REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

03.2026

ECOVIS ProventusLaw

Ruling of the Supreme Administrative Court of Lithuania (LVAT); CJEU clarification (June 2025)

LINK

The Supreme Administrative Court of Lithuania (LVAT) confirmed that the Bank of Lithuania's practice of assessing violations and calculating financial penalties per each individual systematic violation is lawful, proportionate and consistent with EU law.

The case originated from a EUR 370,000 fine imposed in November 2020 on an e-money institution for eight AML/CTF violations. The Vilnius Regional Administrative Court partially upheld the institution's appeal in 2021, annulling two violations and reducing the fine. Both parties appealed to LVAT, which in late 2023 referred the matter to the Court of Justice of the EU (CJEU) for clarification on whether calculating penalties per each systematic violation is consistent with EU regulation. The CJEU issued its clarification in June 2025.

LVAT's extended panel, having regard to the CJEU ruling, found that the Bank of Lithuania had correctly classified the violations as serious and systematic, and that the sanctions imposed were individualised and did not exceed what is necessary to prevent money laundering and terrorist financing – i.e. compliant with the principles of effectiveness and proportionality.

LVAT upheld the Bank of Lithuania's appeal in full, restoring the original EUR 370,000 fine across all eight violations. The ruling is final and non-appealable.

This ruling is of major practical significance. Institutions should not assume that multiple AML/CTF breaches identified in a single inspection will be treated as one consolidated infringement – each systematic violation may attract a separate penalty, substantially increasing overall exposure. The Bank of Lithuania's approach has now been validated at both EU and national supreme court level.
Institutions are strongly advised to review their AML/CTF frameworks holistically, ensuring that monitoring, investigation and STR reporting processes are robust, well-resourced and properly documented.

Decision of the Bank of Lithuania (supervisory enforcement measure)

LINK

Following an inspection, the Bank of Lithuania revoked the e-money institution licence of UAB "PAYTEND EUROPE" due to serious and systematic violations in client relationship and transaction monitoring, AML/CTF risk management and internal controls.

Specifically: monitoring measures were insufficient to detect suspicious client activity; alerts were not always analysed timely or properly; internal investigations were conducted formally or incompletely; suspicious transaction reports were not filed with the Financial Crime Investigation Service (FNTT) even where grounds existed.

The institution lacked effective internal control procedures, clear separation of functions and adequate resources dedicated to AML/CTF. Control functions were not properly separated from business interests.

Furthermore, the institution provided false information to the Bank of Lithuania regarding a high-risk client relationship and failed to preserve and submit related correspondence.

Audited 2024 annual financial statements and other mandatory supervisory reports were not submitted within prescribed deadlines.

The institution was prohibited from providing any financial services as of 4 March 2026 and was required to notify clients within 5 business days.

This case represents the most severe supervisory outcome available. It demonstrates that cumulative failures across AML/CTF monitoring, internal governance, STR reporting, provision of accurate information to the regulator and timely submission of financial statements will result in licence revocation. All licensed payment and e-money institutions should treat this case as a benchmark and conduct a thorough review of their AML/CTF frameworks, internal audit processes and regulatory reporting obligations.

REGULATORY COMPLIANCE UPDATE

EMI, PI REGULATION

03.2026

ECOVIS ProventusLaw

Decision of the Bank of Lithuania Financial Market Supervision Committee

LINK

The Bank of Lithuania has recently confirmed the inclusion of UAB “EECO” and its payment solution into the public list of limited network exemption arrangements. The company provides a payment functionality integrated into electronic student ID cards (“E-wallet – Electronic Student Certificate Payment Function”), which has exceeded the EUR 1 million annual transaction threshold in Lithuania. Following notification, the regulator assessed that the solution qualifies for the limited network exemption under the Law on Payments of the Republic of Lithuania, and included it in the public register of exempted schemes.

Our recommendations:

Under the Law on Payments of the Republic of Lithuania, where the total value of payment transactions executed through a payment instrument in exceeds EUR 1 million over the last 12 months, the service provider is required to notify the Bank of Lithuania. In practice, however, this requirement should not be viewed merely as a formal threshold. Reaching or approaching this level should prompt a careful reassessment of whether the business model genuinely meets the criteria of the limited network exemption. Where there is any uncertainty adopting a proactive notification approach not only ensures compliance but also allows the Bank of Lithuania to assess the applicability of the exemption at an early stage. This can provide valuable regulatory comfort and reduce the risk that the activity is later reclassified as a regulated payment service requiring authorisation.

CCD II in the Baltic States 2026: Consumer Credit and BNPL Licensing Requirements

LINK

Transposing the EU Consumer Credit Directive II into national law

As every business seeking a consumer credit provider license adapts to the new requirements under CCD II, the Baltic consumer credit market is entering a period of significant regulatory change. Lithuania, Latvia, and Estonia are in the process of transposing the EU Consumer Credit Directive II into national law, introducing updated standards for consumer protection, creditworthiness assessments, advertising, and pre-contractual disclosures. CCD II expands the scope of regulated credit, including certain low- and high-value loans and buy-now-pay-later (BNPL) services. It also strengthens requirements for creditworthiness assessments, transparency in pre-contractual information, regulation of automated decision-making, advertising standards, staff competence, remuneration policies, and forbearance measures. Our legal team provides full support in navigating CCD II compliance, compliance, licensing, consumer protection, and fintech regulatory requirements in Lithuania, Latvia, and Estonia.

Resolutions of the Board of the Bank of Lithuania

LINK

The Bank of Lithuania has approved a new framework governing access to the TARGET-LIETUVOS BANKAS payment system.

The Framework sets out the requirements for non-bank financial institutions, such as electronic money and payment institutions, seeking to connect directly to the Eurosystem infrastructure. This development follows changes at EU level allowing national central banks to grant access to the TARGET system to non-bank payment service providers at their discretion. While this opens new opportunities for market participants, access is not automatic and is subject to strict eligibility criteria applied at national level.

while the possibility for non-bank institutions to access the TARGET system represents a significant step towards greater integration into core payment infrastructure, firms should approach this opportunity with careful preparation. Early engagement with the regulator, robust governance arrangements, and a clearly articulated AML/CFT framework will be key factors in successfully obtaining access.

Institutions wishing to apply for TARGET access may contact target2@lb.lt.

Resolutions of the Board of the Bank of Lithuania

LINK

Following the application of the Digital Operational Resilience Act (DORA) and its implementing EU legislation, the Bank of Lithuania has repealed certain national regulatory rules related to ICT risk management and incident reporting.As a result, the remaining provisions relevant to payment service providers and credit institutions have been consolidated into a new unified framework governing notifications to the Bank of Lithuania under the Law on Payments of the Republic of Lithuania. This reflects a broader shift towards harmonised EU-level regulation, where DORA now serves as the primary legal basis for ICT risk management and incident reporting obligations.

Detailed and full Regulatory Compliance Updates on Payments Systems Regulation can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

PERSONAL DATA PROTECTION AND ICT REGULATION

ECOVIS ProventusLaw

03.2026

EDPB publishes 2025 Report on Coordinated Enforcement Action

LINK

The European Data Protection Board (EDPB) has published its 2025 report focusing on the right to erasure under the General Data Protection Regulation (GDPR). This right, often known as the "right to be forgotten," allows individuals to request the deletion of their personal data under certain conditions. The report reveals that while many organisations have implemented processes to handle erasure requests, inconsistencies persist in how they are managed. Some data controllers struggle to balance the right to erasure with other legal obligations, such as compliance with retention requirements under tax or criminal law. The EDPB emphasises the importance of clear guidelines to ensure that the right to erasure is respected without undermining other legitimate interests.

Furthermore, the report identifies common obstacles, including difficulties verifying the requester's identity and technical challenges in deleting data from backup systems or third-party processors. It encourages organisations to adopt robust procedures and invest in technologies that facilitate efficient and secure data deletion.

EU Moves Forward with Single Entry Point for GDPR and Security Incident Reports

LINK

The European Parliament has highlighted progress toward creating a Single Entry Point (SEP) for security incident reporting across the European Union. This initiative is part of the European Commission's Digital Omnibus legislative package, aiming to simplify the process for organizations that need to report security incidents, including personal data breaches, under various EU laws. The SEP will be a centralized digital platform managed by ENISA, the EU Agency for Cybersecurity. It will allow organizations to submit incident notifications required by multiple EU regulations such as GDPR, NIS2, DORA, and the Cyber Resilience Act (CRA) through a single interface.

FC Barcelona faces 500,000 EUR GDPR fine over biometric data processing violations

LINK

Spain's data protection authority, the Agencia Española de Protección de Datos (AEPD), has imposed a €500,000 fine on Fútbol Club Barcelona (FCB) for failing to conduct a legally compliant Data Protection Impact Assessment (DPIA) before processing biometric data. The biometric data involved facial recognition and voice recordings collected during a 2023 digital census update campaign targeting approximately 143,000 club members. The AEPD found that the DPIA submitted by FCB did not meet the necessary GDPR standards, particularly lacking a clear description of biometric data, a genuine assessment of less intrusive alternatives, and an appropriate evaluation of risks. This case underscores the importance for organizations using biometric or high-risk technologies to prepare detailed, substantive DPIAs that honestly assess risks and alternatives.

Dutch DPA Warns of OpenClaw AI Security Risks

LINK

The Dutch Data Protection Authority (AP) warns users and organizations against the use of OpenClaw and similar experimental systems. The reason for this is the rapid pace at which OpenClaw has become popular. These types of open-source systems quickly fail to meet basic security requirements. The use of such experimental AI agents entails significant risks, such as data breaches and account takeovers. Security researchers worldwide have reported that, among other things, a significant portion of the available plugins on OpenClaw contains malware aimed at stealing login credentials or cryptocurrency, for example. Additionally, the platform is vulnerable to hidden commands in websites, emails, and chat messages. This can lead to account takeover, the extraction of personal data, and the theft of access codes.

Court Annuls 746 EUR Million GDPR Fine Against Amazon

LINK

The High Administrative Court of Luxembourg annulled a 746 million EUR fine imposed on Amazon by the Luxembourg Data Per EUR protection Authority (CNPD) for unlawful processing of personal data related to targeted advertising. The court confirmed that Amazon had violated several GDPR provisions, including the lack of a valid legal basis under Article 6(1)(f) GDPR for behavioral advertising and breaches of transparency and data subject rights. However, the court found procedural shortcomings in the CNPD's sanction decision, specifically the failure to assess fault and proportionality before imposing the fine.

Detailed and full Regulatory Compliance Updates 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 03.2026

ECOVIS ProventusLaw

Council of the EU Decision

LINK

The Council imposed restrictive measures on three entities and two individuals responsible for cyber-attacks against EU member states and partners under the EU horizontal cyber sanctions regime, which now applies to 19 individuals and 7 entities.

The newly listed parties are:
Integrity Technology Group (China) – provided products used to compromise over 65,000 devices across six EU member states between 2022 and 2023;

Anxun Information Technology (China) – provided hacking services targeting critical infrastructure of member states and third countries, along with its two co-founders;

and Emennet Pasargad (Iran) – gained unlawful access to a French subscriber database and advertised its contents on the dark web, compromised advertising billboards during the 2024 Paris Olympic Games to spread disinformation and compromised a Swedish SMS service affecting a large number of EU citizens.

All listed individuals and entities are subject to an asset freeze and travel ban; EU citizens and companies are prohibited from making funds or economic resources available to them.

OFAC Sanctions Advisory

LINK

OFAC issued an advisory on sham transactions used to evade sanctions, clarifying that nominal transfers of property by blocked persons do not terminate a blocked interest.

The advisory identifies red flags including transfers to family members or close associates, commercially unreasonable transactions, complex multi-layered structures in high-risk jurisdictions, continued involvement of the blocked person, and transfers close in time to a designation. OFAC cited enforcement actions against GVA Capital Ltd. ($215,988,868 penalty) and IPI Partners as examples of liability arising from dealings through proxy structures.

Council of the EU Decision

LINK

The Council added four individuals to the EU sanctions list under the framework targeting Russia's destabilising and hybrid activities, in particular Foreign Information Manipulation and Interference (FIMI):
Sergey Klyuchenkov (Russian propagandist and TV/radio host), Ernest Mackevičius (Lithuanian-born Russian state television news anchor), Graham Phillips (British-origin propagandist active in Russian-occupied Ukraine) and Adrien Bocquet (French-origin media figure and Kremlin propaganda amplifier).
All four are subject to an asset freeze and travel ban; EU citizens and companies are prohibited from making funds or economic resources available to them. The list now comprises 69 individuals and 17 entities.

Detailed and full Regulatory Compliance

Updates on Financial and Economic

Sanctions can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

03.2026

ECOVIS ProventusLaw

Ruling of the Supreme Court of Lithuania March 24, 2026, in Civil Case No. e3K-3-53-1120/2026

LINK

The Supreme Court of Lithuania clarified that an employee's duty of loyalty not to discredit the employer cannot be interpreted so broadly as to include an obligation to refrain from expressing personal beliefs on matters unrelated to the performance of job functions.

The Supreme Court of Lithuania ruled that the employee's statements, which led to the termination of the employment contract, were not related to his professional activities, as the employee expressed not the employer's but his own opinion on homosexuality in the context of medical science. No actual negative impact on the institution's reputation was proven in the case.

The Supreme Court of Lithuania clarified that the provisions of the Labor Code do not preclude the employer's right to recognize an employee's ethical violation as a gross breach of employment duties; however, an employee's right to express their beliefs may be restricted only to the extent necessary to safeguard the employer's interests related to the proper performance of work duties.

New VDI Requirement: Prevention Reports on Long Periods of Sitting and Standing at Work

LINK

VDI has reminded employers of their obligation to provide information on preventive measures aimed at reducing the risks associated with prolonged sitting and standing at the workplace.

A **thematic report on the prevention of prolonged sitting and standing at work was approved**, together with a **list of companies** subject to inspection via electronic means.

Supreme Court Case on Dismissal During Probation Period

LINK

A negative outcome of the probationary period essentially means that the employee does not meet the employer's job-related expectations, and therefore a certain degree of the employer's subjectivity is permitted when determining whether the employee is suitable for the agreed-upon work. The Supreme Court of Lithuania clarified that, in the event of a dispute regarding the legality of dismissal due to unsatisfactory probation results, the burden of proof on the employer should not be equated with cases where the employment contract is terminated at the employer's initiative due to the employee's fault, as this would negate the purpose of the probationary period as established by law. It is important that the employer be able to adequately justify his decision regarding the reasons why it considers the employee unsuitable for the specific job.

When reviewing a case regarding the legality of dismissal during the probationary period, the court must only verify whether the employer truly had sufficient grounds to conclude that the employee failed the probationary period, whether the employer did not abuse the right established by law, did not act unfairly toward the employee, and whether the employer provided reasons for concluding that the employee was unsuitable for the specific job (duties).

New VDI Guidelines: How to Act in Cases of Workplace Psychological Harassment

LINK

VDI has introduced two new guidelines - one for employees and one for employers - designed to provide clear, practical steps on what to do when facing psychological violence or harassment in the workplace. The guidelines for employees clearly outline where to seek help in cases of inappropriate behavior - when to approach the employer and when to contact VDI or the Labour Disputes Commission. They also emphasize the importance of collecting evidence and taking action without delay.

The employer-focused guidelines highlight that upon receiving a report of potential violence or harassment, immediate action is required. No later than within three working days, a commission must be formed or a responsible person appointed to conduct an investigation. The investigation must be objective, impartial, and prompt, with well-founded decisions communicated clearly to all involved parties.

VDI also notes that not every tense or unpleasant situation at work qualifies as psychological violence or harassment.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

INVESTMENT AND CRYPTO

05.2026

ECOVIS ProventusLaw

ESMA Publication ï Takeaways from the 2025 Call for Evidence on the Retail Investor Journey

LINK

ESMA published its takeaways from the 2025 Call for Evidence on the retail investor journey, outlining concrete actions to make investing more accessible for retail clients. ESMA will focus on three areas:(i) streamlining disclosure requirements and tackling information overload; (ii) reducing complexity in suitability and appropriateness assessments; and (iii) simplifying MiFID II requirements on sustainability preferences. Consumer testing will be used to validate improvements, including for mobile-first users. Stakeholder responses identified key barriers: disclosures are considered too long, too complex and not digital-first; suitability and appropriateness assessments are valued but seen as disproportionately burdensome, particularly for simple products and digital distribution channels; and the integration of sustainability preferences is viewed as overly complex. Non-regulatory barriers were also highlighted, including lack of trust, high fees, low financial literacy and complex cross-border taxation. The report will guide ESMA's future technical advice on MiFID II delegated acts and potential updates to its guidelines, in alignment with the final outcome of the Retail Investment Strategy (RIS). Financial market participants should monitor the forthcoming changes to MiFID II delegated acts and ESMA guidelines closely, as simplification of disclosure, suitability and sustainability preference requirements may require updates to internal processes, client-facing documentation and digital distribution channels. Institutions with mobile-first or digitally distributed products should pay particular attention, as ESMA's consumer testing work is likely to produce more prescriptive guidance on digital investor journeys.

Decision of the Bank of Lithuania (licence issuance under MiCA)

LINK

The Bank of Lithuania granted a crypto-asset service provider (CASP) licence to UAB Micar assets under MiCA. The Lithuanian-capital company intends to provide crypto-asset services to both retail and professional clients in Lithuania, including custody and administration of crypto-assets, exchange into funds or other crypto-assets, execution of orders and other related services. One of its shareholders is UAB FMĮ "Myriad capital", a licensed investment firm. UAB Micar assets is the fourth company to receive a MiCA CASP licence from the Bank of Lithuania, following Robinhood Europe, UAB, UAB "Decentralized" (Coingate) and Nuvei Liquidity UAB. Entities providing or intending to provide crypto-asset services in the EU should ensure they have obtained the appropriate MiCA authorisation, as operating without a licence exposes them to enforcement risk. Existing virtual asset service providers operating under transitional arrangements should monitor their authorisation timelines closely.

ESMA Q&A: Use of Nominee Structures in Crowdfunding

LINK

The European Securities and Markets Authority has clarified the regulatory treatment of nominee (fiduciary) structures in equity crowdfunding under the Regulation (EU) 2020/1503 (ECSPR). The key takeaway is that nominee structures are not prohibited as such, but their use is subject to strict conditions and transparency requirements. In particular, ESMA emphasises that such arrangements form part of the operation of a crowdfunding platform and must therefore be fully disclosed to the competent authority (In case of Lithuania – to the Bank of Lithuania), either at the authorisation stage or prior to implementation. From a practical perspective, the most important limitation relates to the principle that investment decisions must remain with the investor. Nominee structures may only be used after the investor has made a specific decision to invest in a particular project. Any structure that effectively intermediates or aggregates investments in a way that overrides or dilutes individual investor choice is unlikely to be compliant. .The firms must carefully assess whether the nominee arrangement involves elements of custody or safekeeping of financial instruments. Where this is the case, the entity acting as nominee may be required to hold an authorisation under MiFID or CRD frameworks, as custody services are a regulated activity. This creates a potential regulatory overlap risk, which must be addressed at structuring stage.

Consultation paper Draft Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders

LINK

ESMA/EBA Draft Guidelines on Suitability (Management Body & Key Function Holders)
The joint consultation paper issued by the European Securities and Markets Authority and European Banking Authority introduces updated draft Guidelines aimed at further harmonising the assessment of the suitability of management body members and key function holders across the EU financial sector. The Guidelines apply broadly to credit institutions, investment firms, and certain third-country branches, as well as to the competent authorities supervising these entities. In particular, they cover both members of the management body (executive and supervisory functions) and key function holders, including roles such as heads of internal control functions and chief financial officers.

Detailed and full Regulatory Compliance Update on Financial Instruments 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:

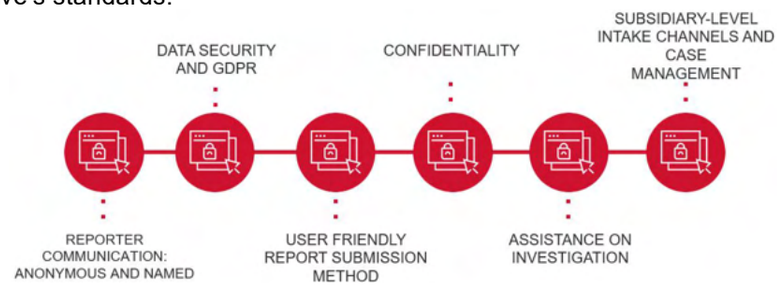
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors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