REGULATORY COMPLIANCE UPDATE

MANDATORY REQUIREMENTS FOR FINANCIAL INSTITUTIONS

ECOVIS ProventusLaw

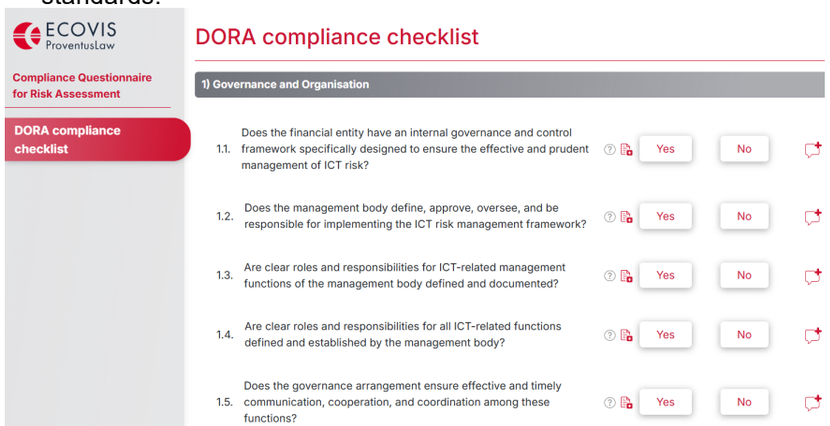
Digital Operational Resiliance Act DORA

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.



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.

Assessment and Gap Analysis

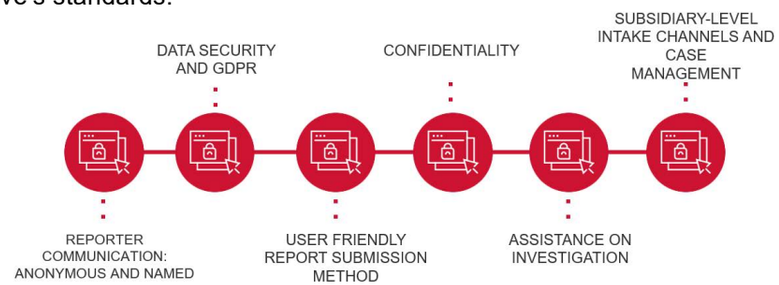
Self-assessment and gap analysis are essential steps, and we are ready to support you in this important endeavour. For this, we have developed a DORA compliance tool designed for self-assessment.

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.

REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

04.2025

ECOVIS ProventusLaw

European Banking Authority

LINK

In April 2025, the European Banking Authority (EBA) published Issue 15 of its AML/CFT Newsletter, highlighting key developments across regulation, supervision, and market risk analysis.

Notably, the EU crypto-asset framework has now entered full implementation. CASPs must establish effective systems and controls under MiCAR and related regulations to prevent misuse for illicit purposes. A joint EBA–ESMA report addressed risks in decentralized finance (DeFi), including vulnerabilities in crypto lending, borrowing, and staking.

The EBA also hosted a workshop on the use of supervisory technology and AI to support AML/CFT supervision, and conducted a peer review on tax integrity practices, identifying areas for further improvement.

Additional developments include the release of Guidelines on restrictive measures compliance, consultation on draft Regulatory Technical Standards central to the future AML/CFT regime, and preparations for the transition to the new EU AML Authority (AMLA). Lastly, the EBA noted continued concerns about de-risking and its impact on EU consumers.

The Bank of Lithuania (BoL)

LINK

The Bank of Lithuania (BoL) has imposed a fine of €3.5 million on Revolut for breaches of anti-money laundering regulations. The violation was identified during a planned inspection, which revealed deficiencies in Revolut's monitoring of business relationships and transactions. These deficiencies resulted in the bank's failure to properly identify suspicious transactions conducted by its customers.

Revolut subsequently requested the opportunity to enter into an administrative arrangement with the BoL. After evaluating the situation, including the bank's acknowledgment of the irregularities and its proactive steps to address the issues, the BoL agreed to enter into such an arrangement. The fine was determined based on the nature, duration, and scale of the infractions, as well as the annual gross revenue of Revolut's parent company, which is registered in Lithuania.

Revolut has expressed its commitment to maintaining high legal compliance standards and has taken immediate steps to rectify the identified procedural shortcomings, emphasizing its ongoing investment in improving financial crime control measures.

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

04.2025

ECOVIS ProventusLaw

Decision of the Supreme Administrative Court of Lithuania

LINK

The Lithuanian Supreme Administrative Court (LVAT) has decided to seek a preliminary ruling from the Court of Justice of the European Union (CJEU) in the dispute between the payment institution "Alternative Payments" and the Bank of Lithuania regarding the revocation of the company's license. The proceedings will be suspended until the CJEU provides its interpretation.

Publication of the Bank of Lithuania

LINK

Electronic money (EMI) and payment institutions (PI) providing payment services can now gain direct access to payment systems across Europe, including retail payment systems managed by central banks. The possibility of direct participation in payment systems was formalized with the adoption of EU legislative amendments and their incorporation into national law. The main principles regarding EMI and PI participation in central bank-managed payment systems were established in the Eurosystem's Policy on access by non-bank payment service providers to central bank-operated payment systems and to central bank accounts, approved on July 18, 2024.

The transition of current CENTROlink service users to direct participants begun on April 9, 2025. During this transition, contracts with holders of addressed BICs will be terminated, and direct CENTROlink participant contracts will be signed. The transition is planned to take place in stages, with full implementation expected by the end of the year.

Publication of the Bank of Lithuania

LINK

In 2024, the Bank of Lithuania received a total of 812 complaints, marking a significant decrease compared to the previous year, when the number of complaints was over double. The majority of complaints were related to the services of banks (41%), electronic money institutions (23%), and insurers (around 13%).

Complaints regarding payment services accounted for 62% of all complaints, while insurance-related complaints made up 14%, and credit complaints 12%. Other complaints were related to investment and other services.

The number of complaints about payment services decreased almost threefold in 2024, from 1,408 to 502. The majority (nearly half) of the complaints related to payment services concerned payment accounts, with many complaints about the restriction or closure of accounts. Over a third of complaints were related to financial fraud, while others were about payment cards and non-cash transactions.

Slides presented by the Bank of Lithuania

LINK

New guidelines allow non-bank payment service providers (NB-PSPs) direct access to TARGET. The guidelines come into effect from June 16, 2025. This will allow NB-PSPs, such as payment institutions and electronic money institutions, to directly participate in the Eurosystem's central bank-operated payment systems.

REMINDER REGARDING REPORTING

Please be aware of the upcoming deadlines for reporting to the State Tax Inspectorate – by 1st of June to submit the reports in terms of:

- accounts where the total annual turnover of all accounts held by the same person with the same financial market participant is at least EUR 15,000;
- the debt obligations owed to a financial market participant as at 31 December of the calendar year;
- balance of accounts at the end of the year, if the total annual balance of accounts of the same person with the same financial market participant at the end of the year is not less than EUR 5,000.

Please note that contributions of supervised financial market participants to the bank of Lithuania for the current year shall be paid by 31st of May.

Detailed and full Regulatory Compliance Report on EMI, PI regulation can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

PERSONAL DATA PROTECTION AND ICT REGULATION

ECOVIS ProventusLaw

04.2025

New Register of Lithuanian Cybersecurity Entities Established

LINK

The new Lithuanian Cybersecurity Entities Register has been formed, currently comprising 1,443 organisations across 11 critical sectors and 7 other highly important sectors. Under the updated Cybersecurity Law, all organisations listed in the register will be required to comply with stricter security standards. Compared to the previous list, the number of registered organisations has increased nearly fivefold, with the majority of newly added entities belonging to the private sector. All registered entities must comply with the provisions set out in the Cybersecurity Law and the Government of the Republic of Lithuania's Resolution of 6 November 2024 on its implementation. A transitional period has been established for the application of the new cybersecurity requirements: 12 months for organisational requirements and 24 months for certain technical requirements, both calculated from the date of the entity's inclusion in the register.

ECOVIS ProventusLaw has developed a **NIS2 compliance self-assessment tool** designed to help organisations evaluate their adherence to the Cybersecurity Law and the related government resolution. The tool allows entities to assess their current compliance status and plan the necessary next steps for full alignment with the applicable standards.

Guidelines 02/2025 on processing of personal data through blockchain technologies

LINK

The European Data Protection Board (EDPB) has released a draft of its Guidelines 02/2025 on the processing of personal data in blockchain technologies, now open for public consultation until 9 June 2025. The guidelines aim to help organisations align blockchain practices with GDPR compliance.

New EU Guidelines on Oversight Cooperation under DORA

LINK

As part of its financial market supervision responsibilities, the Bank of Lithuania will follow the Joint Guidelines on Cooperation and Information Exchange for Oversight Purposes (JC/GL/2024/36), adopted on June 5, 2024, by the Joint Committee of the European Supervisory Authorities (ESAs).

These guidelines establish the practices for cooperation and information exchange between ESAs and national competent authorities (NCAs) to ensure effective and coordinated oversight under the EU Digital Operational Resilience Act (DORA).

State Data Protection Inspectorate Reviews Complaint on Direct Marketing Violation

LINK

The State Data Protection Inspectorate (the Inspectorate) reviewed a complaint filed by UAB „Principo reikalas“ (the Complainant) on May 8, 2024. The Complainant alleged that on April 17, 2024, the Respondent sent a direct marketing email to the Complainant's email address without prior consent. The Complainant requested documentation to validate the legality of this data processing for direct marketing purposes but did not receive any response.

EDPB Annual Report 2024: Safeguarding Personal Data in a Changing Digital Environment

LINK

On 23 April 2025, the European Data Protection Board (EDPB) published its 2024 Annual Report, highlighting key achievements in safeguarding data privacy amid rapid digital transformation. The report reflects the EDPB's strengthened focus on regulatory clarity, stakeholder engagement, and consistent GDPR enforcement across the EU.

EU Plans to Ease GDPR Burden on SMEs

LINK

The European Commission is preparing reforms to the General Data Protection Regulation (GDPR), aiming to reduce administrative burdens—particularly for small and medium-sized enterprises (SMEs)—while preserving its core data protection principles.

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 04.2025

ECOVIS ProventusLaw

The European Anti-Fraud Office

LINK

On April 24, 2025, the European Anti-Fraud Office (OLAF) announced its support for the Lithuanian Customs Criminal Service (MKT) in a significant operation aimed at investigating the circumvention of EU sanctions. The operation, carried out on April 10, included a coordinated raid on a company suspected of unlawfully exporting goods to Russia and Belarus in violation of EU sanctions. During the raid, authorities seized a large quantity of potentially sanctioned goods, weapons, and significant sums of money.The company is alleged to have used routes through Central Asian countries to circumvent EU export restrictions. Preliminary assessments indicate that the value of the seized items is approximately €1.5 million. OLAF provided vital intelligence, analytical support, and advanced tools to assist in the investigation.

The Vilnius Regional Prosecutor's Office is leading the pre-trial investigation, with OLAF working closely with both EU and non-EU authorities to track the export routes and destinations of the sanctioned goods. The investigation's findings could assist other EU Member States in identifying similar illicit trade channels. OLAF Director-General Ville Itälä reaffirmed OLAF's commitment to supporting EU Member States in enforcing sanctions and protecting the EU's financial interests.

The European Council of the European Union

LINK

On April 15, 2025, the High Representative of the European Union issued a formal statement acknowledging the alignment of several third countries with Council Implementing Decision (CFSP) 2025/632, adopted on March 27, 2025. This decision pertains to the imposition of restrictive measures in response to the situation in Belarus and its involvement in the Russian aggression against Ukraine. The Council's decision entails the addition of 25 natural persons and seven legal entities to the list of individuals and organizations subject to restrictive measures, as delineated in Annex I to Decision 2012/642/CFSP. These measures are part of the European Union's ongoing efforts to address actions undermining or threatening the territorial integrity, sovereignty, and independence of Ukraine. The countries aligning with this decision — Albania, Bosnia and Herzegovina, Iceland, Liechtenstein, Montenegro, North Macedonia, Norway, and Ukraine — have committed to ensuring that their national policies conform to the Council's decision. The European Union has taken note of and welcomed this commitment, recognising it as a demonstration of solidarity and shared responsibility in upholding international law and supporting Ukraine's sovereignty.

The European Council of the European Union

LINK

Council Decision (CFSP) 2025/779 of 14 April 2025 amends Common Position 2008/944/CFSP to update the common rules governing the control of exports of military technology and equipment. The amendment strengthens the EU's regulatory framework to better address current security challenges and ensure that military exports align with the Union's values, obligations, and international commitments, including respect for human rights and international humanitarian law. The Decision entered into force upon publication.

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

04.2025

ECOVIS ProventusLaw

European Commission

LINK

Consumers Express Strong Trust in Rights and Product Safety, but Online Threats Undermine Confidence

With trust high but online scams and misleading practices rampant, regulators are intensifying efforts to safeguard shoppers. he European Commission's 2025 Scoreboard shows that 70% of consumers trust businesses to uphold their rights and 68% feel confident in product safety. However, the digital environment remains a vulnerability. Online shoppers are over 60% more likely to face issues compared to offline buyers, and nearly half of consumers have encountered scams or unfair practices like fake reviews. Trust in green claims and environmental considerations also fell significantly, driven by cost concerns and greenwashing skepticism. To bolster consumer protection, the Commission is implementing the new General Product Safety Regulation and the E-Commerce Communication, targeting products from non-EU traders. Upcoming initiatives include the Digital Fairness Act and directives on the right to repair and green transition, aiming to boost transparency, product durability, and digital protections. These efforts will inform the EU's Consumer Agenda for 2025–2030.

European Commission

EU Targets Unfair Practices in Children's Video Games with New Enforcement and Guidelines

LINK

As concerns grow over exploitative in-game tactics, EU authorities have taken decisive steps to protect young consumers. A coordinated enforcement action and new industry guidelines aim to curb manipulative practices involving virtual currencies in online gaming environments. The European Commission, through the Consumer Protection Cooperation Network (CPC), has launched enforcement proceedings against Star Stable Entertainment AB following complaints over potentially harmful marketing tactics directed at children in its game, Star Stable Online. Violations cited include aggressive time-limited purchase prompts, vague pricing of virtual items, and influencer marketing that lacks transparency. The company now faces a one-month deadline to address these breaches and commit to corrective actions.

Simultaneously, the CPC Network has issued new principles for the gaming industry to enhance transparency around virtual currencies. These principles mandate clear pre-contractual pricing, prohibit hidden charges, and stress the need to adapt commercial content to children's vulnerabilities. The initiative builds on existing EU consumer law and is part of broader efforts under the upcoming Digital Fairness Act.

European Commission

LINK

Half of Second-Hand Online Traders Fall Short on Consumer Rights Compliance, EU Investigation Finds

A sweeping investigation by the European Commission and national authorities across 27 countries has revealed widespread non-compliance among online sellers of second-hand goods, raising major concerns over consumer rights and transparency in the fast-growing resale market.

In the latest EU-wide "sweep," 356 online second-hand traders were reviewed, with 52% flagged for potential breaches of EU consumer law. Key violations include failing to clearly inform buyers of their 14-day right of withdrawal (40%), misrepresenting return rights for faulty goods (45%), and disregarding the mandatory one-year legal guarantee for second-hand products (57%). Additionally, environmental claims were frequently misleading – 28% were deemed deceptive or unfair, and another 20% lacked proper substantiation. Authorities also found that a number of traders did not provide essential business details or complete pricing information.

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

04.2025

ECOVIS ProventusLaw

Decision of the Lithuanian Supreme Court

The claimant sought to have her dismissal declared unlawful, contending that her employment with another company could not amount to a gross breach of work duties, particularly given that no non-compete agreement had been concluded with her employer. The first-instance court ruled in her favor, but the appellate court reversed the decision. The claimant then filed a cassation appeal.

The Lithuanian Supreme Court (LAT) confirmed that although no non-compete agreement had been signed, a conflict of interest may arise independently of such contractual arrangements. The Court clarified that a conflict of interest in employment occurs when an employee's actions or affiliations may potentially undermine the employer's interests — whether through ties to other entities or personal motivations. In accordance with Article 24 of the Labour Code (DK), actual damage is not required; the mere risk of harm to legitimate employer interests is sufficient to establish a conflict.

In the case at hand, the claimant held a highly specialized role as Head of the Technology Development Division and took on a similar position at a direct competitor. Even without a formal non-compete clause, this raised a significant risk of conflict, as the employee might be required to prioritize the interests of the new employer over those of the former.

The claimant failed to acknowledge the potential conflict and did not evaluate her conduct critically. This led the employer to conclude that the employment relationship could no longer be sustained without endangering its interests. The Supreme Court upheld the appellate ruling, determining that the claimant had committed a gross breach of work duties under Article 58(3)(7) DK, despite the absence of a contractual restriction.

Importantly, the Court emphasized that employers cannot use internal rules or employment contracts to impose broad, unjustified restrictions on employees' participation in the labor market. Any limitation must be proportionate and linked to legitimate business interests, such as the protection of trade secrets or proprietary knowledge. Purely economic motives — for instance, securing cheaper labor — do not qualify for protection under Article 24(5) DK.

LINK

Our recommendation:

- Even in the absence of a non-compete agreement, employers can enforce duties to avoid conflicts of interest where legitimate business interests are threatened.
- Include clear internal conflict-of-interest policies in job descriptions and handbooks, especially for employees in strategic or sensitive roles.
- Review dismissal procedures to ensure decisions are based on objective risk to the employer's interests, not simply the existence of outside employment.

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

Our recommendations and details are in this file

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

CRYPTO

04.2025

ECOVIS ProventusLaw

The European Securities and Markets Authority

LINK

The European Securities and Markets Authority (ESMA) has provided clarification regarding the applicability of Article 60(5) of the MiCA to registered AIFMs, as defined under Article 3(2) of the AIFMD (Directive 2011/61/EU). Key Points:

- Scope of Article 60(5) MiCA: This provision permits authorised UCITS management companies and authorised AIFMs to offer crypto-asset services equivalent to their existing portfolio management and non-core services, contingent upon prior notification to their home Member State's competent authority at least 40 working days before commencing such services.
- Registered AIFMs, often referred to as sub-threshold AIFMs, are exempt from the full authorisation requirements under the AIFMD and are instead subject to a registration regime.
- ESMA has determined that the provisions of Article 60(5) MiCA do not extend to registered AIFMs. Consequently, these entities are not authorised to provide crypto-asset services based solely on the notification mechanism outlined in Article 60(5) MiCA.

Registered AIFMs seeking to offer crypto-asset services must obtain full authorisation under the AIFMD to leverage the notification process described in Article 60(5) MiCA. Without such authorisation, they are precluded from providing these services under the current regulatory framework. This clarification underscores the regulatory distinction between authorised and registered AIFMs concerning the provision of crypto-asset services within the European Union.

The European Securities and Markets Authority

LINK

The ESMA has released final guidelines to help national competent authorities (NCAs) prevent and detect market abuse in crypto-asset markets under the MiCA. These guidelines aim to ensure a consistent supervisory approach across the EU, focusing on insider dealing, unlawful disclosure of inside information, and market manipulation. The guidelines promote proportional, risk-based supervision, integration into existing practices, and cross-border cooperation. They will apply three months after publication, with NCAs expected to notify ESMA of their compliance status within two months. Key points:

- NCAs are expected to allocate dedicated personnel to crypto-asset supervision and to ensure continuous professional development through structured training programmes focused on digital finance.
- NCAs are advised to establish active coordination channels with AML bodies and consumer protection agencies to strengthen oversight of crypto-asset markets.
- Monitoring frameworks should integrate data from both on-chain and off-chain sources, including social media activity, and employ a combination of automated systems and human oversight to detect abusive behaviour effectively.
- Entities engaged in arranging or executing crypto transactions—referred to as persons professionally arranging or executing transactions (PPAETs)—must maintain and regularly update their surveillance mechanisms to address the evolving nature of market abuse risks.

The European Banking Authority

LINK

The European Banking Authority (EBA) has published new draft Regulatory Technical Standards (RTS) specifying the circumstances in which CASPs must appoint a central contact point (CCP) to support efforts in combating financial crime. CASPs established in one EU Member State may provide services in another, and where they maintain a local establishment, such as a crypto ATM, they are required to comply not only with the AML/CFT obligations of their home Member State but also those of the host Member State. In such cases, the appointment of a central contact point is intended to mitigate money laundering and terrorist financing risks associated with the cross-border provision of crypto-asset services and to facilitate effective AML/CFT supervision and oversight. The draft RTS outline the conditions under which CASPs must appoint a central contact point, as well as the roles and responsibilities of the central contact point. However, the draft RTS do not prescribe the form the central contact point should take or its location within the European Union, in accordance with the EBA's legal mandate.

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