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

08.2025

ECOVIS ProventusLaw

The Center of Excellence in Anti-Money Laundering

LINK

On 3 September 2025, the Center of Excellence in Anti-Money Laundering is organising a one-day online training session titled “Implementation of a Risk-Based Approach to Ensure Financial Inclusion.” The programme will focus on the practical application of the risk-based approach in AML/CFT, highlighting how both public and private sector entities can adopt such methodologies to promote financial inclusion.
Participants are required to register by submitting their full name (accurately, if a certificate of completion is requested), contact details, organisation, and sector (e.g. bank, crypto service provider, law firm, fintech, supervisory authority, etc.).

The Wolfsberg Group

LINK

The Wolfsberg Group released Part II of its Statement on Effective Monitoring for Suspicious Activity: Transitioning to Innovation. The paper stresses that legacy rules-based monitoring has reached its limits and financial institutions must embrace innovative, technology-driven approaches. Supervisors, particularly in the United States, are encouraging the responsible adoption of AI and machine learning to strengthen detection.

The Wolfsberg Group emphasises that success should be measured not by alert volumes but by the precision, recall, and quality of suspicious activity reports, with transparency and explainability remaining non-negotiable. Institutions are urged to balance model risk against financial crime risk, recognising that even imperfect models may uncover threats missed by traditional systems. A hybrid approach, combining rules, supervised and unsupervised methods, is recommended to cover both established and emerging risks.

FATF

LINK

In August 2025, the Financial Action Task Force (FATF) published Annexes A–C to its Money Laundering National Risk Assessment (NRA) Toolkit, designed to support jurisdictions in conducting robust, focused ML/TF risk assessments. Annex A comprises quick-reference guides for notoriously challenging areas, namely corruption, virtual assets and VASPs, legal persons and arrangements, and the informal economy, all highlighted due to their cross-border nature, data limitations, and rapidly evolving typologies. Annex B offers comparative insights on predicate offences like fraud, corruption, drug trafficking, and tax crime, frequently cited across jurisdictions and useful for prioritisation.
Annex C compiles practical NRA methodologies from the World Bank, IMF, and Council of Europe, including self-assessment tools, heatmaps, and sector-specific modules that governments may adapt for their own assessments.

Together, these annexes aim to help jurisdictions overcome resource and data constraints while maintaining focus on both domestic and international ML threats.

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

08.2025

Small and medium-sized businesses can choose both individual payment services and service bundles

LINK

The Bank of Lithuania, aiming to support small and medium-sized enterprises, publishes on its website the fees for payment services intended for this sector. This information helps save time and choose the most optimal service options.

The Business Payment Services Fee Comparison Website provides information designed to meet a variety of business needs. It allows users to compare fees for payment service plans, account management, executed and received payments, business cards, cash operations, as well as card and online payment acceptance services.

The website lists fees from more than 30 banks, credit unions, payment and electronic money institutions that provide payment services to businesses in Lithuania. By viewing various payment service providers' offers in one place, small and medium-sized enterprises (SMEs) can choose the services they need and select one or more providers.

You can find the Business Payment Services Fee Comparison Website here.

Decisions of the Financial Market Supervisory Committee

LINK

The Bank of Lithuania has published the 2024 overview of electronic money and payment institutions' activities. The report provides information on the sector's structure, key developments, participants and their financial results, supervisory actions, and other matters relevant to the sector.

At the end of 2024, the 119 electronic money and payment institutions operating in Lithuania served 2.2 million active clients (30% more than at the end of 2023). Licensed activity revenues of the sector increased by 15%, reaching EUR 571 million, while profit more than doubled to EUR 40.2 million.

The full overview of electronic money and payment institutions' activities can be accessed here.

Decisions of the Financial Market Supervisory Committee

LINK

The Bank of Lithuania, having reviewed the submitted application and information, has granted UAB Bondea a license to operate as a crowdfunding service provider.

Under the Crowdfunding Regulation, the company will be authorized to provide the following crowdfunding services: intermediary services in granting loans, and distributing transferable securities or instruments issued by project owners or special purpose companies for crowdfunding purposes, without the obligation to subscribe them; accepting and transmitting orders related to transferable securities and instruments. The company will also be able to apply credit scoring to crowdfunding projects, propose their pricing, and set interest rates.

Currently, 16 companies in Lithuania hold a crowdfunding service provider license – making Lithuania the fifth in the European Union by this indicator.

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

08.2025

ECOVIS ProventusLaw

Personal Data Security Breaches in Lithuania – H1 2025

LINK

The State Data Protection Inspectorate (VDAI) received 116 reports of personal data breaches (PDBs) in Lithuania in the first half of 2025, affecting 168,822 data subjects.

Breach types:

- Confidentiality breaches: 86%
- Integrity breaches: 2%
- Availability breaches: 10%
- Not considered a PDB: 2%

Causes:

- Human error: 57%
- Other causes (IT system errors, programming issues, etc.): 11%

Cyber incidents: 32%

- 8 cases: ransomware/encryption attacks
- 10 cases: unauthorized access
- 10 cases: social engineering attacks
- 3 cases: login/“brute force” attacks
- 2 cases each: SQL injection & system disruptions

VDAI 2024: Overview of Personal Data Protection Supervision

LINK

The State Data Protection Inspectorate (VDAI) has published its 2024 activity report, presenting the institution's priorities, achievements, and future goals.

Activity Priorities:

Priority 1. Strengthening the prevention of personal data protection violations and contributing to increasing trust in the public sector.

Priority 2. Strengthening international cooperation in the field of personal data protection.

In 2024, the State Data Protection Inspectorate (VDAI) carried out 12 inspections (compared to 46 in 2023 and 44 in 2022), including some unplanned checks.

Growth in Amicable Complaint Resolution

In 2024, 52 complaints were resolved amicably, exceeding the planned target (3%) with an 11% increase compared to the previous year. Since the introduction of this practice in 2022, amicable resolutions have grown by 93%.

Protect Your Email: Practical Recommendations from NKSC

LINK

The National Cyber Security Centre (NKSC) at the Ministry of National Defence continues its series of practical cybersecurity recommendations and has released the second document, aimed at helping organizations protect email – one of the most vulnerable digital services. These recommendations are especially relevant for very small, small, and medium-sized enterprises (SMEs), which often lack even basic security measures or have them improperly configured.

Our recommendations:

Protect your organization from email-based attacks by enabling SPF, DKIM, and DMARC authentication, using strong passwords and multi-factor authentication, and providing regular employee training. Test your defenses with phishing simulations and regularly review email configurations.

You can also check your domain’s security for free using NKSC’s tool: **https://sauguspastas.nksc.lt.**

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 08.2025

ECOVIS ProventusLaw

The White House

LINK

On 6 August 2025, the President confirmed the continuation of the national emergency declared under Executive Order 14066, citing the Russian Federation's destabilising actions against Ukraine as an ongoing and extraordinary threat to the national security and foreign policy of the United States. In this context, the Executive Order introduces an additional 25 percent ad valorem tariff on imports from India that are directly or indirectly linked to Russian-origin oil. The measure is adopted pursuant to U.S. trade and national security authorities, including the International Emergency Economic Powers Act, the National Emergencies Act, and the Trade Act of 1974.

The Order authorises the Secretaries of State, Treasury, Commerce and other senior officials to oversee compliance, evaluate the effectiveness of the sanctions, and recommend further actions as required. The new duty will take effect 21 days from issuance, subject to limited exemptions for goods already in transit prior to 17 September 2025.

European Council of the European Union

LINK

On 16 August 2025, European leaders including President Macron, Prime Ministers Meloni and Starmer, Chancellor Merz, President von der Leyen and others issued a joint statement in response to the Alaska summit between Presidents Trump and Putin. The leaders welcomed President Trump's expressed commitment to pursue peace in Ukraine but emphasised that any further negotiations must include President Zelenskyy and involve European partners.

They reaffirmed their unwavering support for Ukraine's sovereignty and rejected any peace arrangement that would legitimise territorial changes by force or grant Russia a veto over Ukraine's future membership in the EU or NATO. The statement also confirmed their determination to maintain sanctions and economic pressure on Russia's war economy until a just and durable peace is secured.

European Council of the European Union

LINK

On 11 August 2025, the European Union's High Representative announced that Albania, Bosnia and Herzegovina, Iceland, Liechtenstein, Montenegro, North Macedonia, Norway, and Ukraine have aligned with the EU's 18 July 2025 Council Decision (CFSP) 2025/1471, which introduces additional restrictive measures in light of Belarus's role in Russia's aggression against Ukraine. These new measures include expanded export controls, such as optional requirements for prior authorisation when Belarus may be the end destination or end user, and an extended ban on specialised financial messaging services to certain Belarusian credit institutions now elevated to a full transaction ban. The Decision also significantly broadens the scope of goods and technologies subject to export and transit restrictions due to their potential contribution to Belarus's military or industrial capacity.

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

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

08.2025

ECOVIS ProventusLaw

How to Prove Psychological Harassment at Work: Key Evidence and What Employees Need to Know

LINK

Psychological harassment at work is a serious violation of labor law that must be properly identified and documented to ensure an objective investigation. A verbal complaint alone is not sufficient – concrete evidence is required to assess the factual circumstances of the harassment.

When investigating complaints or requests regarding harassment, VDI considers all available information, including the victim's explanation, contextual factors, witness statements, and possible documentary or technical evidence. The clearer and more detailed the evidence provided, the more effectively the situation can be investigated and appropriate measures taken.

Employees who believe they are experiencing psychological harassment or bullying are advised to actively and consciously gather all possible evidence. Important details include not only actions or words but also the context: when, where, and under what circumstances the behavior occurred, whether there were witnesses, and whether the behavior was repeated. Useful evidence can include:

- Saved SMS messages or emails
- Records of work meetings or conversations
- Photos
- Witness statements
- Internal documents indicating indirect signs of harassment.

Repayment of Training Costs: What Employers Need to Know

LINK

Increasingly, employers face situations where they invest in an employee's professional development, cover expensive training, and the employee leaves shortly afterward. Can an employer legally reclaim training costs or deduct them from wages? The State Labour Inspectorate (VDI) clarifies when this is permitted.

Deductions – Only in Cases Defined by Law

Article 150 of the Labour Code lists the limited cases where deductions from wages are allowed. Employers cannot arbitrarily decide what amounts to deduct. Permitted deductions include:

- Refund of employer-provided but unused funds
- Repayment of overpayments caused by calculation errors
- Compensation for damage caused by the employee's fault
- Repayment of unused leave if the employment contract is terminated by the employee without valid reasons or due to the employee's fault initiated by the employer

This means training costs not listed above cannot be deducted from wages.

Avoid Mistakes Before Your Employment Begins: What You Need to Know Before Starting Work

LINK

The State Labour Inspectorate (VDI) reminds employers and employees that employment relationships start even before the employment contract is signed. Clear job postings, honest communication, and proper discussion of essential terms are the first steps toward sustainable employment built on mutual trust.

Clear Job Postings – The Start of Transparency

Employers must include the salary or salary range in all job postings, whether hourly, monthly, or fixed component of the position. Failure to indicate compensation is not only a legal violation but also undermines trust in the employer.

Pre-contractual Relationships – Responsibility for Both Parties

Even before employment begins, the law imposes fundamental duties: gender equality, non-discrimination, fairness, provision of necessary information, and confidentiality. Employers' responsibility starts when a job is posted, so careless statements or actions may lead to disputes. Clear selection procedures should be established and strictly followed.

Essential Employment Contract Terms

A contract is valid only when both parties agree on:

- Job role
- Compensation
- Workplace

The contract must be in writing, in two copies, with one copy for the employee. Employers must notify the State Social Insurance Fund Board (Sodra) at least one day before the employee starts work.

Working Hours, Probation, and Other Agreements

Working hours must be clearly defined without vague terms such as "at least" or "from–to."

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

08.2025

ECOVIS ProventusLaw

The Financial Action Task Force (FATF)

LINK

On 22 August 2025, the President of the Financial Action Task Force (FATF) addressed the United Nations Security Council, emphasising the persistent and evolving threats of terrorist financing.

A particular focus was placed on the increasing abuse of virtual assets by terrorist groups, with evidence that some organisations are systematically leveraging such technologies, using obfuscation techniques, and shifting toward alternatives promoted as more private and secure.

FATF reporting highlights that in 2024, ISIL-K made extensive use of virtual assets for organisational transfers and for collecting international donations. To mitigate these risks, the updated FATF Standards provide enhanced tools for governments and the private sector to monitor developments in the virtual asset sector and to identify potential terrorist financing activity concealed within such transactions.

The FATF President called for full and consistent global implementation of these standards, stronger cooperation between jurisdictions, and closer engagement with the private sector to disrupt the misuse of crypto-assets for terrorist purposes.

Leading global trade associations

LINK

On 19 August 2025, nine leading global trade associations, including the Global Financial Markets Association (GFMA), the Institute of International Finance (IIF), the International Swaps and Derivatives Association (ISDA), and the Futures Industry Association (FIA), jointly submitted a letter to the Basel Committee on Banking Supervision (BCBS) urging a pause in the implementation of the Crypto-asset Exposures Standard (SCO60).

The associations argue that the current framework is outdated, overly restrictive, and risks pushing crypto-asset activities outside the regulated banking sector. They highlight that the rules, scheduled to take effect in 2026, impose punitive capital requirements that make banking engagement with crypto-assets prohibitively expensive, while failing to reflect recent market developments in blockchain technology, tokenisation, and stablecoin regulation.

The letter stresses that properly regulated stablecoins, backed one-to-one by high-quality assets, should be recognised as eligible collateral. It also criticises the distinction between “open” and “closed” blockchains as misguided, urging BCBS instead to focus on actual risk characteristics. Furthermore, the associations argue that major crypto-assets such as Bitcoin and Ether display levels of liquidity comparable to established financial instruments but remain subject to maximum capital charges. Finally, they call for banks to be permitted to use internal risk models for crypto-asset exposures, in line with other asset classes.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

MANDATORY REQUIREMENTS FOR FINANCIAL INSTITUTIONS

ECOVIS ProventusLaw

Digital Operational Resiliance Act DORA

LINK

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

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

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

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

Our DORA Audit Services include:

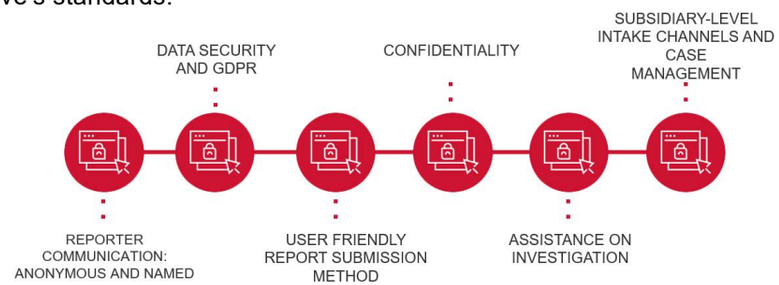
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors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

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

WHISTLEBLOWING DIRECTIVE IMPLEMENTATION
Outsourcing solution for companies

LINK

The EU Whistleblower Directive is mandatory for financial institutions under the **EU Whistleblower Directive** and the **Resolution No. 03-33** of the Board of the Bank of Lithuania. This resolution requires financial institutions to establish a **confidential and secure channel** for reporting breaches of EU law. It establishes minimum standards for reporting mechanisms and safeguards against retaliation for whistleblowers across the European Union, thereby bolstering Environmental, Social, and Governance (ESG) principles.
Ecovis provides a Whistleblowing system as an outsourced channel for companies, ensuring compliance with the EU Whistleblower Directive. Our service offers a convenient solution, as we provide secure and confidential reporting channels that meet the directive's standards.



By entrusting the handling of whistleblower reports to us, companies can streamline the reporting process, enhance transparency, and mitigate the risk of internal bias or conflict of interest.
Ecovis Wistleblowing's outsourced system ensures confidentiality and data security in accordance with directive standards while offering two flexible options for companies.

Option 1: Utilize our system solely as a reporting channel, receiving all reports directly without our involvement in the initial investigation process.
Option 2: Entrust us to handle the investigation process as well.

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