REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

09.2025

ECOVIS ProventusLaw

The Financial Crime Investigation Service (FCIS)

LINK

On 24 September 2025, the Financial Crime Investigation Service adopted Order No. V-221, amending the 2017 Instructions for providers of trust or company formation and administration services. The revised Instructions apply to all such providers in Lithuania that are not auditors or accounting firms and strengthen obligations in line with the AML/CTF Law and the EU requirements.

The amendments introduce a clearer risk-based approach, requiring providers to apply ordinary, simplified, or enhanced due diligence depending on client risk. Enhanced checks are mandatory for high-risk clients, politically exposed persons, and third-country relationships. Service providers must verify client and beneficial owner identities, understand ownership structures, and monitor transactions throughout the business relationship.

The rules also tighten reporting duties: suspicious transactions must be suspended and reported to FCIS, and all cash transactions of EUR 15,000 or more must be declared. Record-keeping obligations are expanded, requiring the maintenance of registers of suspicious and cash transactions, as well as terminated client relationships. Annual audited financial reports and risk-based monitoring procedures must align with international standards.

Responsibility for compliance rests with senior management, who must ensure adequate internal controls, sanctions screening, and staff training. The Instructions emphasise accountability at the governance level and require ongoing updating of internal AML/CTF systems to reflect changes in regulation and risk.

The European Supervisory Authorities

LINK

The European Supervisory Authorities (EBA, EIOPA, and ESMA) have issued a joint statement urging financial institutions to remain vigilant amid heightened geopolitical tensions and economic uncertainties. Their Autumn 2025 Joint Committee Report highlights the deteriorating economic outlook due to global trade tensions and security concerns. While the initial impact of the US–EU preliminary trade agreement was moderate, the authorities caution that risks to financial stability persist, necessitating proactive risk management and adequate provisioning by financial entities.

The European Supervisory Authorities

LINK

In 2025, the Financial Action Task Force (FATF) issued a Handbook on international co-operation in money laundering detection, investigation, and prosecution. The report underlines that cross-border financial crime is becoming faster, more complex, and increasingly difficult to investigate. It distinguishes between formal channels, such as mutual legal assistance and extradition, and informal mechanisms, such as direct intelligence sharing, stressing that both are essential and must be used in parallel.

The key message is that fragmented legal frameworks, slow processes, and weak coordination continue to hinder effective enforcement. FATF therefore calls on countries to improve the speed and quality of requests, invest in secure communication channels, strengthen domestic inter-agency coordination, and adopt digital tools that enable real-time information exchange and joint investigations.

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

09.2025

ECOVIS ProventusLaw

European best practices for the development of the Lithuanian financial market

LINK

By strengthening the competitive landscape of Lithuania's financial market, the Bank of Lithuania reduces the administrative burden and reviews national supervisory requirements in the context of other European Union (EU) countries. When reviewing legal regulation, the Bank of Lithuania follows the principle of risk-based supervision set out in its supervisory policy, which means applying appropriate and more flexible regulation to lower-risk areas to enhance the attractiveness and competitiveness of the Lithuanian financial sector. One of the most important regulatory initiatives was the amendments to the Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing, drafted by The Bank of Lithuania together with other institutions and financial market representatives and which entered into force in July this year. In addition, the Board of The Bank of Lithuania updated its resolution on the supervisory authority's choice to apply the exemptions provided for in EU banking sector regulations. Supervisory authorities are given the possibility to take into account the specificities of the national financial market, impose stricter requirements on higher-risk credit institutions or, following the principle of proportionality, relax certain requirements in lower-risk areas. Moreover, the Board of The Bank of Lithuania approved the updated General Regulations on the Submission and Examination of Applications for the Authorisation of Financial Market Participants Supervised by The Bank of Lithuania and on the Granting of Authorisation. The Bank of Lithuania has taken into account the proposals received to reduce the administrative burden, and therefore applicants will no longer have to submit to The Bank of Lithuania legalised or APOSTILLE-certified documents drawn up or issued in foreign countries in every case.

CENTROlink Clients – Verification of Payee Service

LINK

The Bank of Lithuania will offer clients of its payment system CENTROlink the possibility to verify whether the recipient's name (individual or company) indicated in a payment transfer matches the payment account details. The Board of the Bank of Lithuania has approved the rules governing this new service. Under the Instant Payments Regulation, as of 9 October 2025, all payment service providers (PSPs) using credit transfer and instant credit transfer schemes will be required to offer their customers a Verification of Payee (VoP) service.

Non-bank payment institutions to gain direct access to TARGET payment system from 6 October

LINK

Electronic money (EMI) and payment institutions (PI) providing payment services will be able to gain direct access to the TARGET payment system operated by the Eurosystem as of 6 October, except for the T2S system used for settling securities. When participating in TARGET, payment service providers may:

- reach more than 39,000 system participants directly when making payments;
- settle in central bank money, thereby reducing credit and settlement risk;
- manage liquidity independently from commercial banks or third-party infrastructure;
- use the same infrastructure with banks, which is essential for efficiency, transparency and operational resilience;
- directly access Eurosystem settlement solutions, including the TIPS platform for instant payments.

September 17, 2025 Judgement of the Supreme Administrative Court of Lithuania

LINK

On September 17, 2025, the Extended Chamber of the Supreme Administrative Court of Lithuania (LVAT) partially upheld the appeal of UAB Baltic Financial Company. The court overturned both the 2023 decision of the first-instance court and the resolution of the Board of the Bank of Lithuania, which had denied the company a specialized banking license. Additionally, the part of the case concerning the company's claim for €1,008,124.21 in damages was referred back to the Regional Administrative Court for further examination. The Bank of Lithuania had refused to issue the specialized bank license, claiming that the business plan submitted by the company did not ensure safe and reliable banking operations. The court acknowledged that while the Bank of Lithuania has broad discretion in evaluating whether a business plan ensures safe and sound banking, the court must still review whether that discretion was exercised lawfully.

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

09.2025

EU Court Upholds the Validity of the EU-U.S. Data Privacy Framework

LINK

Another attempt to block EU–US data transfers has failed. The EU General Court confirmed that the EU–US Data Privacy Framework remains valid, meaning companies can continue transferring personal data across the Atlantic without relying on alternative mechanisms such as Standard Contractual Clauses.

What was the case all about?

Philippe Latombe, a French citizen who uses various IT platforms that collect his personal data and transfer it to the United States, asked the General Court to annul the contested decision, arguing that the new US safeguards are insufficient: the Data Protection Review Court (DPRC) lacks independence, and US intelligence agencies continue bulk data collection without proper limits. According to Mr Latombe, the DPRC is neither impartial nor independent but dependent on the executive. Moreover, he submits that the intelligence agencies of that country of collecting bulk personal data in transit from the European Union without the prior authorisation of a court or an independent administrative authority is not circumscribed sufficiently clearly and precisely and is, therefore, illegal.

The General Court dismisses the action for annulment.

1. **The Data Protection Review Court (DPRC) was not impartial or independent but rather dependent on the executive.** The General Court concluded there are “several safeguards and conditions”, in particular those set out in Executive Order 14086 and the Attorney General Regulation (AG Regulation) that were sufficient to guarantee independence, impartiality and effective redress, in both the functioning of the DPRC and also in regard to the appointment and dismissal of judges.
2. **Bulk collection of personal data by US intelligence agencies is illegal.** The Court held that nothing in Schrems II requires bulk collection of personal data subject to prior judicial authorisation. Instead, the CJEU required that such collection be subject to ex post judicial review. Since under US law, intelligence activities are now subject to oversight by the DPRC, the General Court finds that it cannot be considered that the bulk collection of personal data by American intelligence agencies falls short of the requirements arising from Schrems II or that US law fails to ensure a level of legal protection that is essentially equivalent to that guaranteed by EU law.

French SA: Cookies placed without consent: SHEIN fined 150 000 000 EUR by the CNIL

LINK

In August 2023, the CNIL carried out an inspection of the website "shein.com". Based on its findings, the restricted committee - the CNIL body responsible for imposing sanctions - considered that INFINITE STYLES SERVICES CO. LIMITED had failed to comply with its obligations regarding cookies (Article 82 of the French Data Protection Act) and imposed a fine of 150 million euros on the company.

Cookies and advertisements inserted between emails: GOOGLE fined 325 million euros by the CNIL

LINK

The French data protection authority CNIL has imposed fines totalling 325 million EUR on Google LLC (200 million EUR) and Google Ireland Limited (125 million EUR) for breaching French rules on commercial prospecting and the use of cookies.

Interplay between the DSA and the GDPR: EDPB adopts guidelines

LINK

The European Data Protection Board (EDPB) has adopted **guidelines on the interplay between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR).** These are the first set of EDPB guidelines on the interplay between the GDPR and the EU’s recently adopted digital laws.

The DSA aims to complement the rules of the GDPR to ensure the highest level of protection of fundamental rights in the digital space. Its main goal is to create a safer online environment in which the fundamental rights of all users, including the right to freedom of expression, are protected. It applies to online intermediary services, such as search engines and platforms.

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 09.2025

ECOVIS ProventusLaw

The European Commission

LINK

On September 26th, the European Commission adopted its nineteenth package of restrictive measures against the Russian Federation. For the first time, the framework introduces direct prohibitions on the use of crypto-asset platforms by Russian residents, extending the scope of sanctions to cover digital financial services alongside traditional banking and payment infrastructures. The measures aim to curtail the role of crypto - assets in sanctions evasion, including past instances where Russian oil companies and other actors attempted to rely on Bitcoin or stablecoins such as Tether to bypass earlier restrictions.

In parallel, the package imposes restrictions on foreign financial institutions connected to Russia's alternative payment networks and blocks transactions linked to entities operating in Russian special economic zones. The new provisions build on earlier actions, including the designation of the Russian crypto-exchange Garantex, whose wallets were frozen by Tether in cooperation with EU sanctions enforcement. This package signals a decisive shift in the EU's strategy: the digital asset sector is no longer viewed as peripheral but as a central channel through which sanctions must be enforced, reflecting the Union's commitment to closing circumvention pathways and sustaining economic pressure on Russia.

European Council of the European Union

LINK

On 12 September 2025, the EU Council extended its individual sanctions against over 2,500 individuals and entities responsible for undermining Ukraine's territorial integrity, sovereignty, and independence.

These measures, initially imposed in response to Russia's military aggression, have been prolonged until 15 March 2026.

The sanctions include travel bans, asset freezes, and prohibitions on providing funds or economic resources to the listed parties. The EU remains prepared to intensify pressure on Russia, including through additional sanctions if necessary.

Detailed and full Regulatory Compliance report on Sanctions can be found here:
Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

09.2025

ECOVIS ProventusLaw

Employment Relationships Begin Before the First Day of Work – Key Points for Employers and Employees

LINK

Employment formally begins on the first day of work, but the most important decisions are made much earlier – during the recruitment process, when the employer evaluates candidates and the candidate assesses the job offer. The State Labour Inspectorate (VDI) emphasizes that the pre-contractual phase and the start of employment are crucial: transparency and fairness at this stage affect the quality of the entire employment relationship.

Responsibility for Non-Effectiveness of the Contract

The contract only becomes effective once the employee actually starts work.

- If the employee does not start work through no fault of their own, the employer must pay compensation of at least one month's salary.
- If the employee fails to start work due to their own fault and does not notify the employer at least three working days in advance, they must compensate the employer for damages, up to two weeks' salary.

VDI stresses that both parties must act responsibly to avoid last-minute withdrawals or delays that could cause losses.

Essential Agreements Before Starting Work

Before starting work, the employee and employer must agree on:

- Job role (position)
- Salary
- Workplace

Job descriptions can be detailed in internal regulations or job descriptions provided prior to starting work. Contracts should also specify working hours, contract type, and start date.

Failure to settle accounts with an employee can result in huge penalties – they may reach as much as 10,000 EUR

LINK

The State Labour Inspectorate (VDI) reports that in the first half of 2025, as in previous periods, the most frequent claims submitted to the Labour Disputes Commissions (DGK) operating at the VDI's territorial divisions were related to the recovery of wages and payments associated with it. In the first half of 2025, 7,724 such claims were received (compared to 7,360 in the first half of 2024), accounting for about 72.5% (compared to 75% in the first half of 2024) of all claims raised in applications submitted to the DGK during this period.

Working Time Accounting: What Employees on Flexible (Rotating) Schedules Need to Know

LINK

The State Labour Inspectorate (VDI) reminds employers and employees that workers with flexible (summarised) working hours must follow their approved work schedules.

- Work schedules must be communicated to employees at least 7 days before they take effect.
- Any changes to the schedule must be notified at least 2 working days in advance.

This means employers cannot unilaterally require employees to work additional hours that are not included in the approved schedule.

VDI Reminds: Psychological Violence (Mobbing) in the Workplace Is a Serious Misconduct Leading to Dismissal Without Notice

LINK

The State Labour Inspectorate (VDI) reminds that psychological violence (mobbing) is considered a gross violation of work duties, for which an employee may be dismissed without notice and without severance pay.

Although the Labour Code does not use the term mobbing directly, since 1 November 2022, the law has established a prohibition of violence, including psychological violence, and harassment. Violence includes any unacceptable behaviour intended to, or creating a risk of, causing physical, psychological, sexual, or economic harm, violating a person's dignity, or creating an intimidating, hostile, or humiliating environment.

Detailed and full Regulatory Compliance Update on Employment Regulation can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

CONSUMER PROTECTION

09.2025

ECOVIS ProventusLaw

Bank of Lithuania Legal and Licensing department

LINK

Bank of Lithuania updates complaint handling rules, invites comments

The Bank of Lithuania has published a draft amendment to the 2013 Resolution on complaint handling by financial market participants (FMPs). The changes expand the list of FMPs covered, clarify the definition of a complaint, and strengthen safeguards to ensure impartial and objective complaint review. Companies must allocate sufficient resources, provide regular staff training, and review compliance with the rules at least every two years.
The draft also modernises reporting: complaint data must be submitted from 2026 onwards in JSON format via the REGATA system, with new forms allowing classification by service type, nature, and cause. This will improve data quality and enable more effective supervision. Additionally, information on complaint procedures must be made accessible via remote service channels such as mobile apps. Payment and e-money institutions will transition from their current reporting framework to the updated rules.

Our recommendations:

Financial market participants should carefully analyse the draft amendments, particularly the operational impacts of new reporting formats, expanded data requirements, and staff training obligations. Institutions should assess whether current complaint-handling policies align with the clarified definitions and impartiality requirements. Given the consultation deadline of 3 October 2025, market participants are encouraged to submit remarks or proposals to the Bank of Lithuania to ensure practical implementation and proportionate compliance obligations.

State Consumer Rights Protection Authority

LINK

EU online dispute resolution platform shut down – businesses must update websites

As of 20 July 2025, the EU's Online Dispute Resolution (ODR) platform has been permanently closed under Regulation (EU) 2024/3228, which repealed Regulation (EU) No 524/2013. This means businesses engaged in e-commerce are no longer required to display links to the ODR platform on their websites or in their general terms and conditions.
The shutdown also entailed the deletion of all consumer dispute-related data stored on the platform. The State Consumer Rights Protection Authority (VVTAT) advises companies to review and update their online content, ensuring all references to the ODR platform are removed. Going forward, Lithuanian consumers with disputes should turn to VVTAT via the system www.vtis.lt. For purchases from other EU/EEA online shops, complaints should be submitted through the European Consumer Centre Lithuania (ecc.lt).

Our recommendations:

Businesses and their legal advisors should promptly revise website content, contractual terms, and consumer-facing documents to remove outdated references to the ODR platform. Compliance checks should be integrated into regular website audits to avoid misleading information. Companies should also update customer service protocols to direct consumers to the appropriate dispute resolution channels (VVTAT or ECC) and ensure staff are aware of the new process. This will safeguard compliance and reduce legal or reputational risks.

REGULATORY COMPLIANCE UPDATE

CRYPTO

09.2025

ECOVIS ProventusLaw

The Global Finance & Technology Network

LINK

According to the Global Finance & Technology Network's August 2025 report, crypto markets face accelerating risks of market abuse, making regulatory and institutional safeguards increasingly urgent. The findings note that manipulation tactics such as wash trading, pump-and-dump schemes, flash loan exploitation, and maximal extractable value practices are eroding market integrity and investor confidence.

In particular, the report highlights that those arranging or executing crypto trades must establish systems to prevent, monitor, and detect abusive practices, covering both on-chain and off-chain activity.

Regulators and market participants are urged to strengthen surveillance, improve transparency, and ensure international cooperation to address these evolving threats.

The European Central Bank

LINK

European Central Bank President Christine Lagarde has urged the European Union to close existing gaps in its stablecoin regulatory framework, warning that foreign issuers should not be allowed to operate in the EU without meeting the same prudential and transparency standards as EU-based firms.

Although the MiCA Regulation requires stablecoins to be fully backed, Lagarde highlighted that non-EU issuers may still gain market access without equivalent safeguards, creating potential risks to financial stability.

She cautioned that, in times of stress, investors might rush to redeem their holdings within the EU, where regulatory protections are stronger, placing pressure on domestic reserves. Christine Lagarde called for clear equivalence rules, robust cross-border asset safeguards, and stronger international cooperation to prevent regulatory arbitrage.

The Wolfsberg Group

LINK

The Wolfsberg Group published new guidance on how banks should manage financial crime risks when dealing with fiat-backed stablecoin issuers. It confirms that AML/CFT, sanctions, and anti-bribery standards apply just as strictly to stablecoins as to traditional finance, while highlighting blockchain-specific risks.

Banks providing operating, reserve, or settlement accounts must understand the issuer's business model, transaction flows, and governance, including their AML controls, sanctions screening, and blockchain analytics use. Wolfsberg clarifies that banks are not expected to monitor every on-chain transaction, but must ensure issuers operate within stated compliance standards.

Higher-risk issuers, especially those active in unregulated markets or linked to decentralised platforms, require deeper due diligence. The guidance also stresses proper reserve segregation, transparency, and coordination with regulators and law enforcement to enable quick action against suspicious or sanctioned activity.

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

Our recommendations and details are in this file

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

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:

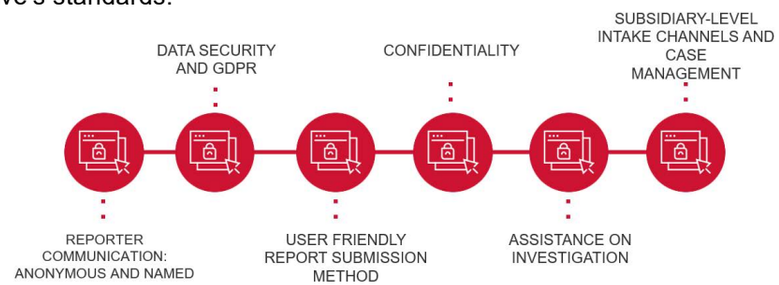
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors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