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

07.2025

ECOVIS ProventusLaw

The European Banking Authority (EBA)

LINK

The European Banking Authority has released its fifth biennial Opinion on money laundering and terrorist financing (ML/TF) risks, signalling a decisive shift in how financial crime vulnerabilities are emerging across the EU. The most notable trend is that risks linked to financial products and services have now surpassed those traditionally associated with customer profiles. Innovation is moving faster than the compliance frameworks meant to regulate it, leaving critical gaps in oversight, particularly in FinTech, crypto, and RegTech domains.

National supervisors are increasingly flagging FinTech as a high-risk area where basic AML controls are either inadequate or entirely missing. Many firms have adopted growth-first strategies, sidelining crucial compliance investments. The crypto sector continues to pose substantial risk, even as the number of authorised CASPs surges. Many providers still lack effective AML/CFT systems, with some operating at the regulatory margins or seeking to evade oversight altogether.

Between 2023 and 2024, regulators identified nearly 300 material compliance weaknesses stemming from unchecked reliance on automation, poor oversight of outsourced solutions, and a lack of internal capability to validate these technologies. The EBA also highlighted that the use of artificial intelligence has added complexity to fraud typologies, with deepfakes and synthetic identities now being deployed to defeat onboarding and monitoring systems.

Sanctions implementation is another area of vulnerability. Supervisors reported persistent weaknesses in how financial institutions screen for targeted individuals and entities, particularly in the context of instant payments and the use of aggregator cards or alternative payment channels that obscure fund origin. While supervisory activity has increased, especially in crypto, payment institutions, and electronic money institutions, the pace of compliance reform within firms remains inconsistent and reactive. The EBA's message is unequivocal: firms must not allow digital innovation to outstrip the controls needed to prevent abuse.

The European Banking Authority (EBA)

LINK

On 11 July 2025, the European Banking Authority released new responses to selected industry questions through its Q&A tool, clarifying interpretations under various EU regulatory frameworks, particularly PSD2 and supervisory reporting standards. Notably:

- The EBA reaffirmed that payment instruments, as defined under Article 4(14) of PSD2, encompass personalised devices and/or procedures used by a payment service user to initiate a payment order. The scope of what qualifies as a payment instrument depends on both functionality and contractual agreement with the provider.
- The EBA provided nuanced clarifications on whether electronic and paper-based postal transfers, particularly those integrated with postal operators' accounting systems, fall under PSD2. While postal transfers made electronically may be within PSD2 scope, paper-based instruments inherently linked to postal infrastructure might be excluded depending on how the services are structured and segregated from regulated payment services.
- The EBA addressed whether certain credit products are exclusive to consumers. The determination depends on the contract terms and intended availability. Products tailored exclusively to natural persons qualify as consumer credit, while those accessible to legal entities fall outside the scope of the Consumer Credit Directive.

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

07.2025

ECOVIS ProventusLaw

FAQ by the Bank of Lithuania

LINK

Q: Do the provisions of the Description of the Management Procedures, Internal Control Systems, and Client Funds Protection Requirements for Electronic Money Institutions and Payment Institutions (effective from January 1, 2026) mean that the boards of electronic money and payment institutions without a supervisory board, which perform supervisory functions assigned to the supervisory authority in this Description, must comply with the requirements set out in Article 33(6)(3) and (7) of the Republic of Lithuania Law on Companies?

A:, The Description does not require electronic money and payment institutions (hereinafter – Institutions) without a supervisory board to assign the functions prescribed in Article 34(11) of the Republic of Lithuania Law on Companies (Law on Companies) to the board, nor does it require applying the additional board composition requirements set out in Article 33(6)(3) and (7) of the Law on Companies related to the delegation of these functions.

The new Description does not regulate the allocation of supervisory functions under Article 34(11) of the Law on Companies among the Institution's bodies. References to the supervisory authority in certain points of the Description (e.g., points 22, 24, 35.1, 35.3, 37, 47, 49, 51, 56, and 57) should be understood as references to the Institution's board when there is no supervisory board, regardless of whether the board has been assigned the functions under Article 34(11) and irrespective of the additional composition requirements.

Therefore, when determining its governance structure, the Institution must evaluate whether the composition of the body allows it to perform the assigned functions and ensure compliance with legal requirements.

Event held by the Bank of Lithuania

LINK

The Bank of Lithuania held an event on the topic: **"Transition of Financial Market Supervision Reports to the REGATA System, Data Collection Updates, and Changes Related to the MiCAR Regulation."**

Key upcoming updates relevant to Electronic Money Institutions (EMIs) and Payment Institutions (PIs):

As part of the upcoming regulatory changes under the MiCAR framework, significant updates are being introduced to EMI/PI reporting requirements.

Timeline & Technical Details:

- Reports for periods ending by December 31, 2025 must be submitted via iAPS under current rules.
- New REGATA-based framework applies from January 1, 2026:
- Ad hoc reports begin submission via REGATA from January 1, 2026.
- First periodic REGATA submissions: 2026 Q1 reports.
- By June 30, 2026, all relevant institutions (except payment initiation and account information service providers) must submit report on major changes of requirements for safeguarding of funds of electronic money holders and/or payment service users (EM008_12) reflecting current status as of submission day.
- Reporting and system testing must begin no later than 2 months before the final deadline for report submission.
- Production environment access is granted no later than 1 month before the final deadline for report submission.

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

07.2025

ECOVIS ProventusLaw

Aspects of the Data Governance Act: trust in data sharing and public benefit

LINK

The State Data Protection Inspectorate (hereinafter – VDAI) draws attention to the fact that there are several European legal acts that are already in force and relate to the regulation of data processing, although they may not be known to part of the public. One such legal act is the Data Governance Act (Regulation (EU) 2022/868). The Data Governance Act (hereinafter – DGA) is intended to unlock the potential of data. Its goal is to promote trust in data sharing. This legal act introduces new requirements for companies that facilitate data exchange and aims to build trust among individuals and businesses regarding data: its availability, use, sharing, and re-use. It empowers people and organizations to control how their data is used. The Act also seeks to remove barriers that hinder the development of a strong, transparent, and fair data economy in Europe.

Targeted modifications of the GDPR: EDPB & EDPS welcome simplification of record keeping obligations and request further clarifications

LINK

The European Data Protection Board (EDPB) and European Data protection Supervisor (EDPS) issued a Joint Opinion on the European Commission's Proposal for a Regulation amending certain regulations, including the GDPR. The European Commission has put forward a proposal aimed at simplifying GDPR compliance and reducing administrative burdens. One key change is the expansion of the exemption under Article 30(5) GDPR, which currently relieves companies with fewer than 250 employees from keeping records of processing activities. Under the new proposal, this exemption would apply to companies and organisations with fewer than 750 employees, unless the data processing is likely to result in a high risk to individuals' rights and freedoms (as per Article 35 GDPR).

VDAI ruling: implementation of the principle of transparency (GDPR Article 5(1))

LINK

In a recent decision, the State Data Protection Inspectorate (hereinafter – VDAI) found UAB "TELE2" (hereinafter – the Company) in breach of the General Data Protection Regulation (hereinafter – GDPR) for failing to properly inform customers about the processing of their personal data during creditworthiness assessments.

The investigation was initiated after receiving two complaints. In the first, a customer (Complainant 1) reported that following phone conversations with TELE2 on April 29 and May 7, 2024, regarding number porting, his personal data was checked in a third-party credit database without his knowledge or consent. The company later acknowledged that its employee had failed to inform the customer due to a mistake and committed to implementing additional technical solutions to ensure proper notification in the future.

While TELE2 justified the processing of data based on its legitimate interest in mitigating financial risk (under Article 6(1)(f) of GDPR), the Inspectorate emphasized that individuals must still be clearly informed of such data processing and their right to object, as outlined in Article 21 of the GDPR.

Information by State Data Protection Inspectorate (VDAI)

LINK

The State Data Protection Inspectorate (hereinafter referred to as the ''VDAI'') receives reports from the public on various instances of disclosure of personal data in possible breach of the General Data Protection Regulation (hereinafter referred to as the ''GDPR''), both in the public and the private sector. Such reports are also received in relation to the publication of information by journalists or other producers and disseminators of public information. VDAI points out that such processing is subject to the requirements for lawful processing of personal data under the GDPR. According to the GDPR, personal data may only be processed (and thus made public) in accordance with the principles relating to the processing of personal data as set out in Article 5 of the GDPR and where such processing can be justified on the basis of at least one of the conditions for the lawful processing of personal data as set out in Articles 6 or 9 of the GDPR.

The Helsinki Statement on enhanced clarity, support and engagement

LINK

The European Data Protection Board (EDPB) adopted a landmark Statement on enhanced clarity, support and engagement. The Statement outlines new initiatives to make GDPR compliance easier, for micro, small and medium organisations, strengthen consistency and boost cross-regulatory cooperation. The EDPB will launch a series of direct and practical resources to simplify GDPR application.

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 07.2025

ECOVIS ProventusLaw

The European Council of the European Union

LINK

On 18 July 2025, the Council of the European Union adopted its 18th package of economic and individual sanctions against Russia in response to its ongoing war of aggression against Ukraine. This latest package, one of the most comprehensive to date, significantly expands restrictions on Russia's energy sector, financial institutions, military supply chains, and circumvention networks operating through third countries. The package entered into force upon publication in the Official Journal on 19 July 2025. Key developments include a reduction in the crude oil price cap from USD 60 to USD 47.60 per barrel, the introduction of a dynamic price adjustment mechanism, and a new import ban on petroleum products refined from Russian crude oil, even if processed in third countries. Transactions involving the Nord Stream 1 and 2 pipelines are also prohibited. In the financial sector, 22 additional Russian banks have been subjected to full transaction bans, extending the total to 45. The measures further apply to foreign financial institutions and crypto-asset service providers that facilitate sanctions evasion, including those using Russia's SPFS messaging system. The EU also imposed an expanded ban on the export of financial software and infrastructure critical to the Russian banking system, with a wind-down period for existing contracts until 30 September 2025. Anti-circumvention provisions were strengthened, with new export controls on dual-use and military-grade goods and a catch-all clause requiring prior authorisation for the export of sensitive technologies, even when routed through non-EU countries. A total of 105 additional vessels were added to the sanctions list for their role in the maritime shadow fleet used to evade oil restrictions, bringing the total number of designated ships to 444.

The UK's Office of Financial Sanctions Implementation (OFSI)

LINK

On 21 July 2025, the UK's Office of Financial Sanctions Implementation (OFSI) published its first dedicated threat assessment on the crypto-assets sector, covering activity from January 2022 to May 2025. OFSI concluded that the sector remains materially exposed to sanctions evasion risks and is underperforming in detection and reporting obligations.

The assessment confirms that the use of anonymity-enhancing technologies, complex transaction layering, and cross-jurisdictional exposure increases the risk of direct or indirect engagement with sanctioned individuals or entities, particularly in relation to Russia, North Korea, and Iran. Firms often fail to identify ultimate beneficiaries or to trace digital asset flows beyond superficial transaction history.

OFSI also noted significant underreporting of frozen assets or breaches under Regulation 70 of The Russia (Sanctions) (EU Exit) Regulations 2019, raising concerns that many UK-based crypto firms may not fully understand or operationalise their sanctions compliance obligations.

OFSI reiterates that crypto-asset firms are subject to the same legal obligations as traditional financial institutions, including asset freezing, reporting, and the application of risk-based due diligence, and are expected to apply more advanced monitoring and blockchain analytics to detect indirect exposure and emerging evasion typologies.

The European Council of the European Union

LINK

On 15 July 2025, the Council of the European Union imposed restrictive measures against nine individuals and six entities linked to Russia's hybrid operations targeting the EU and Ukraine. The designations, aligned with the EU's October 2024 framework on hybrid threats, address activities involving disinformation, interference in democratic processes, and disruption of communications. Sanctioned entities include the Russian Television and Radio Broadcasting Network and senior officials responsible for replacing Ukrainian broadcasts with Kremlin-controlled content in occupied areas. Measures also target the 841st Separate Electronic Warfare Centre and related personnel implicated in GNSS signal interference affecting civil aviation across the Baltic region. Additional listings cover Russian influence and propaganda organisations linked to Yevgeny Prigozhin and Aleksandr Dugin, as well as individuals involved in GRU operations and the dissemination of pro-Russian content via online platforms. All designated persons and entities are subject to asset freezes, travel bans, and restrictions on access to EU financial and economic resources.

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

07.2025

ECOVIS ProventusLaw

EBA (European Banking Authority)

LINK

EBA moves to tackle greenwashing through revised product governance guidelines

As ESG products proliferate in retail banking, the European Banking Authority is consulting on updated governance rules to combat greenwashing and strengthen business conduct. The revisions aim to enhance product oversight without imposing undue burden on financial institutions.

To address the increasing risks of greenwashing in the retail banking sector, the European Banking Authority (EBA) has launched a consultation to revise its Guidelines on Product Oversight and Governance (POG) arrangements. The proposed updates clarify existing requirements for ESG-featured products, aiming to protect consumers from misleading practices and ensure compliance with evolving conduct standards. The revisions focus on select areas, including internal controls, target market assessment, and product distribution, with an emphasis on maintaining a proportionate regulatory approach. These changes are driven by findings from the EBA's 2024 report on greenwashing and align with recent updates to the Capital Requirements Directive and Regulation. The final guidelines are expected by Q1 2026 and will apply from 1 December 2026.

BoL (Bank of Lithuania)

LINK

Lithuanian central bank finds persistent legal gaps in payment service contracts

While most electronic money and payment institutions have improved consumer contracts in response to regulatory scrutiny, key deficiencies remain, particularly in areas of liability, contract changes, and clarity of terms.

Following a re-assessment of electronic money institutions (EMIs) and payment institutions (PIs), the Bank of Lithuania found that although all nine institutions under review made changes to their consumer payment service agreements, not all fully addressed previously identified issues. The review, based on compliance with Law on Payments of Republic of Lithuania, showed varying levels of conformity. Three institutions met 87% of the legal requirements, while others showed partial or significant non-compliance. Common weaknesses included clauses on liability for payment execution, contract modification or termination, and the overall clarity of contract language. In one institution, over half of the clauses were found non-compliant. The Bank of Lithuania will continue engaging with non-compliant institutions to ensure full alignment with legal standards and improved consumer transparency.

BoL (Bank of Lithuania)

LINK

Financial institutions improve payment service experience, but gaps in fraud response and transparency remain

Lithuania's financial institutions report better compliance with consumer protection expectations, but persistent issues in fraud procedures, payment clarity, and service accessibility highlight the need for structural improvements.

According to a 2025 follow-up survey by the Bank of Lithuania, financial institutions now fully meet 91% of regulatory expectations related to the quality of payment services – a slight improvement from the previous year. However, challenges remain in critical areas such as fraud-related processes, communication on reserved funds, clarity on payment limits, and transparency when third-party service providers are involved. Notably, 24% of institutions report only partial compliance with fraud-related payment trace and recall procedures. The lack of 24/7 support lines, opaque dispute processes, and unclear legal relationships with third-party intermediaries contribute to continued customer dissatisfaction. While institutions show high compliance in AML/CTF measures and KYC practices, delayed customer support in risk scenarios (e.g., account blocks) continues to cause frustration.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

07.2025

ECOVIS ProventusLaw

Strict Liability for Illegal Employment: €1,500 Fine Upheld for Labour Code Breaches

LINK

The State Labour Inspectorate (VDI) fined the director of UAB "L." €1,500 for employing third-country nationals without proper permits and failing to notify Sodra on time. The District Court upheld the penalty, confirming that intent is not required for administrative liability.

The violations included:

- Failure to notify Sodra at least one day before employing a Belarusian national, despite a signed employment contract.
- Employment of another Belarusian citizen without a valid work permit, in a position not included in the shortage occupation list.
- Allowing both individuals to work without valid permits and without new contracts during certain periods.

Our recommendations:

To avoid similar sanctions, employers should:

- Verify permits before employment: Ensure that all third-country nationals (non-EU citizens) have valid Lithuanian work permits.
- Submit Sodra notifications on time: Notify Sodra at least one day prior to the start of employment. Late notifications—even if accidental—can trigger fines for illegal employment.
- Understand strict liability rules: Courts may impose fines even for administrative or procedural errors. Lack of intent or minimal harm is not a defence.

Administrative liability for illegal employment is strict and formal—minor mistakes can have real consequences.

Article 52 of the Labor Code - the right to disconnect

LINK

The Lithuanian Parliament is considering Labour Code amendments that would grant employees an explicit right to be unavailable outside working hours, applying to both remote and on-site workers. The measure aims to counter the growing issue of digital overconnectivity, ensuring that rest periods remain free from work obligations and preventing unpaid overtime. Inspired by similar laws in France, Belgium, and Italy, the proposal reflects ongoing EU-wide efforts to safeguard work-life balance in modern, technology-driven workplaces.
Regardless of whether or when the legislative initiative is adopted, employers are advised to proactively regulate after-hours communication to reduce legal risks and foster a healthy work culture. Clear internal rules not only help to ensure compliance with with labour law requirements, but also improve employee satisfaction and reduce burnout.

Our recommendations:

1. Establish or update internal policies (e.g., Work Rules, Remote Work Policy, Communication Policy)
2. Discourage routine after-hours communication
3. Design handover procedures for employee absences
4. Educate employees on their rights.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

CRYPTO

07.2025

ECOVIS ProventusLaw

The Bank of Lithuania

LINK

On 1 August 2025, the Bank of Lithuania reiterated that cryptocurrency service providers which do not intend to obtain a licence under MiCA Regulation must ensure a timely and structured wind-down of their operations. Operators listed in the national registry who plan to cease activities are urged to begin immediate client outreach and asset offboarding, with clear communication regarding service termination timelines and procedures for withdrawing or converting crypto-assets. The Bank underlined that after the transition period ends on 31 December 2025, the provision of any crypto-asset services without appropriate authorisation will constitute illegal financial activity, potentially triggering criminal liability and enforcement action, including website blocking. To safeguard client funds and uphold regulatory integrity, operators must prioritise the full return of customer assets, whether in fiat or crypto, and maintain open, multi-channel communication throughout the process. The Bank has also committed to publishing the names of unauthorised providers and referring suspected criminal breaches to law enforcement. Although over 370 entities are registered, only 120 demonstrate active operations, while only 30 have formally initiated the MiCA licensing process.

The Bank of Lithuania

LINK

On 11 June 2025, the Bank of Lithuania clarified that CASPs intending to offer services involving electronic money tokens (EMTs) must also obtain a payment institution licence under a simplified licensing regime. This requirement, effective no later than 1 March 2026, applies to both custodial and transactional operations involving EMTs, which are legally classified as payment services when executed on behalf of customers. EMT-related transfers or wallets that allow movement of tokens to or from third parties fall under payment regulation and trigger additional licensing and capital requirements. Applicants must submit a dedicated licence application, a business programme, and a business plan that includes a separate section on EMT-related operations. In addition, they must provide three-year capital and financial projections, distinguishing EMT transaction volumes from other crypto services. The Bank of Lithuania stressed that the simplified process does not exempt applicants from supervisory scrutiny, particularly in cases where multiple financial services are provided under a single corporate entity. In such cases, applicants may be required to establish separate legal entities to isolate EMT-related activity.

The European Securities and Markets Authority

LINK

The European Securities and Markets Authority has introduced Final Guidelines establishing minimum standards for knowledge and competence among staff involved in providing crypto-asset services under the MiCA framework. The requirements apply to individuals delivering either information or advice on crypto-assets. Staff providing general information must have completed at least 80 hours of training or possess one year of supervised experience. Those advising clients are subject to stricter requirements, including 160 hours of training or equivalent qualifications, such as a relevant university degree. Ongoing professional development is also required: a minimum of 10 hours annually for information providers and 20 hours for advisers. Staff with at least one year of relevant experience may be deemed competent if the CASP can document their qualifications. Individuals who have not yet met the full requirements may interact with clients under supervision for a transitional period of up to four years.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

CORPORATE

07.2025

ECOVIS ProventusLaw

Corporate Law Reform – Key Amendments Effective 1 July 2026

LINK

On 30 June 2025, the Lithuanian Parliament adopted significant amendments to the Law on Companies, introducing measures designed to enhance corporate governance, enable more flexible capital structuring, and modernize investment frameworks.

Key changes include:

- **Redeemable Shares:** Legal framework introduced for time-limited shares with structured redemption mechanisms.
- **Financial Assistance**: Clear regulation of loans and guarantees for share acquisitions under strict safeguards.
- **Management Powers:** Boards and CEOs to gain authority for capital increases and interim dividend decisions.
- **Procedural Simplifications:** Extended deadlines for financial statements, shorter notice periods for electronic meetings, eased dividend distribution rules, and streamlined liquidation procedures.
- **Board Elections:** Updated re-election rights and flexible commencement dates for board members.

Postponement of Corporate Sustainability Reporting Requirements Approved

LINK

June 25, 2025, the Parliament approved the Law on Reporting of Companies and Groups Companies and the Law on Securities, both prepared by the Ministry of Finance. These laws implement a two-year postponement for certain companies to include sustainability information in their governance reports.

These legislative changes transpose the Stop-the-Clock Directive, adopted on 16 April 2025, which delays the deadlines for corporate sustainability reporting obligations. Under the new rules:

- Large companies (with more than 250 employees, including both public and private limited liability companies, state-owned and municipal companies, and parent companies of large groups) will be required to include sustainability information in their governance reports starting from 2027, instead of 2025.
- Medium-sized and small listed companies will be subject to this requirement from 2028, instead of 2026.

It is estimated that over 200 companies will be affected by these changes.
The requirement to include sustainability information remains in force for large listed companies, banks, and insurance undertakings with over 500 employees. These entities have already reported sustainability information for 2024. Approximately 20 such companies operate in Lithuania.
The amendments also:

- Fully transpose the EU directive requiring third-country parent companies to publish their corporate income tax reports on the subsidiary's website for at least five consecutive years, and to submit them to the data processor of the Register of Legal Entities.
- Exempt parent companies of medium-sized groups (that do not include public-interest entities) from the obligation to prepare consolidated financial statements and consolidated governance reports. This applies to approximately 80 such groups in Lithuania.
- Introduce more flexibility for exemptions from preparing consolidated financial statements and governance reports when these are prepared by the ultimate parent company of a group.

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:

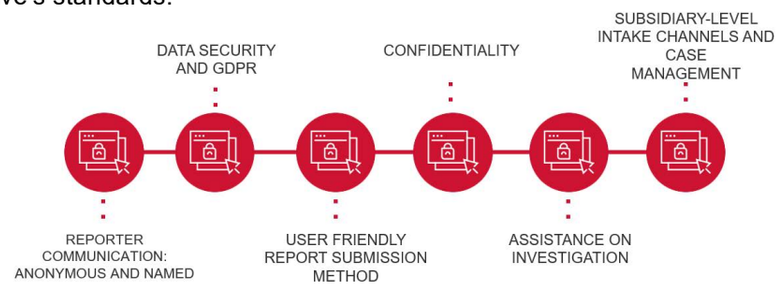
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors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