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

05.2025

ECOVIS ProventusLaw

The Financial Action Task Force (FATF)

LINK

On 19 May 2025, during the 34th Session of the Commission on Crime Prevention and Criminal Justice in Vienna, the FATF, INTERPOL, and the United Nations Office on Drugs and Crime (UNODC) jointly issued a call to action urging states to intensify efforts to combat money laundering and terrorist financing.
This initiative emphasises the need to disrupt the illicit financial gains from crimes such as drug and human trafficking, migrant smuggling, and fraud. A particular focus was placed on improving asset recovery, as global assessments show that most countries remain ineffective in this area. In response, the FATF has strengthened its standards, and the organisations have called for enhanced international cooperation and capacity building to improve financial investigations ahead of the 2026 UN Crime Congress.

The Bank of Lithuania

LINK

On 20 May 2025, the Bank of Lithuania, in cooperation with the Centre of Excellence in Anti-Money Laundering, hosted the conference “The Power of Motivation in Combating Money Laundering” in Vilnius. The event brought together over 500 representatives from both the public and private sectors. The discussions underscored that motivation is a fundamental driving force in the fight against financial crime.
Effective anti-money laundering efforts require strong interinstitutional cooperation, active information sharing, and a values-based commitment to integrity and accountability. Key topics included risks associated with crypto-assets, vulnerabilities in the real estate sector, and the critical role of personal leadership in advancing financial crime prevention.

The European Securities and Markets Authority (ESMA)

LINK

On 7 May 2025, the European Securities and Markets Authority published its Final Report (ESMA74-1103241886-1086) providing technical advice to the European Commission concerning amendments to the Market Abuse Regulation (MAR) and the Markets in Financial Instruments Directive II (MiFID II), specifically focusing on small and medium-sized enterprises growth markets (SME GMs).

This advice forms part of the broader Listing Act initiative, aimed at enhancing access to public capital markets for EU companies, particularly SMEs, by reducing administrative burdens while maintaining market integrity.

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

05.2025

ECOVIS ProventusLaw

Decision of the Board of the Bank of Lithuania

LINK

The Bank of Lithuania found that Fjord Bank AB did not comply with the minimum own funds requirement in the fourth quarter of 2024.

Following established procedures, Fjord Bank AB applied to the Bank of Lithuania to conclude an administrative agreement. After evaluating that the institution self-reported the violation, acknowledged it, and corrected it, the Bank of Lithuania decided to enter into an administrative agreement and, as a sanction, publicly announced the legal breach.

Our recommendation:

1. **Strengthen Capital Management:**
Implement more robust capital planning and monitoring processes to ensure continuous compliance with minimum own funds requirements.

2. **Enhance Risk Assessment:**
Regularly assess financial risks that could impact capital adequacy and proactively adjust capital buffers accordingly.

3. **Improve Internal Controls:**
Establish or improve internal controls to detect potential breaches early and prevent recurrence of non-compliance.

4. **Maintain Transparent Communication:**
Continue the practice of timely and transparent self-reporting of any regulatory breaches or financial irregularities to the Bank of Lithuania.

Disputes over Financial Services: Q1 2025 Review

LINK

In the first quarter of 2025, the Bank of Lithuania reviewed 223 disputes between consumers and financial market participants — 34% more than in Q1 of the previous year and 23% more than the previously recorded highest figures. The number of disputes examined also increased by 26% and 5%, respectively.

This growth was mainly driven by a 17% increase in disputes involving insurers and a twofold increase in disputes with other financial market participants.

Disputes by Service Type

Most disputes concerned non-life insurance services — 98 cases, accounting for 44% of all examined disputes. The most common disagreements were related to property insurance (32), compulsory motor third-party liability insurance (23), and casco insurance (23) contracts. Additionally, 82 disputes involved payment services, making up 37% of all cases. Of these, 53 were related to financial fraud and 18 to non-cash transactions.

Amicable Settlements and Implementation of Decisions

During this period, 36 amicable settlements were reached — 12% fewer than in Q1 2024. However, around EUR 130,000 was paid out due to mediation — more than twice the amount paid in the same period last year (about EUR 60,000). One decision was also made on the substance of a dispute, partially satisfying the consumer's claims. The insurance company implemented the recommended decision.

vilnius@ecovis.lt

REGULATORY COMPLIANCE UPDATE

PERSONAL DATA PROTECTION AND ICT REGULATION

ECOVIS ProventusLaw

05.2025

NIS2 Implementation and Obligations

LINK

The updated Lithuanian Cybersecurity Law, aligned with the EU NIS2 Directive, has expanded the scope of critical and important entities subject to enhanced cybersecurity obligations. Over 1,400 organizations have been officially listed in the National Cybersecurity Subjects Register. These entities must ensure proper risk management, incident response procedures, and internal governance structures in line with NIS2 requirements. Non-compliance may result in significant financial penalties and operational restrictions.

TIS2 Self-Assessment Tool by ECOVIS

To support organizations in navigating the new obligations, we have developed a free online NIS2 self-assessment tool. The tool enables entities to evaluate their current compliance status, identify gaps, and plan necessary actions for alignment with cybersecurity legislation. It is structured to reflect legal requirements and is a practical starting point for legal and risk teams: **https://tis2.ecovis.lt.**

Decision on Direct Marketing and the Right to Access Personal Data

LINK

On May 16, 2025, the State Data Protection Inspectorate (hereinafter – the Inspectorate) issued a decision regarding a complaint about the conduct of direct marketing and the right to access personal data. On May 31, 2024, the Complainant requested UAB "Consilium optimum" (hereinafter – the Respondent) to provide access to their personal data but did not receive a response. Additionally, the Complainant reported that the Respondent sent a direct marketing message via email on May 29, 2024, without consent and offered services by phone on May 30, 2024. The Complainant also criticized contracts containing pre-checked boxes for data use in direct marketing.

Court decision on Vinted, UAB complaint

LINK

On May 22, the Regional Administrative Court dismissed UAB "Vinted's" complaint against the State Data Protection Inspectorate, which had found the company in breach of the General Data Protection Regulation (GDPR). The Inspectorate's decisions followed complaints forwarded by the French data protection authority, alleging improper handling of personal data, including the refusal to fulfill erasure and access requests.

The court confirmed that Vinted violated several GDPR provisions by not clearly informing users of data processing or suspension reasons, issuing vague responses to erasure requests, and failing to inform users of their rights. The company also failed to demonstrate accountability or maintain adequate documentation, breaching Articles 5(2) and 24.

Migration management

LINK

On 28 May 2025, the EDPS issued an Opinion on the Proposal for a Regulation to establish a common system for returning third-country nationals illegally staying in the EU. The Proposal aims to simplify and harmonize return procedures across Member States. Given its impact on individuals' fundamental rights—particularly privacy and data protection—the EDPS calls for a thorough fundamental rights impact assessment.

AI: the Italian Supervisory Authority fines company behind chatbot "Replika"

LINK

On 10 April 2025, the Italian Data Protection Authority (Garante) issued a final decision imposing a €5 million fine on Luka Inc., the U.S.-based developer behind the AI chatbot Replika. The decision follows a self-initiated investigation by the authority, prompted by media reports and preliminary fact-finding on the company's handling of personal data.

UAB "Prime Leasing" Receives Warning for GDPR Violation

The State Data Protection Inspectorate (SDPI) has issued a warning to UAB Prime Leasing after investigating a data subject's complaint regarding the right to erasure (the "right to be forgotten"). The complaint revealed that the company failed to respond to the individual's request, submitted on December 20, 2022, due to a human error by an external service partner.

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 05.2025

ECOVIS ProventusLaw

Financial Crime Investigation Service

LINK

On 12 May 2025, the Klaipėda Regional Prosecutor's Office referred to court a criminal case against a 53-year-old citizen of the Russian Federation, accused of intentionally violating international sanctions imposed by the European Union (EU) Council on the Russian aviation sector. The individual faces charges under Article 123-1(1) of the Lithuanian Criminal Code, which pertains to breaches of international sanctions causing significant harm to the interests of the Republic of Lithuania.
The investigation, led by the Klaipėda Regional Prosecutor's Office and conducted by the Financial Crime Investigation Service (FNTT), revealed two primary incidents:

1. In 2023, the accused, acting as the head of a company registered in Turkey, purchased a CESSNA-type aircraft from a Danish company. In March 2023, he allegedly organized the aircraft's transfer from Denmark to Russia via Sweden and Lithuania, with the aircraft landing at Palanga Airport. A flight plan to Russia was submitted, but permission to proceed was denied.

2. In January 2023, the same individual, as the founder and head of a Kazakhstani company, acquired an R-44 helicopter from a Russian citizen. In April 2023, he reportedly piloted the helicopter from Latvia to Paluknys Airfield in Lithuania, accompanied by a Kazakhstani citizen, and later landed at Kaunas Airport. The intended destination was Russia, but authorization for the flight was not granted.

The European Council of the European Union

LINK

On 20 May 2025, the Council of the European Union announced the lifting of economic sanctions on Syria, marking a significant policy shift following the fall of the Assad regime. This decision aims to support Syria's transition towards an inclusive and peaceful society, free from external interference, and to facilitate economic recovery and reconstruction efforts. While economic sanctions have been lifted, the EU will maintain targeted sanctions related to the former Assad regime, including those based on security grounds and human rights violations. This approach is both gradual and reversible, contingent upon the new Syrian government's adherence to principles of inclusivity, pluralism, and peace.

The European Council of the European Union

LINK

On 20 May 2025, the Council of the European Union adopted the 17th package of sanctions against the Russian Federation in response to its ongoing war of aggression against Ukraine. This comprehensive set of measures aims to sever Russia's access to critical military technologies and diminish its energy revenues, which are instrumental in sustaining its military operations. A significant focus of this package is the targeting of Russia's "shadow fleet" of oil tankers and their operators, as well as major Russian oil producers. Additionally, the sanctions encompass actions against Russia's hybrid activities, domestic human rights violations, and the use of riot control agents by Russian forces in Ukraine.

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

05.2025

ECOVIS ProventusLaw

European Securities and Markets Authority (ESMA)

LINK

ESMA Seeks Stakeholder Input on Streamlining the Retail Investor Journey

To support investor engagement and regulatory simplification, ESMA has launched a Call for Evidence on how retail investors interact with investment services under MiFID II. This initiative aims to identify barriers and explore changes that could enhance participation in EU capital markets.

ESMA's Call for Evidence examines investor behaviour, the impact of social media, and challenges posed by complex financial disclosures. It also evaluates how MiFID II rules are applied in practice, including suitability and appropriateness assessments, and investigates whether current frameworks for products like crowdfunding support or hinder retail participation. By encouraging responses from a wide range of stakeholders, including consumer organizations, the regulator aims to ensure that simplification efforts do not compromise investor protection. The deadline for responses is 21 July 2025.

European Banking Authority (EBA)

LINK

Rising Protected Deposits

EU Deposit Guarantee Scheme (DGS) funds have reached the legally mandated target of €79bn, bolstering depositor confidence and enhancing financial stability. The milestone comes as protected deposits continue to grow, reaching €8.6tn in 2024—a 3.2% annual increase.

Following a decade-long accumulation phase, all 33 national DGSs in the EU have met or exceeded the 0.8% target ratio of financial means to covered deposits, as mandated by the Deposit Guarantee Schemes Directive (DGSD). These funds, contributed by credit institutions, ensure that deposits up to €100,000 per depositor per bank are reimbursable within seven days of a bank failure. The European Banking Authority (EBA) highlighted that all DGSs now have adequate financial capacity and contingency mechanisms, including supplementary contributions and short-term liquidity provisions. Transparency and accountability remain central, with annual public data covering the entire European Economic Area, including Iceland, Norway, and Liechtenstein.

European Securities and Markets Authority (ESMA)

LINK

ESMA Presses Social Media Giants to Curb Unauthorized Financial Promotions

In a move to combat growing online financial scams, ESMA has called on major digital platforms to proactively block unauthorized financial advertisements that mislead retail investors and erode trust in capital markets.

ESMA addressed a letter to top social media and platform companies—including X, Meta, TikTok, Google, and Reddit—urging stronger controls against the spread of unauthorized financial services. These ads, often disguised as legitimate investment opportunities, increasingly target retail investors, resulting in significant financial harm and undermining the integrity of the financial system. The regulator emphasized that digital platforms have a responsibility to act as gatekeepers against fraudulent financial content. ESMA's message aligns with a parallel initiative by IOSCO, highlighting the international regulatory consensus on addressing online financial misconduct. The coordinated regulatory pressure marks a shift toward holding digital intermediaries accountable in investor protection efforts.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

05.2025

Decision of the Šiauliai Regional Court

LINK

The recent Lithuanian appellate court ruling has clarified the rules of international jurisdiction in labour disputes involving foreign employees working for Lithuanian employers.

The case involved a Belarusian citizen employed by a Lithuanian company. After the employment relationship ended, the employee initiated a labour dispute by filing a complaint with the Lithuanian Labour Disputes Commission (LDC). Following the LDC's decision, the employer sought to challenge the outcome in court, but the first-instance court rejected the claim, citing a lack of jurisdiction due to the employee's residence outside Lithuania.

The appellate court overturned the decision, holding that because the employee had voluntarily initiated the dispute in Lithuania, Lithuanian authorities — including the courts — retain jurisdiction throughout the proceedings. This means the employer could rightfully file a claim in Lithuanian court, even though the employee lives abroad.

Our recommendation:

We recommend employers to include a jurisdiction clause in employment contracts with foreign employees, specifying that disputes will be resolved in Lithuanian courts. This provides certainty and avoids future jurisdictional challenges.

Lithuanian Supreme Administrative Court (LVAT)

LINK

On 7 May 2025, the Lithuanian Supreme Administrative Court (LVAT) referred a preliminary question to the Court of Justice of the EU (CJEU) regarding national rules under the Law on Restrictive Measures in Response to Military Aggression Against Ukraine. The case concerns a dual citizen of Israel and Russia whose application for a temporary residence permit in Lithuania was rejected due to the absence of a valid visa or residence permit, despite her visa-free entry as an Israeli national.

Lithuanian law currently suspends residence permit applications from Russian citizens unless they hold a valid visa or EU residence permit. The applicant argues this requirement is disproportionate and discriminatory, given her Israeli citizenship and visa-free status under EU Regulation 2018/1806.

The LVAT seeks clarification on whether national rules may require a valid visa or permit from dual nationals—such as Russian-Israeli citizens—despite visa-free entry granted to one of their nationalities. Proceedings are suspended pending the CJEU's decision.

vilnius@ecovis.lt

REGULATORY COMPLIANCE UPDATE

CRYPTO

05.2025

ECOVIS ProventusLaw

The Bank of Lithuania

LINK

On 20 May 2025, the Bank of Lithuania issued a public statement urging entities intending to provide crypto-asset services to initiate the licensing process without delay. The Bank emphasised that, in accordance with forthcoming regulatory requirements, all crypto-asset service providers operating within the jurisdiction must obtain the necessary authorisation to continue their activities legally.
The licensing process is comprehensive and time-consuming, and postponing the application may result in operational disruptions or non-compliance with the established legal framework.
The Bank of Lithuania highlighted the importance of early engagement with the supervisory authority to ensure a smooth transition into the regulated environment and to uphold the integrity and stability of the financial system.

The Bank of Lithuania

LINK

On 30 May 2025, the Bank of Lithuania granted its first CASP licence under the MiCA Regulation to Robinhood Europe, UAB. The licence authorises Robinhood Europe, UAB to provide regulated crypto-asset services throughout the EU.
The Bank of Lithuania confirmed that such licences will only be issued to applicants who meet strict regulatory standards, including a transparent ownership structure, verifiable and lawful sources of funding, and the appointment of competent and qualified management. As part of the licensing process, the central bank conducts comprehensive assessments of the reputation of shareholders and executives, as well as the applicant's financial soundness and operational preparedness.
This regulatory milestone is a key step in implementing the EU-wide framework in Lithuania and reinforces the jurisdiction’s commitment to market integrity, financial stability, and consumer protection in the crypto-asset sector.

The UK Financial Conduct Authority (FCA)

LINK

On 28 May 2025, the FCA released Consultation Paper CP25/14, outlining proposed regulations for fiat-backed stablecoins and cryptoasset custody. This initiative aims to integrate stablecoins into the UK's financial regulatory framework, ensuring they function reliably as a medium of exchange rather than speculative assets.

The FCA's proposals stipulate that qualifying stablecoins must be fully backed by secure, liquid assets on a one-to-one basis. These backing assets are to be held under a statutory trust with an independent custodian, separate from the issuer's group. Redemption at face value is mandated, ensuring that holders can retrieve the full value of their stablecoins upon request.

Additionally, custodians are required to segregate client cryptoassets, maintain robust recordkeeping, and perform daily reconciliations. The consultation period for these proposals is open until 31 July 2025, with final rules expected to be published in 2026.

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:

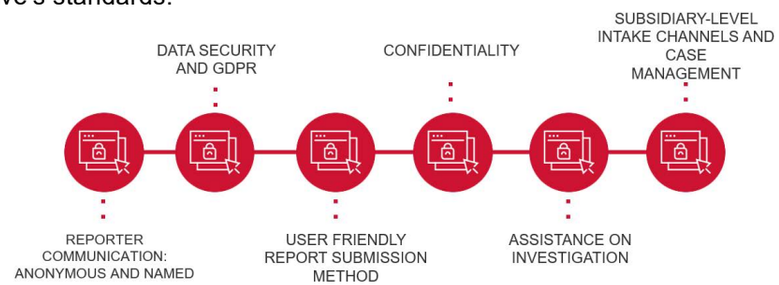
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors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