# REGULATORY COMPLIANCE UPDATE

## AML/CTF REGULATION

11.2024

### The Bank of Lithuania

LINK

Encouraged by the Bank of Lithuania, banks have significantly improved the customer experience in implementing anti-money laundering measures. Four commercial banks operating in Lithuania have improved their customer experience in implementing AML measures in 2023. The measures and actions taken by these banks to improve the customer experience were based on an agreement reached with the Bank of Lithuania at the beginning of 2023, which had identified a number of uncertainties in the AML requirements for consumers.

**Key Improvements in customer experience:**

- Customers can update their cognitive questionnaires based on previously submitted versions, with necessary adjustments, additions, and validation, eliminating the need to complete the form from scratch.
- Explanations are provided for the customer insight questionnaire, or the questionnaires are tailored to different user groups by removing irrelevant questions.
- Customers are informed of the option to negotiate an extended deadline for submitting requested information or to request a reasonable extension if needed.
- Banks aim to obtain as much information as possible from public systems and registers, reducing the burden on customers to provide such data themselves.

### The Financial Conduct Authority (FCA)

LINK

The UK's Financial Conduct Authority (FCA) has fined Metro Bank PLC £16,675,200 for failing to properly monitor over 60 million transactions, valued at over £51 billion, for potential money laundering between June 2016 and December 2020. The bank's automated transaction monitoring system, implemented in June 2016, did not function as expected due to an error in data feeding, resulting in transactions on the day an account was opened and subsequent transactions until account records were being overlooked. Despite concerns raised by junior staff in 2017 and 2018, the issue was not identified or resolved until July 2019. Even after this fix, Metro lacked consistent mechanisms to ensure proper transaction monitoring until December 2020.

### Anti-Money Laundering Competence Centre

LINK

Financial fraud attacks have grown increasingly effectively, with the AML Competence Centre reporting nearly €5 million in real losses to the public during the third quarter of 2024. Analysis of fraud incidents from July to September revealed that fraudsters continue to rely on familiar tactics, notably telephone scams, investment fraud, and email interception schemes. Attempts to defraud individuals and businesses totaled €8.9 million, but actual losses amounted to €4.8 million. Financial institutions successfully protected 42% of the funds targeted by fraudsters.

### The Bank of Lithuania

LINK

Lithuanian e-money and payment institutions will gain access to Eurosystem and EU payment systems starting April 2025. Simultaneously, the EU's Markets in Crypto-Assets Regulation (MiCA) will come into effect, requiring cryptocurrency service providers to become licensed financial market participants or cease operations. Currently, such providers are not licensed in Lithuania but are subject to limited oversight by the Financial Crime Investigation Service (FNTT).

The National Money Laundering and Terrorist Financing Risk Assessment Report (2019–2022) identifies cryptocurrency and e-money/payment institutions as high-risk for money laundering and terrorist financing. Efforts to strengthen AML/CFT frameworks, including enhanced compliance and capital requirements (minimum equity of EUR 125,000), have resulted in the deregistration of 300 non-compliant entities in Lithuania.

***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

11.2024

### Supreme Court of Lithuania (SCL) decision

LINK

The Supreme Court of Lithuania reviewed a case concerning the right of a bank to unilaterally terminate a bank account agreement with a client, setting out clear guidelines on the lawful and proportionate grounds for such actions. The SCL concluded that a bank can only terminate an agreement under two conditions:

- when the grounds for termination are explicitly listed in the agreement.
- when significant reasons exist, even if not outlined in the agreement, such as when client activities pose a genuine risk of money laundering or terrorist financing. However, the bank must demonstrate that terminating the agreement is necessary and proportionate to manage the identified risk.

The SCL also emphasized that banks must inform clients about the reasons for termination with sufficient detail and adhere to legal provisions restricting the disclosure of information related to preventive measures (Article 23(1) of the Law on the Prevention of Money Laundering and Terrorist Financing).

The decision reinforced the need for payment service providers to substantiate their actions, avoid formalism, and operate with due caution. The ruling also set a precedent for protecting client rights while ensuring that financial institutions operate transparently and proportionately.

### The Bank of Lithuania decision

LINK LINK LINK

The Bank of Lithuania has submitted a draft amendment to Resolution No. 247 of the Board of the Bank of Lithuania on the requirements for electronic money and payment institutions concerning internal control, risk management, and protection of received funds. The main changes proposed in the draft resolution are related to stronger governance and risk culture, enhanced internal control systems, client funds protection, requirements for wind down plan.
The deadline for submitting comments and proposals to the draft Resolution is December 13 via TAIS system or email prieziura@lb.lt

### The Bank of Lithuania organized a seminar "CENTROlink ABIC Participants Transition Plan"

LINK

Lithuanian electronic money institutions (EMIs) and payment institutions ("PIs") providing payment services will be able to have direct access to the payment systems operated by the Eurosystem central banks, including the TARGET payment system, from April next year. EMIs and PIs will also be able to apply for direct participation in payment systems operating in other European Union (EU) countries. On November 20, 2024, the Bank of Lithuania organized a seminar titled "CENTROlink ABIC Participants Transition Plan," focusing on upcoming regulatory changes for payment system participants. The event detailed the transition to a direct participation model, emphasizing safeguarding accounts, liquidity management, and compliance with PSD2 and Settlement Finality Directive( SFD) directives.
On December 3, 2024, the Bank of Lithuania hosted a session titled "Liquidity Management Options in CENTROlink after Transferring Safeguarding Accounts." Presentation explored options for managing liquidity across SCT and SCT INST schemes, both for TARGET system participants and non-participants.

### Announcement from the Bank of Lithuania

LINK

As of November, new legislative amendments in Lithuania allow the Bank of Lithuania and financial market participants to resolve identified operational shortcomings more effectively through administrative settlements.
Previously, the legal framework permitted the Bank of Lithuania to conclude settlements with financial market participants only through the courts. The new administrative settlement mechanism enables out-of-court agreements, significantly streamlining the process.

### REMINDER ON REPORTING

Please be aware that the fourth quarter and the calendar year is coming to an end, meaning that quarterly and annual reports will have to be prepared and submitted. This includes:

- Report on Statistical Payment data and Statistical data on Fraudulent Payments;
- Reports for supervision of the implementation of money laundering and terrorist financing prevention measures;
- Financial reports (at all times be aware of the capital adequacy requirements).

***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

ECOVIS ProventusLaw

**11.2024**

### New rules to bolster the resilience of technology and other third parties providing key services to financial firms in the UK

LINK

UK financial regulators, the Financial Conduct Authority, Bank of England, and Prudential Regulation Authority have confirmed new rules to bolster the resilience of technology and other third parties providing key services to financial firms.

### For the attention of Special Entities under the updated Cybersecurity Law

LINK

The European Union Agency for Cyber Security (ENISA) is developing implementation guidelines to assist EU Member States and cyber security actors in implementing the technical and methodological requirements for cyber security risk management measures set out in the European Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024.

### Polish SA: administrative fine

LINK

A catering company in Poland, Res-Gastro M. Gaweł Sp. k., reported a lost flash drive containing sensitive personal data, including employee details like names, addresses, PESEL numbers, and financial information. The data was stored in unencrypted files, revealing a lack of robust data protection measures.

### EBA, ESMA and EIOPA publish deadlines for the collection of information under DORA

LINK

The European Supervisory Authorities (ESAs) have published a decision on the information that competent authorities need to provide to them in order to identify third-country providers of critical information and communication technology (ICT) services under the Digital Operational Resilience Act (DORA). The Decision specifies that competent supervisory authorities, after collecting information from financial market participants, have until 30 April 2025 to provide information on the registers of financial entities' arrangements with ICT third party service providers.

### Results of the Inspection on the Compliance of Short-Term Vehicle Rentals with Data Protection Requirements

LINK

The data protection authorities of the Baltic States initiated a joint preventive inspection to evaluate the compliance of the short-term vehicle rental sector with the requirements of the General Data Protection Regulation (GDPR).

During the inspection, violations indicating deficiencies in data protection compliance were uncovered. The most significant issues included a lack of transparency—failure to provide meaningful information to data subjects—and improper selection of legal bases. Some companies relied on inappropriate legal grounds or failed to sufficiently justify their use.

### Guidelines 02/2024 on Article 48 GDPR

LINK

The European Data Protection Board (EDPB) published guidelines for public consultation on Article 48 of the GDPR regarding data transfers to third-country authorities and approved a new European Data Protection Seal.

These **guidelines** focus on requests aiming at direct cooperation between a third country public authority and a private entity in the EU (as opposed to other scenarios where personal data is exchanged directly between public authorities in the EU and in third countries respectively, e.g. on the basis of a mutual legal assistance treaty). Such requests may come from all kinds of public authorities, including those supervising the private sector such as banking regulators and tax authorities, as well as authorities dealing with law enforcement and national security.

***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 11.2024

ECOVIS ProventusLaw

### The European Banking Authority

LINK

The European Banking Authority (EBA) has issued two sets of final guidelines, including EBA/GL/2024/15, which establish common EU standards for financial institutions (FIs) and crypto-asset service providers (CASPs) on governance, policies, procedures, and controls for compliance with Union and national restrictive measures.

Guideline EBA/GL/2024/15 specifically targets the effective implementation and operation of screening systems used for sanctions compliance.

### The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)

LINK

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has announced extensive measures to limit Russia's access to the international financial system in response to its ongoing war against Ukraine.
These actions aim to disrupt financial channels used by Russia to support its military operations.

### The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)

LINK

The Office of Foreign Assets Control (OFAC) has issued updated sanctions compliance guidance aimed at the maritime transport industry, focusing on commodities brokers, insurers, ship management service providers, ship brokering companies, and port authorities. This guidance builds upon the 2020 joint guidance released by OFAC, the U.S. Department of State, and the U.S. Coast Guard. While not legally binding, the updated guidance recommendations to help industry participants establish proactive compliance frameworks.

Key areas of focus include:

- Deceptive Sanctions Evasion Shipping Practices: Identifying and mitigating risks related to deceptive practices in shipping.
- Transactional Documents: Detecting sanctioned parties and evasion tactics in transactional documents.
- Vessel Registration: Addressing sanctions evasion risks in the context of vessel registration.
- Sanctions Clauses in Contracts: Encouraging the inclusion of sanctions clauses in shipping contracts to enhance compliance, while cautioning that these clauses are complex legal instruments and not absolute safeguards against enforcement risks.

### The United States Department of the Treasury's Office of Foreign Assets Control (OFAC) AML Center conducts training on sectoral sanctions compliance.

LINK

The United States Department of the Treasury's Office of Foreign Assets Control (OFAC) has imposed sanctions on 26 entities, individuals, and vessels linked to the Al-Qatirji Company. This Syrian conglomerate, already sanctioned in 2018 under Executive Order 13582 for facilitating oil sales between the Syrian regime and ISIS, has now been re-designated pursuant to Executive Order 13224 for terrorism-related activities. The recent sanctions highlight the following key activities:

- Facilitation of oil sales: the Al-Qatirji Company facilitated oil transactions from Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) to Syria and the People's Republic of China (PRC).
- Absence of Chinese purchaser sanctions: despite evidence presented by OFAC, no Chinese purchasers of IRGC-QF-sourced oil were sanctioned under Executive Order 13846, which governs post-JCPOA Iran sanctions. This leaves room for potential future actions targeting Chinese entities linked to Iranian oil transactions.

***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

11.2024

### Lithuanian Banks Improve Customer Experience in Anti-Money Laundering Measures

LINK

Four commercial banks operating in Lithuania have significantly improved their customer experience regarding anti-money laundering (AML) prevention measures throughout 2023. These improvements were implemented following an agreement with the Bank of Lithuania in early 2023, after identifying that AML requirements were causing considerable confusion among consumers.

According to Vaidas Cibas, Director of the Financial Market Supervision Department at the Bank of Lithuania, there has been a notable decrease in complaints about banks' client due diligence procedures. The improvements include:

- Enhanced communication tools to help customers understand complex AML requirements
- Streamlined know-your-customer (KYC) questionnaires
- New dedicated website sections explaining AML requirements
- Simplified customer notifications
- Improved staff training for customer service

Key improvements in customer experience include the ability to update KYC information based on previous submissions rather than starting from scratch, customized questionnaires for different customer groups, flexible deadlines for information submission, and increased use of government databases to reduce the burden on customers.

### Fight with fraudsters

LINK

The Bank of Lithuania emphasizes that financial fraud has increased more than sevenfold over the past four years, with scammers extracting tens of millions of euros annually from victims.

According to Simonas Krėpšta, Board Member of the Bank of Lithuania, effective combat against financial fraud requires unified efforts from institutions, financial market participants, and electronic communications service providers, especially as financial services become increasingly digital and borderless. Until now, there has been no single institution responsible for financial fraud prevention, while existing legal regulations sometimes fail to meet current needs, and there are limitations in information sharing between mobile service providers and payment service providers.

To address these challenges, the Bank of Lithuania suggests making financial fraud prevention a state priority, establishing a coordinating institution, and strengthening information exchange and technical solutions among all stakeholders.

### European Commission press release EC action on Temu

LINK

The European Commission has opened formal proceedings against Temu under the Digital Services Act (DSA) to investigate four main concerns:

- The platform's measures to prevent the sale of non-compliant products and control rogue traders in the EU.
- The potentially addictive design features of the platform, including game-like reward programs.
- The transparency and options in Temu's product recommendation systems.
- Compliance with data access requirements for researchers.

Temu, designated as a Very Large Online Platform in May 2024 with 92 million monthly EU users, could face penalties if found in violation of DSA Articles 27, 34, 35, 38, and 40. The Commission will gather additional evidence, though there's no set deadline for concluding the investigation. This action does not prevent other authorities from taking separate enforcement measures under consumer protection or product safety regulations.

***Detailed and full Regulatory Compliance report on Consumer Protection Regulation can be found here:***

*Our recommendations and details are in this file*

# REGULATORY COMPLIANCE UPDATE

## EMPLOYMENT

11.2024

ECOVIS ProventusLaw

### Labour Code Amendments

LINK

From **1 January 2025**, amendments to the Law on the Legal Status of Foreigners will come into force.

Key changes:

**1. Labour Market Test Abolished**
Foreign workers will no longer be assessed for suitability to the Lithuanian labour market. The Shortage Occupations List will also be discontinued, simplifying migration procedures.

**2. Introduction of a Quota System**
- Annual quotas will limit permits to 1.4% of Lithuania's population (approx. 40,000).
- Exceptions: graduates of Lithuanian institutions, those with temporary protection, or cases with exceptional circumstances.
- Exceeding quotas requires employers to offer at least 1.2 times the average wage.

**3. Additional Quotas**
From 2026, collective agreement parties may propose extra quotas (up to 20%) for their members, subject to approval.

### Order of the Minister of the Interior of the Republic of Lithuania

LINK

From **1 December 2024**, new rules tightened the submission process for temporary residence permits and national visas through external service providers.

Key Changes:

4. **Eligibility Restriction**: Applications are only accepted from citizens of the country where the external service provider operates.

5. **Exceptions**: Exemptions apply to specific categories of applicants, including those applying for:
Family reunification.
- Study purposes.
- High-skilled jobs.
- Positions as lecturers or researchers.

Citizens of Australia, Japan, the United Kingdom, the United States, Canada, New Zealand, and South Korea are not affected by these restrictions and can continue to apply under existing procedures.

### Law Ammendments

LINK

Amendments to the Labour Code, which will enter into force on 1 January 2025, clarifies the concept of violence and harassment. The amendments clarify that unacceptable behaviour by the employer itself (a natural person or the manager of legal person) will be considered as violence or harassment.
At the same time, the Administrative Offences Code of the Republic of Lithuania imposes fines of between EUR 500 and EUR 3 000 on company managers or other responsible persons for violation of the prohibition of violence and harassment by failing to take the necessary measures to ensure prevention, by failing to provide active assistance to victims or in the event of a breach of the prohibition of violence or harassment by the company manager.
The amendment to the Labour Code also stipulates that the Chief State Labour Inspector of the Republic of Lithuania will approve a description of the minimum measures necessary for the elimination and/or control of violence and harassment and will provide for the regularity of training on the prevention of violence and harassment.

**We recommend the following actions:**

1. **Update Workplace Policies.** Employers should revise internal policies to explicitly address violence and harassment, including unacceptable behaviour by employers or managers.
2. **Implement Regular Training.** We recommend conducting regular training for all employees and managers on preventing and addressing violence and harassment in the workplace.
3. **Establish Confidential Reporting Channels.**
4. **Ensure Compliance.** Employers should regularly review their practices and assign specific responsibilities to ensure compliance with the new regulations, avoiding fines.
5. Support Victims. It is recommended that employers provide support to victims, including access to counseling, legal advice, and necessary adjustments to the working environment.

info@proventuslaw.lt

# REGULATORY COMPLIANCE UPDATE

CRYPTO

11.2024

ECOVIS ProventusLaw

**The European Commission**

LINK

The European Commission has issued six Regulatory Technical Standards (RTS) applicable to CASPs under the MiCA regulation.
The RTS package includes the following standards:

- RTS outlining the procedure for obtaining approval of a crypto-asset white paper.
- RTS defining the information that financial entities must provide in their notification of intent to offer crypto-asset services.
- RTS specifying the requirements to ensure continuity and regularity in the delivery of crypto-asset services.
- RTS establishing the methodology for calculating the number and value of transactions involving asset-referenced tokens and e-money tokens denominated in non-EU currencies used as a means of exchange.
- RTS outlining the conditions for the establishment and functioning of consultative supervisory colleges.
- RTS detailing the information required in an application for authorization as a crypto-asset service provider.

**The Wolfsberg Group**

LINK

The Wolfsberg Group has released a set of frequently asked questions (FAQs) aimed at providing financial institutions with guidance and clarity on key concepts and risks associated with the digital assets market. These FAQs serve to enhance understanding by offering precise definitions and explanations of emerging trends and regulatory considerations.
Key highlights from the FAQs:

– The FAQs define digital assets as cryptographically secured digital representations of value or rights. These include virtual assets, cryptocurrencies, NFTs with inherent value, stablecoins, and tokenized deposits. Digital assets often rely on distributed ledger technology (DLT) for trading, exchange, or investment purposes.
– The FAQs differentiate between fiat-backed stablecoins and other stablecoins, emphasizing the need for financial institutions to assess their collateralization mechanisms. Fiat-backed stablecoins: generally more stable due to proper collateralization and subject to higher regulatory oversight; other stablecoins: present higher risks arising from inconsistent reserve requirements and their potential for misuse on a global scale.
– The FAQs provide detailed explanations of emerging innovations, including:
o Tokenized Assets: Digital representations of traditional assets.
o Layer 1 (L1) and Layer 2 (L2) Protocols: Base blockchain networks and scaling solutions, such as rollups, designed to increase transaction efficiency while maintaining L1 security.
o Initial Coin Offerings (ICOs): Tools for fundraising in the digital assets market. These innovations are outlined to assist financial institutions in evaluating their potential risks and benefits.

**The European Commission**

LINK

The European Commission adopted a Delegated Regulation that supplements the Markets in Crypto-assets Regulation (MiCAR). This regulation establishes regulatory technical standards specifying how CASPs should present transparency data. The regulation addresses both pre-trade data (including bid and ask prices and the depth of trading interest) and post-trade data (covering the price, volume, and time of executed transactions). The regulation will be subject to review by the Council of the European Union and the European Parliament and, if no objections are raised, will be published in the Official Journal of the European Union and take effect 20 days thereafter.
Key Provisions:

– The regulation outlines specific requirements for both Centralized Exchanges (CEXs) and Decentralized Exchanges (DEXs), taking into account their distinct operational models.
– CASPs are required to disclose bid and ask prices along with the depth of trading interests, based on the type of trading system employed.
– CASPs must make public all transaction information, including any amendments or cancellations to previously reported trades.
– Data must be presented separately for pre-trade and post-trade information, with the option for disaggregation by individual crypto-asset or grouping by asset type.

***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

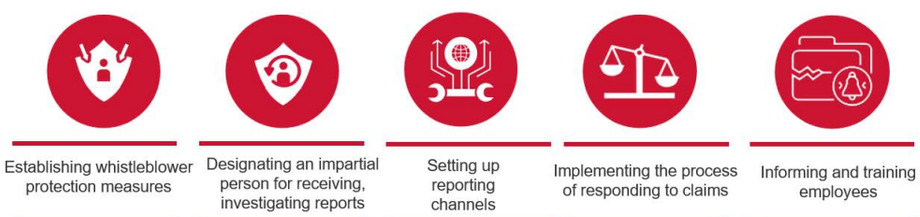
**LINK**

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.

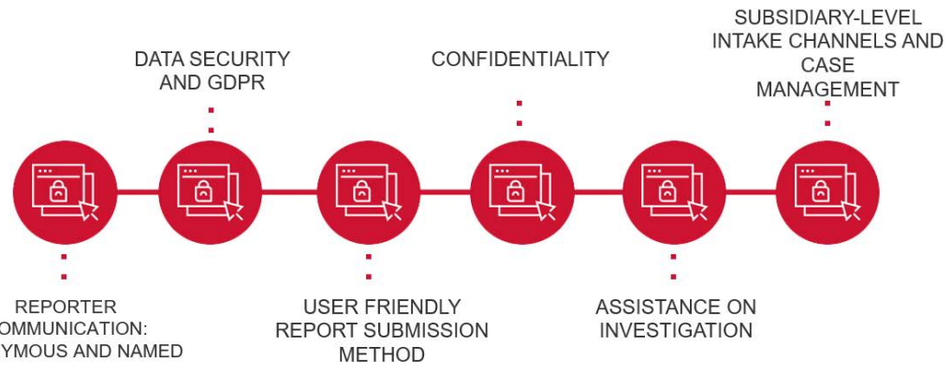
Under the EU Whistleblower Directive, organisations must establish secure and confidential reporting channels for whistleblowers. The reporting process is designed to ensure the protection of whistleblowers and the effective handling of reports of wrongdoing.




### 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.