Very High Risk Sectors:

• Virtual Currency Exchanges and Depository Virtual Currency Wallet Operators (VCSOs): This sector has been assigned a very high ML risk score, indicating a pressing need for heightened supervisory scrutiny.

• Electronic Money Institutions and Payment Institutions: This sector also received a very high risk score, necessitating substantial oversight to mitigate potential vulnerabilities.

2. High Risk Sectors:

• Real Estate: This sector is rated as high risk, warranting careful monitoring and regulatory attention.

• Money Remittance Services: Identified as a high-risk area, this sector requires vigilant oversight to combat potential ML and TF activities.

• Accountants, Auditors, and Tax Consultants: These professions are also classified as high risk, underscoring the need for enhanced regulatory measures.

Detailed and full Regulatory Compliance report on AML/CTF regulation can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

EMI, PI REGULATION

10.2024

ECOVIS ProventusLaw

Events organised by the Bank of Lithuania

1. The Investment Services and Companies Supervision Division of the Bank of Lithuania's Financial Market Supervision Department is organizing a consultation event, "Crowdfunding – One Year of EU Regulation," on November 27, 2024, at 10:00 A.M.

2. The Financial Market Supervision Department of the Bank of Lithuania will hold a consultation event titled "Current Issues in Payment Services" on November 28, 2024, at 10:00 A.M.

Guidelines published by EBA

LINK LINK

The Bank of Lithuania will follow the European Banking Authority's (EBA) Guidelines on the resubmission of historical data under the EBA reporting framework (EBA/GL/2024/04) when supervising the financial market.

Financial sector entities reporting under the EBA's Supervision and Resolution Reporting Framework (e.g. credit and payment institutions, brokerage firms) should comply with the requirements of the Guidelines and follow them. The Guidelines apply from 17 October 2024.

The Guidelines set out the requirements for financial sector entities to resubmit to a supervisory or resolution authority data from previous periods if they contain mistakes, inaccuracies or changes. It also sets out the specific circumstances in which it is not necessary to correct historical data.

Contribution rates of supervised financial market participants in 2025

LINK LINK

The Board of the Bank of Lithuania approved Resolution dated on 14th of October 2024 No 03-115 On approval of the contribution rates of supervised financial market participants in 2025. This Resolution, along with Resolution of the Bank of Lithuania No 03-73 On the approval of the description of the methodology for calculating the contributions of supervised financial market participants and the payment procedure, set the rates of the contributions for financial market participants, as well sets deadlines and procedure of payment of such contributions.

Electronic money institutions

Their contribution base is income related to the issuance of electronic money and/or the provision of payment services of the previous calendar year. Rate of contributions in 2025 is 0.65 percent, counting from the contribution base. Maximum contribution is set to be 0.65 percent, counting form the contribution base.

Payment institutions

Their contribution base is income related to the provision of payment services of the previous calendar year. Rate of contributions in 2025 is 0,65 percent counting from the contribution base. Maximum contribution is set to be 0.65 percent, counting form the contribution base.

Publication by the Bank of Lithuania

LINK

The Bank of Lithuania aims to update the financial market supervision policy and supplement it in the light of the recommendations of the European Union and international institutions, the strategic objectives of the Bank of Lithuania, the results of the surveys of financial market participants and the supervisory practice, and to emphasise the important principles of financial market supervision, which are expected to contribute to greater clarity, better dialogue, a more reliable financial market and better value for consumers. The draft is available here.

Publication by the Bank of Lithuania

LINK

In the first half of this year, the Bank of Lithuania received 521 complaints—almost half as many (-44%) compared to the same period last year. This change was mainly driven by a significant reduction in the number of complaints about payment services.

Detailed and full Regulatory Compliance Report on EMI, PI regulation can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

PERSONAL DATA PROTECTION AND ICT REGULATION

10.2024

ECOVIS ProventusLaw

Our New DORA Compliance Tool

Our firm has developed a comprehensive DORA (Digital Operational Resilience Act) compliance tool designed to assist organizations in evaluating and ensuring their alignment with DORA's regulatory requirements. This tool provides organizations with a checklist, covering all key aspects mandated under DORA, to help simplify compliance tracking and maintain a resilient digital operational environment.

What the DORA Compliance Tool Offers:
The tool guides users through critical areas, including governance and organization, ICT risk management, system protection, response and recovery plans, and third-party risk management. Each section of the checklist contains targeted questions that correspond to specific articles of DORA. Book a call to request an access to our DORA self-assessment compliance tool (book a call).

Updated Law on Cyber Security of the Republic of Lithuania implementing NIS2 Directive came into force

LINK

The updated Republic of Lithuania Law on Cybersecurity (the "Cybersecurity Law") entered into force on 18 October 2024.

The Cybersecurity Law implements the following European Union legislation:

- NIS Directive 2;
- The Cybersecurity Act;
- Regulation of the European Parliament and the Council establishing a European Centre of Excellence for Cyber Security Industry, Technology and Research and a Network of National Coordination Centres.

The provisions of the NIS2 Directive implemented in the Cybersecurity Act will strengthen the cybersecurity governance model in Lithuania.

CJEU Ruling on Legitimate Interest Basis for Commercial Purposes

LINK

The Court of Justice of the European Union (CJEU) addressed the extent to which organizations can rely on the "legitimate interest" basis under the GDPR when processing personal data for commercial purposes, such as marketing, without user consent. The CJEU clarified that a controller's commercial interest may be regarded as necessary for the purposes of the legitimate interests pursued by that controller.
The CJEU recalled the three-prong criteria it has set for determining whether a processing can be justified under Article 6(1)(f) of the GDPR. The CJEU outlined three conditions for determining this:

- Pursuit of a lawful, legitimate interest by the data controller or third party.
- Necessity of data processing for this interest.
- Ensuring the interest isn't outweighed by data subjects' rights.

Belgian DPA fines company €45,000 for GDPR violations in employment context

LINK

Belgium DPA issued 40k EUR daily fine on Belgian company until it rectified having:

(1) failed to display both an 'accept all' and a 'reject all' button on the first layer of its cookie banner.
(2) used misleading colors in its cookie banner, directing users towards the choice of consenting to cookies by highlighting the 'accept all' button.

Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

LINK

On 8 October 2024, the European Data Protection Board ("EDPB") issued draft Guidelines 1/2024 concerning the processing of personal data based on legitimate interests under Article 6(1)(f) of the GDPR ("Guidance"). The public consultation on the Guidance will run until 20 November 2024.
Article 6(1)(f) allows for data processing when it serves the legitimate interests of the controller or a third party, provided that these interests are not overridden by the data subject's interests, rights and freedoms. The Guidance provides valuable interpretative indications which will help organisations navigate this fundamental and yet complex aspect of data protection law while supporting their data strategies.

Detailed and full Regulatory Compliance update on PERSONAL DATA PROTECTION and ICT Regulation can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

FINANCIAL AND ECONOMIC SANCTIONS 10.2024

ECOVIS ProventusLaw

Guidance by the European Commission

LINK

The European Commission has issued updated guidance for industry to address the prevention of Russian export control and sanctions evasion. This guidance is designed to aid industry in identifying Russian evasion tactics, safeguarding G7 technology from unauthorized appropriation, minimizing reputational risk, and mitigating liability exposure, all while reinforcing the effectiveness of existing export controls and sanctions.
In early 2023, the G7 introduced the Enforcement Coordination Mechanism (ECM) to promote compliance with these regulatory measures.
By September 2023, the ECM had further established a Sub-Working Group on Export Control Enforcement to facilitate enhanced information-sharing and to develop best practices for detecting and preventing export violations.

This guidance document offers support to industries through:

1. A comprehensive list of items at high risk of diversion to Russia.
2. Updated indicators signaling potential evasion of export controls and sanctions.
3. Best practices for identifying and managing these risks.
4. Screening tools and resources to support robust due diligence processes.

The Financial Crimes Investigation Service Guidelines

LINK LINK

The Financial Crimes Investigation Service (FCIS) has issued updated guidelines detailing obligations for Lithuanian entities regarding international sanctions compliance, specifically under the UNSCR 1373 framework.

Obliged entities must verify entities for Financial Sanction Checks against:

- EU international financial sanctions lists,
- UN Security Council resolutions on targeted sanctions, and
- The UNSCR 1373 list managed by FCIS.

All assets — including funds, financial assets, property, and economic resources — belonging to persons or entities on the UNSCR 1373 list must be frozen immediately upon identification.

Reporting Requirements:
If funds or other financial assets are frozen under these sanctions, entities must notify FCIS within 2 working days.

Lithuania's AML Center conducts training on sectoral sanctions compliance.

LINK

Lithuania's AML Center recently conducted a comprehensive training session on sectoral sanctions compliance, focusing on the nuances and implications of sanctions, particularly those affecting the Russian and Belarusian markets. The session provided insights into Lithuania's implementation of these sanctions, best practices for compliance, and the red flags that financial institutions should look for when identifying potential sanctions evasion.
Participants explored the regulatory landscape, compliance requirements, and tools essential to managing sectoral sanctions risk. Through case studies and interactive discussions, the AML Center's speakers emphasized the importance of proactive risk management to ensure that financial institutions are well prepared to navigate and comply with Lithuania's stringent sanctions measures.

Detailed and full Regulatory Compliance report on Financial and Economic Sanctions can be found here:

Our recommendations and details are in this file

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

CONSUMER PROTECTION

10.2024

European Banking Authority (EBA)

LINK

Consumer Protection Day in Budapest

The European Supervisory Authorities (ESAs) held their 11th annual Consumer Protection Day in Budapest, focusing on “Empowering EU consumers: fair access to the future of financial services.”
Key topics included the use of artificial intelligence (AI) in financial services, improving access to consumer-centric products, and promoting sustainable finance. Panel discussions emphasized both the opportunities and risks of AI, the need for improved financial literacy, and the simplification of sustainable finance disclosures for retail investors. Industry participants urged regulators to issue clearer guidance for compliance with the upcoming EU AI Act.

Our recommendation:
Organizations need to enhance their product design and disclosure practices to be more consumer-centric, with particular attention to vulnerable customers and complex products.
Companies should conduct gap analyses of their current practices against expected regulatory requirements and establish dedicated governance committees to oversee AI implementation and compliance.

BEUC news feed

LINK

OECD Consumer Policy Ministerial Meeting

At the first OECD Consumer Policy Ministerial Meeting, a landmark Declaration was adopted, emphasizing the need for stronger consumer protections in the context of the digital and green transitions.
The Declaration focuses on three critical areas: tackling harms in digital markets, addressing misleading environmental claims, and improving product safety in global trade. BEUC Director General Agustín Reyna highlighted the importance of collaboration between authorities and consumer organizations to ensure consumer safety and trust. The Declaration aims to empower consumers against manipulative digital practices, enforce clear environmental labelling, and hold online marketplaces accountable for unsafe products.

Our recommendation:
Digital businesses should review and strengthen their consumer protection frameworks, particularly focusing on transparent practices and eliminating potentially manipulative design patterns in their digital interfaces and marketing strategies. Companies must ensure their environmental claims are verifiable, specific, and backed by clear evidence, while implementing robust documentation systems to support any green marketing statements.

State Consumer Rights Protection Authority (Lithuania)

LINK

Amendments to the Law on the Protection of Consumer Rights

An amendment to Article 40 of the Law on the Protection of Consumer Rights enters into force on 1 November to ensure more transparent information to consumers about the assignment and management of their debts. The law regulates the specificities of out-of-court recovery of debts arising from consumer contracts and establishes liability for non-compliance with the requirements.

Our recommendation:

Companies managing consumer debts should immediately review and update their information-sharing practices to ensure compliance with the new requirements. Transparent communication and robust internal procedures will not only align with the law but also foster trust with consumers by respecting their rights throughout the debt management process.

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

10.2024

ECOVIS ProventusLaw

Labour Code Amendments

On 17 October The Seimas has approved amendments to the Labor Code that will enter into force on 1 January 2025. Below is an overview of the main changes.

1. The minimum monthly wage will increase by 1,038 euros starting from 1 January 2025.
2. Recently the amendments to the Labour Code were approved that will enter into force on 1 January 2025.

- **Termination of employment during the trial period**

The employee can submit a request for termination of employment before the end of the probationary period, **but this notice may be withdrawn no later than the working day following the day on which it is submitted.**

- **Regarding overtime work**

The employer may only assign overtime work with the employee's written consent, except in the following exceptional cases.
Overtime work shall be paid at the rate of not less than one and a half times the employee's salary.
Overtime work on a rest day that is not scheduled or overtime work at night shall be paid at least twice the employee's salary, and overtime work on a public holiday and/or overtime work on a public holiday at night shall be paid at least two and a half times the employee's salary.

- **Regarding work on the day before a public holiday**

On the day before a public holiday, the working day shall be shortened by 1 hour, except for employees working on a reduced-hours basis. If, due to the specificities of the organisation of work or the uninterrupted activity of the employer, it is not possible to shorten the working day for the employee, he/she will have to be paid for this hour as overtime work.

- **Regarding liability for breach of the prohibition of violence or harassment**

The definition of violence or harassment has been clarified by stating that unacceptable behaviour is defined as inappropriate behavior by the employer and other employees.

- **On the re-election of the Labour Council**

The deadline for the election of a Labour Council that has not been held is clarified; new elections of the Labour Council must be held 6 months after the Electoral Commission's decision to declare the election of the Labour Council as not having been held.

- **Concerning the terms of the non-interruptible 2-month parental leave**

Clarification of the 62 calendar days as part of the non-interruptible 2-month period of parental leave.

LINK

Our recommendation:

To prepare for the 2025 changes to the Labor Code, we recommend:

- **Policy Updates:** Review and update all employment policies to ensure alignment with the new requirements regarding wages, overtime, and worker protections.
- **Employee Education:** Train employees on their rights and inform them about the changes, while also preparing management to comply with updated harassment and safety protocols.

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

CRYPTO

10.2024

ESMA launches survey on legal entities identifiers

LINK

On October 18, 2024, the European Securities and Markets Authority (ESMA) initiated a survey to assess the potential impacts of incorporating alternative identifiers to the Legal Entity Identifier (LEI) in reporting and record-keeping requirements. This initiative seeks feedback from financial market participants, including Crypto Asset Service Providers (CASPs), to evaluate the implications of such alternatives in current and future regulatory frameworks.

Our recommendation:

CASPs should participate in ESMA's survey to provide insights on the adoption of alternative identifiers, ensuring that forthcoming regulations under the Markets in Crypto-Assets (MiCA) framework are both effective and practical.

ESMA Advocates Cybersecurity Audits in MiCA Authorisation Standards

LINK

On October 11, 2024, ESMA responded to the European Commission's adjustments to the Regulatory Technical Standards (RTS) for crypto-asset service providers (CASPs) under MiCA. These standards outline authorization and notification procedures critical for CASPs' operations. ESMA voiced concerns over the removal of third-party cybersecurity audits, emphasizing their importance for market stability and investor safety. The authority urged the Commission to reinstate this audit requirement to ensure robust cybersecurity for CASPs.

ESMA Proposes ESG Disclosure Standards for Crypto-Asset Securities

LINK

In its October 28, 2024, consultation paper, the European Securities and Markets Authority (ESMA) recommends enhanced disclosure requirements for non-equity securities, including crypto-assets, that are marketed as incorporating Environmental, Social, and Governance (ESG) factors. These proposals aim to align with the Markets in Crypto-Assets (MiCA) Regulation, ensuring that investors receive comprehensive information on ESG-related claims associated with crypto-assets.

Our recommendation:

Crypto issuers with ESG claims should closely follow ESMA's consultation outcomes and be ready to adapt their disclosures, aligning with MiCA's future standards for transparency and investor protection.

ESAs Finalize Rules for European Single Access Point (ESAP)

LINK

On October 29, 2024, the European Supervisory Authorities (ESAs) published the final implementing technical standards for the European Single Access Point (ESAP). ESAP aims to centralize access to public financial and sustainability information across the EU, enhancing transparency and data availability. The platform is scheduled to begin collecting information in July 2026, with public access commencing by July 2027.

Our recommendation:

Crypto-asset service providers should prepare to integrate their financial and sustainability disclosures with ESAP, ensuring compliance with forthcoming transparency requirements under the Markets in Crypto-Assets (MiCA) regulation.

Bank of Lithuania Calls for quality applications from Crypto-asset Service Providers

LINK

On October 31, 2024, Bank of Lithuania announced its readiness to license crypto-asset service providers (CASPs) under the Markets in Crypto-Assets (MiCA) regulation. With over 300 CASPs operating in Lithuania, the bank emphasized the need for applicants to thoroughly understand legal requirements and meet high operational standards. Key focus areas include the integrity of shareholders and management, financial transparency, and robust risk management. Bank of Lithuania encourages current CASPs to assess their compliance with MiCA and submit applications from December 30, 2024.

Detailed and full Regulatory Compliance report on Crypto Regulation can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

EU WHISTLEBLOWING DIRECTIVE

ECOVIS ProventusLaw

Whistleblowing Directive Implementation

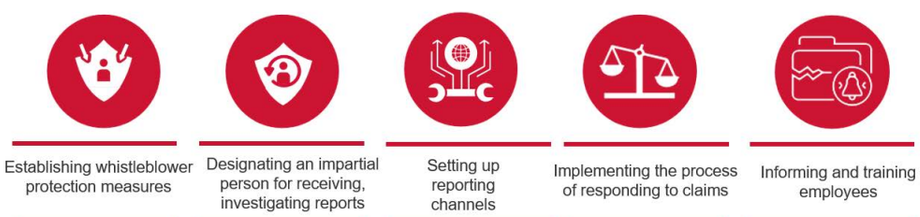
LINK

The EU Whistleblower Directive is mandatory for all organisations with more than 50 employees. **For financial institutions this legislation is mandatory regardless of number of employees** and is designed to protect individuals who report breaches of EU law. It establishes minimum standards for reporting mechanisms and safeguards against retaliation for whistleblowers across the European Union, thereby bolstering Environmental, Social, and Governance (ESG) principles. This directive underscores transparency, accountability, and responsible conduct, aligning with broader ESG objectives to promote sustainable and ethical business practices across the European Union and beyond.

This Directive introduces several key provisions, including:

1. Scope: The directive covers many areas where EU law applies, including public procurement, financial services, product safety, environmental protection, public health, consumer protection, and more.
2. Reporting Channels: Member states and certain private entities must establish secure and confidential reporting channels for whistleblowers. These channels must be easily accessible and capable of handling reports effectively.
3. Protections: The directive prohibits retaliation against whistleblowers, including dismissal, demotion, harassment, and discrimination. It also requires member states to provide effective remedies for whistleblowers who experience retaliation.
4. Confidentiality: Whistleblowers' identities must be kept confidential throughout the reporting process unless disclosure is necessary for investigation or legal proceedings.
5. Follow-Up: Once a report is submitted, the relevant authorities or organisations must acknowledge receipt and provide feedback to the whistleblower within a reasonable timeframe.

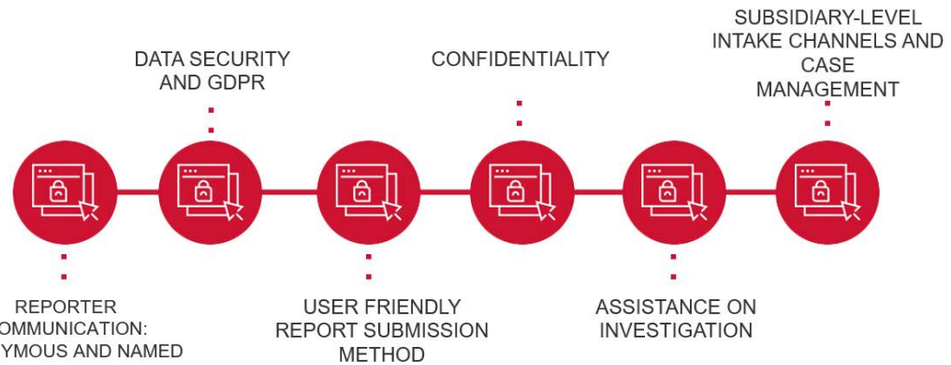
Under the EU Whistleblower Directive, organisations must establish secure and confidential reporting channels for whistleblowers. The reporting process is designed to ensure the protection of whistleblowers and the effective handling of reports of wrongdoing.



WHISTLEBLOWING SOLUTION BY ECOVIS
Outsourcing solution for companies

LINK

Ecovis provides a whistleblowing system as an outsourced channel for companies, ensuring compliance with the EU Whistleblower Directive. Our service offers a convenient solution, as we provide secure and confidential reporting channels that meet the directive's standards. By entrusting the handling of whistleblower reports to us, companies can streamline the reporting process, enhance transparency, and mitigate the risk of internal bias or conflict of interest. This allows organisations to focus on their core activities while effectively managing whistleblowing cases.



Discover how Ecovis Whistleblowing's outsourced system ensures confidentiality and data security in accordance with directive standards while offering two flexible options for companies:

Option 1: Utilize our system solely as a reporting channel, receiving all reports directly without our involvement in the initial investigation process.
Option 2: Entrust us to handle the investigation process as well.

Whether companies require a reporting channel only or a comprehensive investigative service, Ecovis Whistleblowing provides a reliable solution tailored to their needs, fostering transparency and compliance with the EU Whistleblower Directive. Contact us at vilnius@ecovis.lt, and we will ensure compliance with the Whistleblowing Directive tailored to your specific situation and available resources.