REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

10.2025

ECOVIS ProventusLaw

The European Banking Authority (EBA)

LINK

On 14 October 2025, the European Banking Authority (EBA) published its first comprehensive report on white labelling in EU financial services. The report highlights that white labelling, whereby a financial institution provides products and services under a partner's brand, is widely used and growing, particularly in payments, credit provision, and open banking. Approximately 35% of responding EU banks employ white labelling arrangements, including cross-border applications, often involving non-financial partners such as retail chains, telcos, and BigTechs.

While the model supports innovation, market access, and financial inclusion, it also introduces notable compliance, AML/CFT, consumer protection, and supervisory challenges. Key concerns include opacity regarding the ultimate service provider, potential mis-selling, fraud, reliance on partners' KYC procedures, and limited visibility for NCAs, particularly in arrangements not formally classified as outsourcing or agency. The EBA plans to embed white labelling in its 2026 Union Supervisory Priorities, develop supervisory tools, and promote convergence across NCAs without requiring changes to EU law.

The Financial Action Task Force

LINK

On 24 October 2025, the Financial Action Task Force (FATF) removed Burkina Faso, Mozambique, Nigeria, and South Africa from its list of jurisdictions under increased monitoring, commonly referred to as the "Grey List." Jurisdictions are included on this list when they exhibit strategic deficiencies in AML/ CTF, or proliferation financing frameworks but have committed to addressing these deficiencies in cooperation with the FATF. Removal from the Grey List reflects substantive progress in remedying the identified deficiencies. The FATF continues to encourage a risk-based approach to financial flows while safeguarding legitimate humanitarian and non-profit activities.

The European Supervisory Authorities

LINK

On 9 October 2025, the European Banking Authority (EBA) published its report addressing ML/TF risks in crypto-asset services, drawing on recent supervisory cases across the EU. The report highlights persistent vulnerabilities among CASPs, including unlicensed operations, forum shopping between jurisdictions, weak AML/CFT frameworks, and complex or opaque ownership structures. Notably, some firms attempted to circumvent oversight through multi-entity networks, offshore structures, and misuse of reverse solicitation.

Key findings underscore widespread gaps in customer due diligence, sanctions screening, Travel Rule compliance, and staff training, particularly among smaller operators such as crypto-ATM providers. Supervisory authorities also identified high-risk partnerships and attempts by CASPs to acquire banks or affiliate with previously sanctioned entities to maintain operations.

The report emphasizes the critical role of the new EU framework, including MiCA, the upcoming AML Regulation (AMLR), and the Sixth Anti-Money Laundering Directive (AMLD6), to enhance governance, beneficial ownership transparency, and cross-border supervisory coordination. Until the AMLA becomes fully operational by 2028, national competent authorities retain primary oversight, with EBA and ESMA coordinating crypto-specific supervisory efforts.

The report functions primarily as a strategic reference, outlining regulatory expectations and priorities, rather than providing operational guidance or compliance templates. It signals that governance, ownership transparency, risk management, and cross-border oversight will be focal areas for supervisory attention under the evolving EU crypto regulatory framework.

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

10.2025

ECOVIS ProventusLaw

New consumer protection measure for payment services

LINK

Banks, credit unions, electronic money and payment institutions have begun checking whether the name of the payment recipient matches the name of the account holder. This new safeguard is designed to prevent fraud and accidental misdirected payments. This EU-wide “beneficiary name check” service aims to ensure that funds are transferred to the intended person or company. It will help reduce both social-engineering fraud scenarios and cases where money is sent to the wrong account by mistake.

The Bank of Lithuania has built the technical infrastructure within the CENTROlink payment system to enable participants to offer this service to their customers. Seventy financial institutions have already completed testing and are now providing this functionality.

The recipient’s details are checked before the user confirms the payment — immediately after the account number and recipient name are entered. The payer will see one of four messages:

1. Full match – the name fully matches the actual account holder.
2. Close match – minor differences (e.g. typo, missing symbol); the system will show the corrected information. Note: company names must be written in full with legal form (e.g. UAB, AB, VšĮ).
3. No match – significant discrepancy, a possible sign of error or fraud. This may also appear if you saved templates such as “Mom” or “Electricity bill”; enter the full legal name instead.
4. Unable to verify – e.g. transfer outside the euro area or technical issues; the provider must inform you and state the reason.

Important: verification results are shown only within the payment service provider’s environment (online banking, app, or branch) and only when initiating a payment. Banks and other providers will never send emails or SMS with links asking you to verify a recipient or enter personal data.

Full information on the beneficiary name check service is available on the Bank of Lithuania website.

Our recommendations:

Financial institutions should ensure clear communication to customers about the new beneficiary name-check step and proactively warn that validation messages will appear only inside the secure banking environment. Internal fraud-response and customer-support teams should be trained to treat “no match” and “unable to verify” cases as potential fraud triggers and be prepared to guide users accordingly. Institutions should also review and update their own payment templates and client instructions to reduce false mismatches caused by abbreviations, incomplete names or legacy templates.

Bank of Lithuania Publishes 2026 Fee Schedule for Financial Market Supervision

LINK

The Bank of Lithuania has released the maximum supervision fee rates and forecasted total amounts for 2026 for various groups of supervised financial market participants.

Key highlights:

- For credit institutions (and foreign bank branches established in Lithuania outside the EEA), the fee base is average annual assets, with a maximum rate of 0.0153%, forecasting a total fee pool of about €10.218 million.
- For EEA-licensed foreign bank branches established in Lithuania: rate 0.00513%, forecast of €0.590 million.
- For consumer credit lenders (excluding credit institutions and their branches): rate 0.0125%, forecast of €0.132 million.
- For electronic money institutions and foreign-licensed branches in Lithuania: rate 0.65%, forecast of €3.022 million.
- For payment services institutions: rate 0.65%, forecast €0.778 million.
- A new item: “Institutions issuing asset-backed tokens” (under the crypto regulation) have a fee base of annual revenues and a forecast minimum payment of €3,000.
- The total forecasted supervision fees across all categories for 2026 amount to around €19.31 million.

Implications for market participants:

- Supervised entities should review their applicable fee base (assets, revenues, or other metric) and anticipate the supervision cost under the new schedule.
- The fee rates differ significantly by category of institution - from large credit institutions to fintech/payment service providers and crypto-related firms.
- Entities newly subject to supervision under evolving regulation (e.g., token issuers, crypto service providers) must note the minimum fee thresholds (€3,000) and ensure budgeting appropriately.

This schedule gives transparency and enables institutions to budget ahead for 2026 supervision costs and align internal financial planning accordingly.

Detailed and full Regulatory Compliance report on Payment Services Regulation

REGULATORY COMPLIANCE UPDATE

PERSONAL DATA PROTECTION AND ICT REGULATION

10.2025

ECOVIS ProventusLaw

EDPB and European Commission Publish First Joint Guidelines on DMA-GDPR Interplay for public consultation

LINK

The European Data Protection Board (EDPB) and the European Commission have jointly endorsed new guidelines clarifying how the Digital Markets Act (DMA) aligns with the General Data Protection Regulation (GDPR).

The guidelines explain how the DMA and GDPR operate together: both aim to protect individuals in digital environments, though with different and complementary objectives - the GDPR safeguards rights and privacy, while the DMA promotes fairness and contestability in digital markets. Many DMA obligations involve personal data processing and refer directly to GDPR concepts. The new document clarifies how such provisions should be implemented so that DMA compliance does not breach EU data protection law. Examples include choice and valid consent under Article 5(2) DMA when combining or cross-using personal data in core platform services, and provisions on third-party app distribution, data portability, access requests and interoperability of messaging services.

The Court of Justice of the European Union narrows/clarifies scope of "personal data" in pseudonymised transfers; sets aside General Court ruling on 4 September 2025

LINK

The Court of Justice of the European Union (hereinafter - CJEU)

CJEU set aside the General Court's judgment which had annulled an EDPS decision concerning the Single Resolution Board (hereinafter – SRB) transfer of pseudonymised comments to Deloitte in the Banco Popular resolution context.

The CJEU held that:

- **Personal opinions are personal data** by their nature, as they express the author's thinking and are inherently linked to that person - the EDPS did not need to re-examine content/ purpose/effects to conclude that the data "related" to the commenters.
- **Pseudonymised data are not always personal data for everyone,** depending on whether the recipient can re-identify the person under the circumstances - reiterating previous case-law.
- **Information-duty is judged at collection and from the controller's perspective,** not from the recipient's (Deloitte's) point of view after pseudonymisation - SRB had to inform data subjects before transfer regardless of Deloitte's ability to identify.

Coordinated Enforcement Framework: EDPB selects topic for 2026

LINK

At its October plenary, the European Data Protection Board (EDPB) set the theme for its next Coordinated Enforcement Framework (CEF) action. In 2026, authorities across Europe will focus on how organisations meet the GDPR's transparency duties (Articles 12–14) — ensuring people know when and how their data is used.Through the CEF, national Data Protection Authorities (DPAs) investigate the same topic in parallel, then share findings for an EU-wide analysis. This joint effort promotes consistent enforcement and stronger cooperation.

EDPS unveils revised Guidance on Generative AI, strengthening data protection in a rapidly changing digital era

LINK

The European Data Protection Supervisor (EDPS) published its revised and updated guidelines on the use of generative Artificial Intelligence (AI) and processing of personal data by EU institutions, bodies, offices, and agencies (EUIs), reflecting the fast-moving technological landscape and the evolving challenges posed by generative AI systems.

This updated guidance reinforces the EDPS' commitment to advising EUIs to help them fully comply with their data protection obligations set out in Regulation (EU) 2018/1725.

Credit rating agency Experian fined €2.7M for GDPR violations

LINK

The Dutch Data Protection Authority (DPA) has imposed a €2.7 million fine on Experian for breaching the General Data Protection Regulation (GDPR). Experian, a major credit reporting company providing data to telecom operators, online retailers, and landlords, was found to have violated several key transparency and data protection requirements. The investigation, launched in 2023 following multiple complaints, revealed that Experian failed to explain the reasons for collecting certain personal data. Moreover, the company did not provide individuals with sufficient information regarding how their data was used - and, in some cases, failed to inform them that their data was being processed at all.

Extension of UK adequacy decisions: EDPB adopts opinions

LINK

The EDPB adopted two opinions on the European Commission's draft decisions on the extension of the validity of the UK adequacy decisions under the *General Data Protection Regulation (GDPR)* and the *Law Enforcement Directive (LED) until December 2031.*

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 10.2025

ECOVIS ProventusLaw

The European Council of the European Union

LINK

EU Adopts 19th Sanctions Package Against Russia

The European Union has approved its 19th package of restrictive measures against Russia, expanding sanctions across energy, finance, and technology. The package introduces a phased ban on Russian liquefied natural gas (LNG), ending short-term imports within six months and all long-term contracts by 2027.

New measures extend asset freezes and restrictions to additional Russian banks, crypto service providers, and third-country intermediaries involved in sanctions evasion. The EU also imposes tighter limits on the movement of Russian diplomats and enhances coordination on enforcement and circumvention tracking.

This marks the most extensive EU sanctions update since 2023, targeting key revenue channels of Russia's war economy while signalling stronger scrutiny of financial and crypto-linked transactions.

European Securities and Markets Authority

LINK

On 16 October 2025, the European Securities and Markets Authority (ESMA) published its Second Consolidated Report on Sanctions, providing a comprehensive overview of enforcement actions taken by national securities markets supervisors across the European Union in 2024.

The report shows that over 970 administrative sanctions and other measures were imposed, a level broadly consistent with 2023, while the total value of fines exceeded €100 million. Most significant sanctions continue to relate to infringements of the Market Abuse Regulation (MAR) and the Markets in Financial Instruments Directive II (MiFID II).

The report provides detailed breakdowns by type of sanction, revealing that more than 60% were financial penalties and around 10% were imposed via settlement procedures, which collectively accounted for over €20 million.
ESMA notes considerable variation among national authorities in sanctioning practices and emphasises the need for greater consistency across the Union, highlighting that sanctions are one of multiple tools to enforce compliance and protect market integrity.

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

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

10.2025

ECOVIS ProventusLaw

State Labour Inspectorate on application to labour dispute

LINK

In order to protect violated rights, it is important to take into account the deadlines for applying to the labor dispute commission established in the Labor Code: a participant in labor relations may apply to the labor dispute commission with a request to examine a labor dispute within 3 months, and in cases of unlawful dismissal, unlawful termination of employment, and violation of a collective agreement, within one month of becoming aware or should have become aware of the violation of their rights.

State Labour Inspectorate on illness

LINK

With the number of cases of illness on the rise, the State Labor Inspectorate (VDI) reminds employers that they must comply with the procedures established by law regarding the payment of sick pay and employee rights in matters of leave and employment relationships.

Key observations:

- The first days of illness are paid by the employer;
- Transfer of vacation due to illness;
- Dismissal due to illness – prohibited;
- No work during sick leave;
- Extension of the probationary period;
- Remote work if no sick leave certificate has been issued.

State Labour Inspectorate on working days before holidays

LINK

Working hours are not reduced only for those employees who are subject to reduced working hours, such as healthcare professionals, teachers, lecturers, pharmacists, and others, as well as public sector employees whose working hours are reduced due to raising children under the age of three.

Key points to note:

- If an employee works in several positions for the same employer, the total length of the working day is shortened, rather than separately for each position.
- If a work shift begins on the day before a public holiday and ends on the public holiday itself, it is shortened by one hour.
- If public holidays fall consecutively, working hours are reduced before each public holiday.
- If an employee works two shifts, both of which fall on the day before a public holiday, each shift is reduced by one hour.

Work will no longer be able to follow you home: employees' right to "switch off" will be strengthened

LINK

The Seimas is considering amendments to the Labor Code that would clearly establish the right of remote workers to "disconnect" - not to answer calls, respond to emails, or other digital inquiries after official working hours.

The initiators of the amendments to Article 52 of the Labor Code seek to establish that: "An employee has the right to disconnect from digital devices and be unavailable to the employer outside working hours."

In this way, the initiators of the amendment to the Labor Code seek to ensure the right of employees to turn off their digital devices in order to protect their physical and mental health and well-being and to remain unreachable during non-working hours.

Decision of the Civil Division of the Supreme Court of Lithuania

LINK

The Supreme Court (LAT) clarified that Labour Code rules on pay for work performed on rest days are mandatory. Under Article 144(1), employees must receive double pay if they work on a rest day at the employer's request. However, if the change in schedule is initiated by the employee for personal reasons, double pay does not apply. The LAT emphasized that this rule aims to protect employees from unexpected schedule changes imposed by employers. The employer bears the burden of proving that any schedule change occurred at the employee's request.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

CONSUMER PROTECTION

10.2025

ECOVIS ProventusLaw

The Bank of Lithuania

LINK

On 13 October 2025, the Bank of Lithuania together with the European Supervisory Authorities, issued a warning concerning the risks associated with crypto-assets and the limited consumer protection available in this sector. The statement emphasised that, while crypto-assets may contribute to innovation and competition within the EU financial system, not all such assets or services fall under the scope of MiCA Regulation, leaving consumers potentially unprotected. It was underlined that MiCA applies to electronic-money tokens and asset-referenced tokens, but not to unique NFTs, which remain outside the regulatory perimeter. Consumers were urged to verify whether service providers are licensed within the EU, assess the security and reliability of custody arrangements, and exercise heightened caution when engaging with non-EU or unlicensed platforms, which may pose significant financial and operational risks.

Our recommendations:

- Verify the licensing and MiCA status of all partner or third-party crypto-asset service providers before any cooperation or referral.
- Strengthen due diligence and client-risk assessments for customers engaging with unregulated or third-country crypto platforms.
- Ensure that custody arrangements and wallet structures provide clear segregation and transparency on client-asset protection.

The Bank of Lithuania

LINK

Lithuanian Central Bank Urges Crypto Service Providers to Finalize Licensing and Inform Clients

Wth the transition period ending on December 31, 2025, the Bank of Lithuania reminds virtual currency exchanges and wallet operators that only licensed entities will be allowed to provide crypto-asset services. Both service providers and clients are urged to prepare for the new regulatory regime.

Since early 2025, nearly 50 companies have applied for a crypto-asset service provider license, yet only one has been approved. Many submissions lacked sufficient preparation, failing to meet even the minimum licensing requirements. The Bank is reviewing several pending applications and aims to finalize them by the end of the year. Operators not seeking a license must inform clients promptly of their intention to cease operations and provide clear asset withdrawal instructions. Unlicensed activity after the deadline may result in blocked websites and public listing as illegal entities.

The Bank also urges investors to confirm whether their chosen providers are licensed or in the process of obtaining authorization, emphasizing that using unlicensed operators could expose them to significant financial and legal risks.

Our recommendations:

Financial institutions and regulated entities should enhance due diligence on counterparties offering crypto-related services and ensure cooperation only with licensed providers.

Court of Justice of the European Union

LINK

Consumer protection rights travel with the assigned claim

The company took over the consumer claims arising from the contract with the bank. The bank argued that the company could not make claims against it arising from consumer legal relations.

Objective of ensuring a high level of protection for consumers precludes a broad interpretation of the concept of waiver referred to in Article 22(2) of Directive 2008/48, as envisaged by the referring court, which would also result in the prohibition of the assignment of rights which those consumers derive from that directive. Such assignment is one of the legal options, which may be provided for by the national legal system, to allow consumers to defend their rights by sparing themselves difficulties and costs that might deter them from taking steps personally in relation to the seller of supplier concerned.

Article 22(2) of Directive 2008/48 must be interpreted as not precluding national legislation that allows a consumer to assign a claim arising from the infringement of a right conferred on him or her by the national legislation implementing the directive to a third party which is not a consumer.

It is not necessary, in order to ensure the effectiveness of the system of consumer protection intended by Directive 93/13, for the national court, hearing a dispute between two sellers or suppliers, such as a company which is the assignee of the rights of a consumer and the seller or supplier which is the other party to the contract with that consumer, to examine of its own motion whether a clause in the contract concluded by that consumer is unfair.

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

CRYPTO

10.2025

ECOVIS ProventusLaw

The Bank of Lithuania

LINK

On 27 October 2025, the Bank of Lithuania provided an update on the status of applications for authorization as a CASP. Since the beginning of the year, nearly 50 applications have been submitted, with a small number currently under review and one license granted. The Bank aims to issue decisions on the applications under review before the end of the year. Recent submissions have largely not met the Bank's foundational requirements. The Bank emphasizes that applicants should carefully consider their readiness before filing, as incomplete or inadequate applications may not be accepted, and that the number of CASP licenses to be granted this year is limited.

The Financial Stability Board (FSB)

LINK

On 16 October 2025, the Financial Stability Board (FSB) published the findings of its first peer review assessing the implementation of its Global Regulatory Framework for Crypto-Asset Activities, including recommendations for CASPs and global stablecoin arrangements (GSCs). The review indicates that while jurisdictions have made progress in regulating crypto markets, significant gaps remain, particularly in the oversight of stablecoins, cross-border coordination, and financial stability risk management.

Key findings include limited adoption of comprehensive stablecoin regulation, inconsistent frameworks across jurisdictions, and underdeveloped supervisory measures for liquidity, prudential oversight, and risk reporting. Most regulators continue to focus primarily on anti-money laundering, counter-terrorist financing, and consumer protection. The report highlights that fragmented rules and regulatory inconsistencies may encourage regulatory arbitrage, reduce interoperability, and pose potential systemic risks in the stablecoin sector.

The European Systemic Risk Board

LINK

On 20 October 2025, the European Systemic Risk Board (ESRB) published its 2025 assessment of systemic risks stemming from crypto-assets, with a focus on stablecoins, crypto-investment products (CIPs), and multi-function groups (MFGs). The report underscores that risks from crypto-assets have moved beyond theoretical concerns and now pose macro-financial relevance.

Key observations include the predominance of USD-backed stablecoins, accounting for nearly all market capitalization, which exposes the EU to U.S. monetary and policy shifts. Multi-issuer stablecoin models, where the same token is issued inside and outside the EU, create regulatory gaps, heightening contagion risk in case of runs. While MiCA provides a regulatory foundation, it currently lacks targeted tools to address cross-jurisdictional schemes and potential liquidity stress.

The report also notes rapid growth in CIPs, significant institutional adoption, and rising complexity of MFGs that combine issuance, trading, and custody functions, introducing conflicts of interest, governance opacity, and systemic risk potential. ESRB further highlights cyber resilience gaps for non-EU linked entities and supports DORA as a baseline framework while calling for expanded supervisory measures and international coordination.

European Securities and Markets Authority

LINK

On 25 September 2025, the European Securities and Markets Authority (ESMA) clarified responsibilities under the MiCA Regulation for crypto-assets admitted to trading prior to 30 December 2024, often referred to as "legacy" tokens.

ESMA confirmed that offerors and persons seeking admission to trading of these legacy crypto-assets are only required to comply with MiCA marketing communication rules and are not obligated to prepare new white papers. Operators of trading platforms, however, must ensure that by 31 December 2027 a MiCA-compliant white paper is prepared, notified, published, and updated as required. Other CASPs, pursuant to Article 66(3) of MiCA, are required only to provide hyperlinks to any existing registered white papers and are not responsible for creating new ones. Crypto-assets not listed on trading platforms may remain without a MiCA white paper beyond 2027.

This three-year transition window allows platforms to align documentation and act as key compliance gatekeepers for pre-MiCA tokens.

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

Our recommendations and details are in this file

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

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:

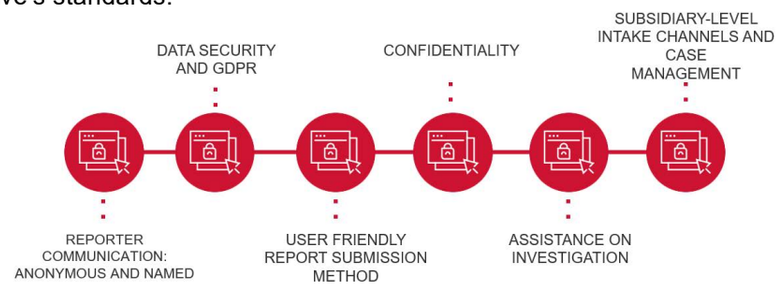
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors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