REGULATORY COMPLIANCE UPDATE

ECOVIS TOOLS FOR COMPLIANCE

ECOVIS ProventusLaw

Digital Operational Resiliance Act DORA

LINK

European Union's (EU) binding Digital Operational Resilience Act (DORA) regulation aims to strengthen the IT security of financial companies such as banks, payment an e-money insurance companies, and investment firms. **Financial institutions are now legally required take digital resilience seriously.**

ECOVIS ProventusLaw offers the **DORA Compliance Self-Assessment Tool**, helping businesses:

- Assess ICT risk management, incident reporting, resilience testing and third-party management.
- Review compliance status with around 200 targeted questions.
- Strengthen digital resilience and mitigate cyber risks.

Contact us	Get access	Complete questionnaire	Gap analysis and planning
• Reach out to request access to the tool.	• This online tool has safe log-in access and a safety guarantee.	• This tool possesses nearly 200 questions on various topics according to DORA Articles and covers all necessary areas for DORA compliance.	• If needed, consult our experts to develop a clear action plan to prepare for full DORA compliance.

Want to know if your organisation complies with DORA requirements? Contact us by e-mail vilnius@ecovis.lt, get access to our compliance self-assessment tool and seek expert advice.

FREE NIS2 SELF-ASSESSMENT TOOL

LINK

ECOVIS ProventusLaw offers a free, user-friendly **NIS2 self-assessment tool** designed to help organisations evaluate their alignment with the Cybersecurity Act and the Lithuanian Government's NIS2 implementation requirements.

The tool features structured questionnaires covering key NIS2 areas. Results can be exported in PDF format for internal use or expert review upon completion.

This user-friendly resource helps organisations:

- Understand the cybersecurity requirements under national law.
- Evaluate their current compliance status.
- Identify regulatory gaps and plan next steps.

The tool is structured according to the legal provisions and supports organisations in building a roadmap toward full conformity.
Whether you're newly listed in the register or simply want to assess your readiness, our experts at ECOVIS ProventusLaw are here to help. We provide tailored legal support and practical guidance for navigating the complex cybersecurity landscape.

Check out our NIS2 self-assessment tool here: **https://tis2.ecovis.lt/**

Upon your request, the ECOVIS ProventusLaw team can perform your compliance analysis, identify gaps, provide you with a plan of further action along with our recommendations, and help you implement the above requirements.
Considering your company's specific needs, we offer different service packages – from basic compliance assessment to comprehensive legal and cybersecurity assurance.

NIS2 self-assessment tool

REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

06.2025

ECOVIS ProventusLaw

The Seimas of the Republic of Lithuania

LINK

The Seimas of the Republic of Lithuania approved the draft law amending the Law on the Prevention of Money Laundering and Terrorist Financing (PPTFPĮ). Although the amendments have not yet entered into force pending signature, the essential forthcoming legal modifications are already evident. The proposed changes aim to ease regulatory burdens, enhance flexibility in compliance procedures, and harmonise national requirements with EU practices. The principal amendments include the following:

1. The requirement for apostilled or legalised powers of attorney has been removed, provided the document is issued in an EU Member State. This change is a significant procedural simplification welcomed by market participants.
2. Institutions are no longer required to explicitly demand documents or information to ascertain the client's control structure and business activities. Instead, they must now undertake reasonable measures, allowing more discretion in determining what constitutes a proportionate and risk-based approach. Documentation is no longer mandatory per se.
3. The law now allows financial institutions to collect customer and beneficial ownership information from other reliable and independent sources, including databases and registers, where the relevant data is not available in official registers of EU Member States.
4. The regulation of simplified identity verification has been substantively revised. The previous exhaustive list of circumstances allowing the application of SDD has been replaced by risk indicators which suggest potentially lower risk. Financial institutions must consider these indicators when determining whether to apply SDD. Additionally, the €1,000 threshold for electronic money has been abolished. However, identity verification obligations remain mandatory even under SDD.

The Bank of Lithuania

LINK

On 26 June 2025, the Bank of Lithuania announced the introduction of a new anti-fraud measure, coming into effect on 9 October 2025, which will be binding on all euro area payment service providers. This includes banks, credit unions, electronic money institutions, and payment institutions operating within the SEPA and instant euro payments infrastructure.

Under the new regime, all payment service providers must verify that the name of the intended beneficiary, as provided by the payer, corresponds to the actual legal account holder of the beneficiary's IBAN. This verification must occur automatically and in real-time, prior to the execution of the payment, via the provider's electronic interface (e.g., internet banking or mobile app).

Verification outcomes will be categorised into four result types: (i) full match, (ii) near match (with the corrected name shown), (iii) no match, and (iv) verification unavailable. Despite the verification result, the payer will retain the right to proceed with the payment at their discretion.

Importantly, the legal liability regime accompanying this measure stipulates that if the payer confirms the transaction despite a warning (e.g., a mismatch), the liability for the payment remains with the payer. However, if the provider fails to execute the verification service or executes it incorrectly, and this results in the misdirection of funds, the provider may be held liable and will be required to reimburse the payer.

Additionally, the Bank of Lithuania has emphasised that payment service providers are strictly prohibited from communicating verification outcomes or payment-related confirmations via external email or SMS messages containing links, due to the elevated risk of phishing and fraud. All verification information must be provided within the secure environment of the institution's official electronic platform.

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

06.2025

ECOVIS ProventusLaw

Event by the Bank of Lithuania

LINK

In June the Bank of Lithuania organized an event to present its expectations regarding governance, risk management, and internal control frameworks applicable to electronic money institutions (EMIs) and payment institutions (PIs).

Changes in Legal Regulation

New Governance and Internal Control Requirements (Effective January 1, 2026 – BoL Resolution No. 247) include but are not limited to:

- Allocation of the areas of responsibility among members of collegiate bodies
- The bodies of EMIs/PIs are responsible for:
  - ✓ establishment, design and implementation of the management system;
  - ✓ strengthening of the internal risk culture;
  - ✓ development and implementation of conflicts of interest management measures;
  - ✓ monitoring of the effectiveness of the management system.
- The board is responsible for setting out the principal rules of risk management and internal audit organisation.
- EMI/PIs must appoint persons responsible for monitoring, control, and ensuring compliance with requirements for the safeguarding of client funds and for monitoring and ensuring compliance with capital requirements. These persons may be responsible for several control functions, except for the person responsible for the internal audit.
- EMIs/PIs bodies must establish accountability requirements for the second line internal control officers who are directly accountable to them.
- Agent oversight must include registration in the register of intermediaries, clear separation of responsibilities between the EMI/PI and their intermediaries, monitoring and supervision of the activities of agents, inspections - at least annual.

Risk Management Framework Requirements

- Risk management must include settlement, liquidity, operational, money laundering and terrorist financing, compliance, market, counterparty credit, concentration, business conduct risk and other risks which are relevant to the institution‘s activity (licensed or not).
- Applies the “comply or explain” principle.
- Mandatory involvement of the risk management officer (CRO) in the decision-making process regarding significant risk management, the possibility of directly informing the supervisory body and the collegial management body.

Article by the Bank of Lithuania

LINK

Payment institutions providing payment services will be required to verify whether the name of the payee indicated in a payment instruction matches the owner of the specified bank account (IBAN), before executing a transfer.

For every SEPA or instant credit transfer in euros, payment service providers will be required to show whether the payee's name (or full name in the case of individuals) matches the actual owner of the provided IBAN. The verification is based on information stored in the payee’s payment service provider’s system. Verification check will be conducted before the payment is confirmed, right after the payer inputs the payee's IBAN and name. Regardless of the result, only the payer has the authority to confirm (authorize) the payment.

The Bank of Lithuania also published a new Frequently Asked Questions (FAQ) section regarding the payment account holder name and IBAN verification service.

REMINDER ON REPORTING

Please make sure that by 1st of June you have submitted the reports to State Tax Inspectorate as per deadlines indicated in the excel reporting calendar. This includes:

- Reporting on client’s annual turnover, if the total annual turnover of all accounts held by the same person with the same financial market participant is at least EUR 15,000;
- Reporting on client’s balance, if the total annual balance of accounts of the same person with the same financial market participant at the end of the year is not less than EUR 5,000;
- The debt obligations owed to a financial market participant as at 31 December of the calendar year.

Please make sure that by 1st of July you submitted the reports to State Tax Inspectorate on reportable account.

As well, please be aware that the second quarter has ended, meaning the following reports had to be submitted. This includes:

- 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 Payment Services Regulation can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

PERSONAL DATA PROTECTION AND ICT REGULATION

06.2025

ECOVIS ProventusLaw

Bank of Lithuania hosted a consultation event focused on third-country risk management

LINK

On June 5, 2025, the Bank of Lithuania hosted a consultation event focused on third-country risk management, bringing together financial market participants to discuss the evolving regulatory landscape under the Digital Operational Resilience Act (DORA) and related EU and national frameworks.

Key Topics Covered:

- Regulatory updates
- ICT services and contracts
- Outsourcing of other critical or important functions
- Notification obligations
- Ongoing monitoring and exit strategies
- Sub-outsourcing and concentration risk

Council and European Parliament reach deal to make cross-border GDPR enforcement work better for citizens

LINK

The Council, represented by the Polish presidency of the Council of the EU, and the European Parliament secured a provisional deal on a new law which will improve cooperation between national data protection authorities when they enforce the General Data Protection Regulation (GDPR) in cross-border cases.

The European co-legislators agreed on rules that will streamline administrative procedures relating to, for instance, the rights of complainants or the admissibility of cases, and thus make enforcement of the GDPR, which has been in application since 25 May 2018, more efficient.

Latvian Data Protection Authority Develops E-Learning Course Now Available in Lithuanian

LINK

The Data Protection Authority of Latvia (hereinafter – Latvian DPA), implementing the project “Remote Training Program in the Field of Data Protection,” with support from the European Commission’s funding programme “Citizens, Equality, Rights and Values,” has developed an interactive personal data protection training course (hereinafter – the Course).

The Course is designed primarily for small and medium-sized enterprises but is also useful for representatives of associations, foundations, sole proprietors, and anyone interested in learning more about data protection.

Massive Password Leak: NCSC Advises How to Protect Yourself and Your Accounts

LINK

The National Cyber Security Centre (NCSC) under the Ministry of National Defence is responding to one of the largest recorded data breaches to date. According to cybersecurity researchers, data from as many as 16 billion active user accounts has been made public. Affected platforms include Apple, Google, Facebook, Telegram, GitHub, Microsoft, and others.

EDPB publishes final version of guidelines on data transfers to third country authorities

LINK

The EDPB has adopted the final version of the guidelines on data transfers to third country authorities. In its guidelines, the EDPB zooms in on Art. 48 GDPR and clarifies how organisations can best assess under which conditions they can lawfully respond to requests for a transfer of personal data from third country authorities (i.e. authorities from non-European countries).

SPE training material on AI and data protection

LINK

The EDPB presented two new Support Pool of Experts (SPE) projects*: Law & Compliance in AI Security and Data Protection and Fundamentals of Secure AI Systems with Personal Data. The two projects, which have been launched at the request of the Hellenic Data Protection Authority (HDPA), provide training material on AI and data protection.

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 06.2025

ECOVIS ProventusLaw

The Financial Action Task Force (FATF)

LINK

The report called Complex Proliferation Financing and Sanctions Evasion Schemes, published by FATF in June 2025, identifies significant vulnerabilities in the global financial system related to the financing of weapons of mass destruction.

It highlights that only 16% of assessed jurisdictions effectively implement targeted financial sanctions under United Nations Security Council Resolutions concerning proliferation. Illicit actors are employing increasingly sophisticated methods to evade sanctions and circumvent export controls, including the use of intermediaries, concealment of beneficial ownership, exploitation of virtual assets, and manipulation of maritime and shipping sectors.

The Democratic People's Republic of Korea (DPRK) is identified as a principal actor generating revenue through cyberattacks, overseas labour, and other illicit activities. These findings underscore the urgent need for enhanced global vigilance and cooperation to address these complex risks.

The Lithuanian Financial Crime Investigation Service (FCIS)

LINK

In 2024, the Lithuanian Financial Crime Investigation Service (FCIS) received 82,300 suspicious transaction reports (STRs), reflecting a decrease of approximately 16 percent compared to 98,588 reports in 2023. The majority of these reports were submitted by banks and their branches, with a marked increase in reporting from VASPs as well as gambling and lottery operators. The FCIS observed a significant rise in STRs related to attempts to circumvent EU sanctions, particularly through the sale of luxury vehicles, trade in dual-use goods, the establishment of shell companies in third countries, and document forgery aimed at concealing sanctioned Russian or Belarusian ownership. In 2024, such reports numbered 305, up from 193 in the previous year. Furthermore, the FCIS conducted 18 on-site inspections of reporting entities, including 11 VASPs, resulting in administrative penalties exceeding €1.8 million, with individual fines ranging from €3,500 to €1.06 million, and issued one official warning. Additionally, the FCIS granted 392 exemptions or authorisations under international sanctions regulations, facilitated inter-agency cooperation, and processed 66 STRs related to sanctions evasion, of which 23 were escalated to national or EU authorities for further investigation.

The European Council of the European Union

LINK

On 30 June 2025, the Council of the European Union extended its economic sanctions against Russia for an additional six months, until 31 January 2026. These measures, initially implemented in 2014 and significantly expanded since February 2022, aim to address Russia's ongoing destabilising actions in Ukraine. The sanctions encompass a wide range of sectoral restrictions, including limitations on trade, finance, energy, technology, dual-use goods, industry, transport, and luxury goods. Notably, they include a ban on the import or transfer of seaborne crude oil and certain petroleum products from Russia to the EU, the de-SWIFTing of several Russian banks, and the suspension of broadcasting activities and licenses in the EU for several Kremlin-backed disinformation outlets. Additionally, specific measures are in place to counter sanctions circumvention.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

CONSUMER PROTECTION

06.2025

ECOVIS ProventusLaw

The State Consumer Rights Protection Authority

LINK

EU Accessibility Requirements Become Mandatory for Digital Products and Services

Starting June 28, 2025, businesses in Lithuania must comply with new accessibility requirements ensuring that products and services are usable by all consumers, including persons with disabilities. These obligations stem from the EU Accessibility Act and are enforced through national legislation and oversight by authorities like the State Consumer Rights Protection Authority (VVTAT).

The accessibility requirements, set out in the Law on Accessibility of Products and Services, apply to medium and large enterprises and cover a wide range of goods and services—such as websites, mobile applications, e-commerce platforms, banking services, e-books, and transport-related elements.
Companies must ensure their offerings meet technical standards for accessibility, such as compatibility with screen readers, keyboard navigation, and appropriate color contrast. Very small enterprises (fewer than 10 employees and under €2 million in turnover) are exempt. Enforcement will be shared among multiple authorities, with VVTAT providing guidance and industry support. Companies are urged to assess whether their services fall under the scope of the law and prepare accordingly using official recommendations and standards like EN 301 549.

Our recommendation

Institutions should initiate cross-functional planning with IT, legal, to ensure timely compliance and staff training.

Alignment with official obligations and proactive communication with supervisory authorities will mitigate legal and reputational risks arising from non-compliance.

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

06.2025

ECOVIS ProventusLaw

Decision on the civil case

LINK

The Supreme Court of Lithuania clarified that a mere undertaking by an employer submitted to the Migration Department to employ a foreign national does not, in itself, constitute the conclusion of an employment contract between the parties. The Court emphasised that an employment relationship only commences after an assessment has been made as to whether the prospective employee genuinely possesses the qualifications necessary to perform the job functions, and upon agreement being reached on the essential terms and conditions of employment. The case concerned a dispute between a foreign national (the claimant) and a logistics company (the respondent), at whose invitation the claimant had travelled to Lithuania to work as a driver of international freight transport vehicles. The respondent had submitted a request to the Migration Department for the issuance of a temporary residence permit for the claimant, which was duly granted. However, upon arrival in Lithuania, the claimant failed to pass a practical driving test for lorry operation organised by the respondent, following which the respondent refused to enter into an employment contract with him. The courts of first instance and appeal found that an employment contract had been concluded but had not come into force due to no fault of the claimant, and accordingly awarded him compensation and damages from the respondent.The Supreme Court of Lithuania overturned the procedural decisions of the lower courts. It held that, notwithstanding the employer's declared intention to employ the foreign national in the course of immigration procedures, the employer retains the right to assess the foreign national's abilities prior to concluding an employment contract. As the claimant failed to demonstrate the requisite qualifications through the practical skills test administered by the respondent, the respondent was justified in terminating the recruitment process. Accordingly, no employment contract was lawfully concluded, and the claimant is not entitled to compensation or damages.

Decision on the civil case

LINK

On 5 June 2025, the Supreme Court of Lithuania delivered a ruling clarifying the legality of dismissals in the context of organisational restructuring and the outsourcing of part of a business. In this case, a healthcare institution, aiming to reduce losses, decided to discontinue the in-house production of dental prostheses and instead outsource these services to third parties. As a result, the positions of dental technicians were abolished, and the employees concerned were dismissed. The employees challenged the dismissals, arguing that the employer had first asked them to accept a significant pay cut—nearly threefold—and, upon their refusal, restructured the organisation and eliminated their roles, outsourcing the functions to an external provider. The employees claimed this violated Article 45(2) of the Lithuanian Labour Code, which prohibits terminating an employment contract under Article 57 if the employee refuses to accept a lower salary. They also argued that the outsourcing constituted a transfer of part of the business, in which case employment continuity must be ensured. The Supreme Court rejected the employees' claims, holding that an employer has the right to independently organise its activities, including decisions on its structure, workforce, positions, and operational efficiency. The Court stressed that genuine organisational changes that render an employee's function redundant can justify dismissal, even if the employee previously refused to accept a lower wage. Such dismissals do not breach the prohibition under Article 45(2) if the reorganisation is real and lawful. In conclusion, the Court confirmed that employers may reorganise and optimise their operations for efficiency, provided the changes are genuine and comply with legal requirements. Employee rights must be respected, but they cannot prevent legitimate business restructuring.

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

LINK

As of 1 June 2025, Lithuania no longer recognizes non-biometric passports issued by the Russian Federation as valid travel documents for entry into its territory. The restriction does not apply to rail transit between Kaliningrad and mainland Russia. For Russian nationals holding residence permits issued by Lithuania or other EU/EEA/ Schengen countries, the same restriction will take effect on 1 December 2025, allowing time to replace non-biometric passports.

Exceptions may be granted on a case-by-case basis for members of the democratic opposition, independent media, or civil society, where the purpose of travel aligns with Lithuania's national interests.

This measure aligns with similar restrictions already adopted by other EU Member States and reflects national security concerns and ICAO travel document standards.

vilnius@ecovis.lt

REGULATORY COMPLIANCE UPDATE

CRYPTO

06.2025

ECOVIS ProventusLaw

The European Banking Authority & the Bank of Lithuania

LINK

On 10 June 2025, the European Banking Authority (EBA) issued a No Action Letter clarifying the treatment of EMTs under the MiCA and the Second Payment Services Directive (PSD2). As EMTs qualify both as crypto-assets under MiCA and electronic money under PSD2, CASPs engaging in activities such as transferring EMTs on behalf of clients or providing custodial wallets with transfer functionality may face dual licensing obligations. To reduce the regulatory burden during the transition to MiCA, the EBA recommended that NCAs temporarily suspend full enforcement of PSD2 requirements for EMT services until 1 March 2026. During this period, information submitted for MiCA authorisations may be used to streamline PSD2 licensing, with core obligations such as strong customer authentication, fraud monitoring, and capital adequacy still applying. The EBA also confirmed that crypto-to-EMT exchanges fall outside PSD2's scope and do not require a licence.

On 11 June 2025, the Bank of Lithuania issued a corresponding No Action Letter confirming that, from 2 March 2026, CASPs offering EMT payment services must obtain a payment institution licence under PSD2 or cease such activities. The Bank encourages use of simplified licensing pathways during the interim and expects CASPs to ensure compliance with key safeguarding, security, and capital requirements.

The European Securities and Markets Authority

LINK

On 20 June 2025, the European Securities and Markets Authority (ESMA) issued Q&A 2579, interpreting key provisions of Regulation (EU) 2023/1114 on MiCA. ESMA clarified that when an EU-licensed CASP shares its order book with a non-EU platform, regardless of whether the platforms are part of the same corporate group, the non-EU platform is deemed to be operating a trading platform in the European Union without authorisation.

ESMA considers "management of an order book" as tantamount to the operation of a trading platform under Article 3(18) MiCA. Such arrangements are in breach of Articles 59, 60, and 63 MiCA, which require prior authorisation and regulatory oversight for trading platforms within the EU. As a result, any infrastructure that facilitates cross-border liquidity pooling or order matching between MiCA-regulated and non-regulated platforms is considered non-compliant with EU law.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

MANDATORY REQUIREMENTS FOR FINANCIAL INSTITUTIONS

ECOVIS ProventusLaw

Digital Operational Resiliance Act DORA

LINK

European Union's (EU) binding Digital Operational Resilience Act (DORA) regulation aims to strengthen the IT security of financial companies such as banks, payment and e-money insurance companies, and investment firms.

We would like to point out that you must assess your readiness. Key Steps to Ensure Compliance:

- Involve the Management Board: Ensure executive leadership actively oversees ICT risk management.
- Strengthen ICT Risk Frameworks: Implement policies and controls aligned with DORA requirements.
- Incident Reporting Processes: Develop standardised protocols for detecting and reporting ICT incidents.
- Policy and Procedure Updates: Align response plans and testing protocols with DORA's legal framework.
- Review Third-Party Contracts: Ensure vendor contracts meet DORA's risk management and oversight standards.

At ECOVIS ProventusLaw, we help financial institutions translate regulatory obligations into actionable strategies. With our deep legal and ICT risk expertise, we implement effective internal audit systems tailored to DORA's strict requirements—ensuring compliance and true operational resilience.

Our DORA Audit Services include:

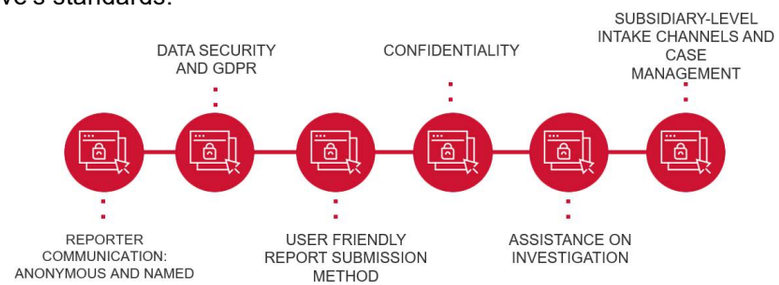
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors meet DORA standards

Want to know if your organisation complies with DORA requirements? Contact us by e-mail vilnius@ecovis.lt, get access to our compliance self-assessment tool and seek expert advice.

WHISTLEBLOWING DIRECTIVE IMPLEMENTATION
Outsourcing solution for companies

LINK

The EU Whistleblower Directive is mandatory for financial institutions under the **EU Whistleblower Directive** and the **Resolution No. 03-33** of the Board of the Bank of Lithuania. This resolution requires financial institutions to establish a **confidential and secure channel** for reporting 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.
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.
Ecovis Wistleblowing'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.

Contact us at vilnius@ecovis.lt, and we will ensure compliance with the Whistleblowing Directive tailored to your specific situation and available resources.