REGULATORY COMPLIANCE UPDATE

MANDATORY REQUIREMENTS FOR FINANCIAL INSTITUTIONS

ECOVIS ProventusLaw

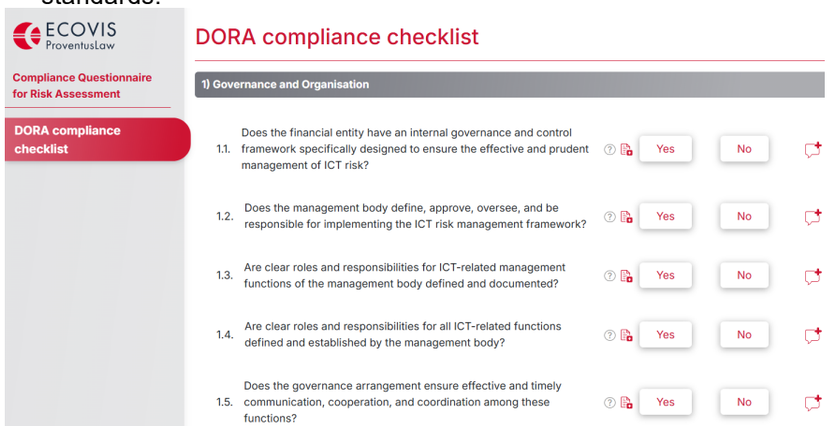
Digital Operational Resiliance Act DORA

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

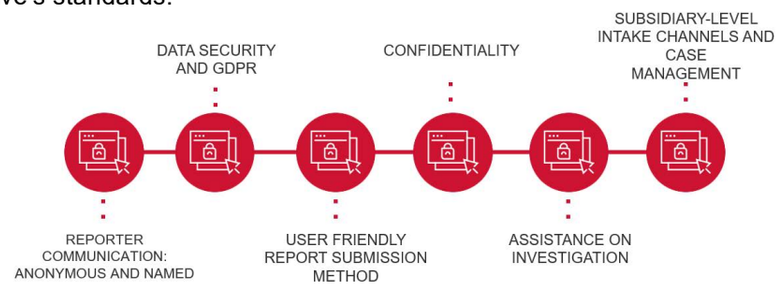
Self-assessment and gap analysis are essential steps, and we are ready to support you in this important endeavour. For this, we have developed a DORA compliance tool designed for self-assessment.

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

03.2025

ECOVIS ProventusLaw

The European Banking Authority (EBA)

LINK

The European Banking Authority (EBA) has launched a public consultation on four draft Regulatory Technical Standards (RTS) to support the EU's new AML/CFT framework. These RTSs will guide financial institutions and supervisory authorities in complying with the revised legal framework.

The proposed RTSs cover key areas, including AMLA's criteria for determining which financial institutions will be subject to direct supervision, a harmonised methodology for assessing ML/TF risks, customer due diligence requirements, and a framework for imposing sanctions and penalties. These standards aim to ensure consistent supervision across Member States and reduce regulatory burdens for cross-border institutions. The EBA will submit its final response to the European Commission by 31 October 2025.
The consultation paper is open for comments until 6 June 2025 via the EBA's website.

The Global Terrorism Index 2025

LINK

The Global Terrorism Index 2025 highlights a global decline in terrorism-related deaths, driven primarily by a reduction in attacks in conflict zones. However, terrorist activity remains prevalent in regions like the Sahel, with the rise of violent extremist groups. Online radicalisation is contributing to a growing threat of lone-actor terrorism. Despite a drop in attacks, terror-related fatalities remain a significant concern due to shifting patterns in how terrorism is executed and the evolving role of various terrorist organisations.

The Bank of Lithuania

LINK

The Bank of Lithuania has invited financial market participants to engage in a consultation on customer due diligence requirements and related matters concerning the prevention and supervision of ML/TF. This consultation is part of the European Banking Authority's development of four draft regulatory technical standards, which aim to clarify the compliance obligations of financial institutions under the new AML/CFT package, as outlined in Regulation (EU) 2024/1624.

The consultation, running until 6 June 2025, specifically focuses on the information institutions will need to collect during customer due diligence processes. Financial market participants are encouraged to submit their comments or alternative proposals through the provided link. A virtual public discussion on the proposals will be held on 20 April 2025, with registration open until 8 April 2025. The final draft standards are expected to be submitted to the European Commission by 31 October 2025.

Center of Excellence in Anti-Money Laundering

LINK

In 2024, Lithuania saw a surge in fraud cases, causing significant financial losses. Fraudsters attempted to steal €35 million, with over €20 million successfully transferred. However, financial institutions prevented €15 million in suspicious transactions and recovered €2.6 million, though the public still faced a net loss of €17.3 million.

The number of fraud cases rose sharply from 7,881 in 2022 to 13,691 in 2024, with fraudulent transfers increasing from €11.8 million to €20 million. Investment and telephone fraud were the most damaging schemes, accounting for nearly €10 million in losses. Authorities stress the need for stronger prevention, institutional cooperation, and public awareness.

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

03.2025

ECOVIS ProventusLaw

Resolution No 03-33 by the Bank of Lithuania

LINK

The Bank of Lithuania has adopted the Resolution No 03-33 Amending resolution No 247 of the Board of the Bank of Lithuania of 30 December 2009 On requirements for electronic money institutions and payment institutions regarding internal control, risk management and safeguarding of received funds (hereinafter – the Resolution). The institutions must comply with requirements in terms of wind-down plan starting from 9th of April 2025.

Publication by the Bank of Lithuania

LINK

Lithuania's electronic money institution (EMI) and payment institution (PI) sector recorded significant financial growth in 2024, with income from licensed activities jumping by 25% to €622 million and the amount of payment transactions increasing by 33% to €152 billion. However, the competitive environment remains unchanged, with a tenth of institutions continuing to dominate the market in both cases.

Publication by the Bank of Lithuania

LINK

Foreign companies continue to take a keen interest in the development opportunities offered by the Lithuanian financial market. According to data of the Bank of Lithuania's Newcomer Programme, more than 150 foreign companies interested in business opportunities in Lithuania applied to the regulator in 2024. The Bank of Lithuania strives to ensure that licenses granted in Lithuania meet the highest quality standards, therefore the focus is on quality rather than quantity, while attempting to prevent irregular activities at the early stages.

Consultation on the Review of the Supervision Fee Calculation Methodology and Maximum Limits

LINK

The Bank of Lithuania has completed its review of the methodology for calculating supervision fees for financial market participants, including the maximum fee limits, to ensure proportionality and efficiency.The goal of the review was to guarantee fairness in fee collection, both horizontally and vertically, ensuring that the financial burden on market participants is proportionate to their business scale, supervision intensity, and clearly defined maximum limits.

Publication by ECB

LINK

The Eurosystem has positively concluded its exploratory work for offering a Verification of Payee (VoP) service for payment service providers (PSPs) building on the services developed by the Banco de Portugal and Latvijas Banka. The decision will help PSPs in the Single Euro Payments Area (SEPA) to comply with their legal obligations for credit transfers in euro, as outlined in the EU Instant Payments Regulation (Regulation 2024/886).

The two solutions offered by these Eurosystem central banks have been designed in accordance with the VoP scheme developed by the European Payments Council. The solutions will achieve SEPA-wide reach and will benefit from the coordination by the Eurosystem. Thus, any PSP in the euro area will be able to fulfil its obligation to offer a VoP service to their customers by 9 October 2025, using one of the two solutions.

Frequently Asked Questions (FAQ) document for financial institutions using CENTROlink

LINK

The Bank of Lithuania has published an updated Frequently Asked Questions (FAQ) document for financial institutions using CENTROlink, its payment system that ensures access to SEPA (Single Euro Payments Area). The new FAQ addresses key regulatory, technical, and operational aspects of participation, particularly in light of upcoming changes affecting electronic money institutions (EMIs) and payment institutions (PIs).

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

03.2025

ECOVIS ProventusLaw

VDAI Issues Ruling on Unauthorized Marketing Emails

LINK

In a recent ruling, the State Data Protection Inspectorate (hereinafter - VDAI) found a company in breach of the Republic of Lithuania Law on Electronic Communications (hereinafter - ERĮ) after it sent unsolicited marketing emails without obtaining prior consent from the recipients. VDAI has directed the company to ensure that any future marketing emails are sent only after obtaining the proper consent from recipients.

The State Data Protection Inspectorate (VDAI) conducted an investigation regarding the legality of video surveillance

LINK

The State Data Protection Inspectorate (VDAI) conducted a n investigation into the legality of video surveillance in one of the crisis centers. The inspection determined that the video surveillance carried out within the center was excessive and did not comply with the General Data Protection Regulation (GDPR) requirements. According to Article 6(1)(f) of the GDPR, such data processing can be lawful if it is necessary and proportionate and does not infringe on data subjects' rights.VDAI's analysis revealed that surveillance cameras were installed not only in common areas such as corridors and entrances but also in locations that ensure a certain level of privacy, such as above the dining table and near restroom doors.The inspection found that while warning signs were posted within the center, the information provided was insufficient, and not all residents could clearly understand the extent of the surveillance. Articles 13 and 14 of the GDPR stipulate that the data controller must provide the data subject with all relevant information.

VDAI Ruling: Payment Reminder Emails Must Respect Data Subject Rights

LINK

The State Data Protection Inspectorate (VDAI) has issued a ruling regarding a company that continued sending payment reminder emails to a customer despite the individual's request to opt out. The investigation found that while the company lawfully processed personal data under Article 6(1)(f) of the GDPR, its failure to respect the data subject's right to object under Article 21 constituted a violation.The Inspectorate emphasized that companies cannot use technical limitations as an excuse for failing to uphold data subject rights. Under Article 24 and 25 of the GDPR, data controllers are required to design their systems to ensure compliance with data protection principles from the outset. This ruling highlights the importance of flexible and transparent communication systems that allow individuals to manage their data preferences.

Personal data was processed in the Public Management Agency in breach of GDPR requirements

LINK

The Supreme Administrative Court of Lithuania (hereinafter - LVAT), in its ruling of March 26, reviewed a dispute concerning the decision of the State Data Protection Inspectorate (the Inspectorate). The case established that Public Management Agency (hereinafter – Agency) had unlawfully accessed personal data in the State Civil Servants Register (VATARAS) for over two years. Nineteen Agency employees viewed the personal data of a specific individual 244 times without a legitimate basis or purpose. Furthermore, the employees were not properly informed about data protection regulations, and the Agency failed to monitor how data was being handled. These actions were deemed violations of the General Data Protection Regulation (GDPR).

Recommendations from the State Data Protection Inspectorate (VDAI) on security measures for personal data processed by online shops

LINK

The State Data Protection Inspectorate (VDAI), after conducting a monitoring of personal data security measures in online stores, provides recommendations.

It is recommended to conduct regular audits of privileged access rights to ensure that access to personal data is granted only to employees who need it for their duties. Clear and documented procedures should be established to ensure that unnecessary or outdated data is securely deleted once the retention period expires.

Implementing advanced encryption solutions to protect personal data both during transmission and storage is advised.

Strict change management procedures should be adopted, covering the implementation of new systems, software, or data processing methods.

Organizations should periodically review their data protection policy, updating it according to the latest legal requirements and best practices.

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 03.2025

ECOVIS ProventusLaw

The Seimas of the Republic of Lithuania

LINK

Amendments to the Financial Regulatory Directive's instructions pertaining to the implementation of international sanctions have entered into force as of 18 March 2025, following the Protocol's conciliation.

The European Council

LINK

On March 27, 2025, the EU imposed sanctions on 25 individuals and 7 entities linked to the Belarusian regime, including members of the Central Election Commission responsible for the 2025 presidential election, judges involved in politically motivated sentencing, and businesses supporting the Lukashenka regime, such as Ridotto LLC and Belorusskiye Loterei.
These measures aim to penalise actions undermining democracy and human rights, as well as Belarus's military cooperation with Russia in the Ukraine conflict.

The European Council

LINK

On March 19, 2025, the EU welcomed Albania, Bosnia and Herzegovina, Iceland, Liechtenstein, Montenegro, North Macedonia, Norway, and Ukraine aligning their policies with the EU's restrictive measures against Belarus, in light of its involvement in the Russian aggression against Ukraine. The EU renewed and amended Decision (CFSP) 2025/385 to maintain the sanctions until February 2026.

The U.S. Department of the Treasury

LINK

On March 28, 2025, the U.S. Department of the Treasury updated the Specially Designated Nationals (SDN) List by adding new individuals under counter-terrorism sanctions. These individuals are now subject to primary and secondary sanctions administered by the Office of Foreign Assets Control (OFAC).
Details on these updates can be found: OFAC Recent Actions.

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

03.2025

ECOVIS ProventusLaw

European Banking Authority (EBA)

EBA Highlights Payment Fraud, Indebtedness, and De-Risking as Key Consumer Risks

LINK

The European Banking Authority's latest Consumer Trends Report identifies payment fraud, rising consumer debt, and financial de-risking as critical issues impacting EU consumers. Fraudsters are exploiting social engineering tactics to bypass security measures, while inadequate creditworthiness assessments contribute to growing indebtedness. Meanwhile, de-risking practices are limiting access to essential banking services for vulnerable groups.

The report, based on data from national authorities, consumer groups, and industry bodies, underscores that payment fraud remains the top concern. Fraudsters increasingly use social engineering to trick consumers into making unauthorized payments, bypassing strong customer authentication requirements. Indebtedness is also rising, driven by the proliferation of short-term credit products like Buy-Now-Pay-Later (BNPL), often coupled with inadequate creditworthiness assessments and insufficient transparency in lending terms.

Additionally, the report highlights a growing trend of financial de-risking, where banks refuse to onboard or offboard consumers—particularly migrants, refugees, and those with poor financial histories—limiting their ability to participate in the EU economy. The EBA plans to take further action in 2025/26 to address these risks and strengthen consumer protection across the region.

Recommendation of ECOVIS ProventusLaw:

Financial institutions should enhance fraud prevention strategies by strengthening consumer authentication and educating customers on social engineering tactics.

Lenders must ensure robust creditworthiness assessments and improve transparency in loan terms to prevent over-indebtedness.

The Bank of Lithuania

LINK

Record Number of Financial Disputes in Lithuania: Insights from the Newly Released Consumer Dispute Resolution Report

The Bank of Lithuania has released its latest Consumer Dispute Resolution Report, revealing that a record 751 consumer disputes were reviewed in 2024, with nearly €400,000 paid out through settlements. Disputes with insurers surged by 35%, mainly over vehicle insurance claims, while disputes with banks fell by over 20%. However, fraud schemes are becoming more sophisticated, underscoring the need for stronger consumer protection.

Nearly half of all disputes (49%) involved insurance companies, driven by rising repair costs and extreme weather events. Meanwhile, disputes with banks, which made up 41% of cases, saw a decline due to improved fraud prevention efforts. Despite this progress, scammers are using increasingly sophisticated techniques, such as fake websites and impersonation tactics. The newly released report provides key insights and recommendations for financial institutions to mitigate these risks.

Recommendation of ECOVIS ProventusLaw:

Financial institutions should enhance preventive measures to reduce disputes and strengthen fraud protection. Insurers must adjust claims assessment processes to account for rising repair costs and climate-related damages while improving transparency with customers. Banks should continue investing in advanced fraud detection and customer education to counter evolving scams. The Consumer Dispute Resolution Report offers essential guidance on best practices for dispute prevention and resolution.

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

03.2025

ECOVIS ProventusLaw

Lithuanian Court Confirms CEO Personal Liability for Governance Failures

LINK

The Lithuanian Court of Appeals has reaffirmed that a company's CEO may be held personally liable for breach of fiduciary duties, improper business decisions and violation of mandatory legal requirements. The decision underscores that failure to convene shareholders' meetings when required by law, as well as delays in initiating insolvency proceedings, can result in civil liability.

If a company's equity falls below half of its registered capital or if insolvency becomes apparent, the CEO must take immediate action, including informing shareholders and initiating the necessary proceedings. Failure to comply with these obligations may result in legal claims and financial consequences for CEOs.if a company's equity falls below half of its registered capital or if insolvency becomes apparent, the CEO must take immediate action, including informing shareholders and initiating the necessary proceedings. Failure to comply with these obligations may result in legal claims and financial consequences for CEOs.

The State Labour Inspectorate press release

LINK

According to the Labor Code (Article 32), the job function is an essential part of the employment contract, specifying the tasks associated with a particular profession or qualification.

The job function must be detailed in a job description, and the employer must provide this information to the employee prior to the start of work. At the employee's request, the employer must provide additional details about the job function within five working days.
While the employment contract should not contain a list of duties, it does define the nature of the work. Job descriptions can clarify these functions, but they must be consistent with the contract. Job functions may be combined if additional duties are performed outside the primary role, or grouped if multiple tasks are performed simultaneously, but this must be clearly agreed upon by both parties.

The State Labour Inspectorate press release

LINK

The State Labour Inspectorate reminds employers of the essential aspects to be considered to avoid errors and ensure smooth leave management. Common employer mistakes in managing annual leave:

- Lack of attention to leave usage
- Lack of leave planning
- Failure to ensure continuous leave
- Unmanaged leave advances and balances
- Late Leave Payments

Recommendation:

- Proactively ensure timely use of leave, which benefits both health and productivity.
- Create a clear leave schedule in advance and involve employees in the planning process.
- Monitor and ensure that employees use their accrued leave.
- Maintain accurate leave records and plan leave carefully.
- Ensure timely payment of leave compensation, taking into account employee preferences.

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

03.2025

ECOVIS ProventusLaw

Bank of Lithuania

LINK

The Bank of Lithuania emphasises the importance of complete and consistent information regarding the shareholders and managers of cryptocurrency companies seeking a licence. While the Bank has received over ten applications for a cryptocurrency service provider licence, most were incomplete and returned for revision. The primary reason for rejection is the failure to submit essential documents necessary to assess the directors and shareholders properly. Under the applicable legislation, directors and shareholders must provide certificates of good repute from both their country of citizenship and residence, if different. Additionally, shareholders must ensure that the origin of their funds is well-documented and consistent. Special attention is given to assessing the suitability of shareholders and directors, particularly in light of the 2025 National Security Threat Assessment published by the Department of State Security. The report highlights an increase in failed financial sector investments in Lithuania by individuals with links to Russia, raising concerns about potential attempts to circumvent international sanctions. The Bank of Lithuania is committed to ensuring that only reliable and transparent entities gain access to the market. Given that a cryptocurrency service provider licensed in Lithuania may offer services throughout the EU, maintaining strict licensing standards is essential to safeguarding both national and EU financial security.

European Securities and Markets Authority

LINK

The European Securities and Markets Authority (ESMA) has issued new guidelines defining when crypto-assets are classified as financial instruments under MiFID II. The guidance confirms that a crypto-asset's economic function and associated rights—rather than its label or whether it is tokenized—determine whether it falls under financial regulation. This ruling provides greater clarity for firms operating in the crypto sector and reinforces the principle of substance over form in regulatory assessments. A crypto-asset will be regulated as a financial instrument if it exhibits the characteristics of transferable securities, derivatives, money-market instruments, or collective investment undertakings, regardless of its label. Unique NFTs generally fall outside MiFID II, but fractionalized NFTs may be considered financial instruments if their division results in a loss of uniqueness. Tokens with both utility and financial features will be classified based on their financial characteristics, not their intended designation.

Trading Environment Matters: A crypto-asset can qualify as a negotiable instrument even if it is not listed on a traditional securities exchange, as long as it is transferable and traded in a capital market-like setting.

Crypto-assets that replicate short-term debt instruments, such as savings tokens pegged to fiat currencies with yield, may be treated as money-market instruments. Meanwhile, synthetic tokens providing exposure to indexes, future prices, or asset baskets could be classified as derivatives, even if settled in cryptocurrency.

European Securities and Markets Authority

LINK

The European Securities and Markets Authority (ESMA) has clarified that under the MiCAR, CASPs cannot designate agents to provide crypto-asset services on their behalf. Unlike the tied agent regime under MiFID II, MiCA does not include provisions allowing third parties to receive and transmit client orders or provide advice on behalf of a CASP.

Article 59 of MiCA stipulates that only authorised CASPs or certain financial entities meeting the notification requirements under Article 60 may provide crypto-asset services within the EU. As MiCA does not establish a regulatory framework for CASP agents, any entity acting in such a capacity must be independently authorised as a CASP.

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