REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

11.2025

ECOVIS ProventusLaw

Center of Excellence in Anti-Money Laundering

LINK

The Center of Excellence in Anti-Money Laundering conducted an analysis highlighting the issues faced by market participants in the field of money laundering. While preparing the report, the following observations were made:

- The most frequently mentioned breaches are Articles 9, 17, 22, and 29 of the Law on the Prevention of Money Laundering and Terrorist Financing. These are the core provisions covering the obligations of obliged entities. Focusing on these areas can help prevent systemic errors and avoid significant fines.
- The severity of breaches is not fully clear. Sanctions range from warnings to license revocation. To understand where mistakes occur most often, close cooperation between the public and private sectors is particularly important. Only together can recurrence be prevented.
- Strengthening competencies, client identification remains the area in which errors most frequently occur. Training, workshops, and practical sessions focused on recurring mistakes are essential.
- Future challenges, the entry into force of EU-level legislation, such as the AMLA Regulation and the Sixth AML Directive, implies an even greater need for adaptation and investment in prevention systems.

The Center of Excellence in Anti-Money Laundering values the contribution of market participants in building a sustainable, resilient, and effective financial system, in which prevention functions as a natural part of organizational culture and mistakes are seen as opportunities to improve and strengthen trust.

The European Parliament

LINK

In November 2025, the European Parliament issued an in-depth analysis on the future of EU AML policy, outlining how the new AML framework and the creation of AMLA will transform supervision across the Union. The report stresses that digital finance, particularly crypto-assets, blockchain-based activity and decentralised finance, has become central to modern financial-crime risk, with laundering techniques increasingly shifting from physical channels to digital, cross-border networks. It further confirms that CASPs are fully integrated into the category of obliged entities and must now comply with CDD, monitoring and reporting requirements comparable to those imposed on traditional financial institutions. At the same time, the analysis notes that fully decentralised models remain largely outside existing regulatory coverage and emphasises that AMLA will need sophisticated technological tools, including blockchain analytics and real-time monitoring, to address these gaps. The report also highlights that AMLA, working alongside the EBA and ESMA, will coordinate EU-level oversight of crypto-asset activity as part of a broader effort to position the Union as a global leader in digital-finance AML standards.

FATF

LINK

In October 2024, the FATF released comprehensive guidance on asset recovery, representing the most extensive modernisation of global confiscation standards in several decades. The document redefines asset recovery as a complete operational cycle encompassing detection, tracing, interim restraint, confiscation, management and, where appropriate, the return of assets to victims or jurisdictions. It frames these stages within a structured, policy-driven lifecycle that integrates financial investigation techniques with clear safeguards for fundamental rights and due process. The guidance places particular emphasis on the need for rapid interim measures, acknowledging that digital payments and crypto-asset transfers can remove assets from reach within moments. It elevates non-conviction-based confiscation to the same level of legitimacy as conviction-based approaches, signalling a significant shift in FATF expectations. Cross-border enforcement is strengthened through revised standards obliging jurisdictions to recognise and act on both provisional and final foreign orders. Throughout the paper, extensive case studies illustrate practical implementation across traditional and digital-asset contexts, while underscoring the requirement that all powers operate within a proportionate and rights-respecting 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

11.2025

ECOVIS ProventusLaw

Bank of Lithuania Enhances Implementation of European Supervisory Authorities' Guidelines

LINK

To provide greater regulatory clarity for financial market participants, the Bank of Lithuania has reviewed and improved its practice of implementing guidelines and recommendations issued by the European Supervisory Authorities (ESAs).

Starting 1 September 2025, following the entry into force of the Board Resolution on the application of certain ESA guidelines, the Bank of Lithuania will no longer issue separate decisions of the Financial Market Supervision Committee or Board resolutions confirming compliance with specific ESA guidelines - except in cases where this is necessary to ensure financial stability or consumer protection. This change aims to enhance transparency, simplify communication with supervised entities, and improve operational efficiency.

A new dedicated webpage on the Bank of Lithuania's website will continuously publish and update the list of ESA guidelines applicable to the Lithuanian financial market. The list will indicate which specific guidelines and recommendations are relevant for each type of financial market participant.

Decisions of the Financial Market Supervision Committee

LINK

The Bank of Lithuania has imposed a fine and additional obligations on the electronic money institution Paysera LT, UAB after determining that the institution failed to comply with previously issued supervisory instructions. Earlier in September, the Bank of Lithuania fined Paysera LT, UAB for failing to submit its annual and quarterly financial statements. The institution was instructed to provide these statements and a corrective action plan by 30 September of this year to ensure that similar breaches would not occur in the future. Paysera LT, UAB did not fully comply with the Bank's instructions. While its quarterly reports were eventually submitted with minimal delay (for which no additional sanction was applied), the action plan was submitted with significant delay and was incomplete. The annual financial statements have still not been submitted. For failing to submit its annual financial statements by the required deadline (a delay now amounting to seven months), the Bank of Lithuania has imposed a fine of EUR 20,000 on the institution.

Decisions of the Financial Market Supervision Committee

LINK

The Bank of Lithuania has determined that the electronic money institution Curve Europe UAB failed to approve its annual financial statements and profit (loss) allocation decision after the end of the financial year, and did not submit its audited financial and activity reports to the Bank of Lithuania within the required deadlines.

In line with applicable procedures, Curve Europe UAB approached the Bank of Lithuania requesting the possibility to enter into an administrative agreement. After evaluating that the institution acknowledged the violations and has already remedied them, the Bank of Lithuania decided to conclude an administrative agreement. Taking into account the significant delays in the submission of required data and other relevant circumstances, the Bank of Lithuania imposed a fine of EUR 22,500 on the company.

Detailed and full Regulatory Compliance report on Payment Services Regulation

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

PERSONAL DATA PROTECTION AND ICT REGULATION

11.2025

European Commission Proposes Revisions to GDPR and Other Digital Rules Under Digital Omnibus Package

LINK

The European Commission has presented its Digital Omnibus Package, a wide-ranging update to EU digital legislation aimed at simplifying rules, reducing administrative burdens, and providing more legal certainty for businesses. If adopted, the package would introduce significant changes to data protection, cookie rules, cybersecurity, and the EU AI Act.

Key proposals include:

• Revised definition of personal data: GDPR would exclude information where identification of an individual is unlikely or legally prohibited.

• AI development and deployment: Processing personal data for AI training and development would be recognized as a legitimate interest.

• Expanded exemptions to data subjects' rights: Controllers could refuse access requests in cases of abuse or charge reasonable fees, particularly for scientific research purposes.

• EU-wide data breach reporting: A single-entry portal would simplify breach notifications across multiple EU laws.

• Harmonized DPIA guidance: The EDPB would create EU-wide lists of processing activities that require or do not require a Data Protection Impact Assessment (DPIA), along with a standardized template and methodology.

Data Protection: Online Marketplace Operators Are Controllers of Personal Data Published on Their Platforms

LINK

The Court of Justice of the European Union (Hereinafter - CJEU) has clarified that operators of online marketplaces are considered controllers of personal data contained in advertisements published on their platforms. Accordingly, before publishing such ads, they must, among other things, identify listings containing sensitive personal data and verify whether the user posting the ad is indeed the person whose data is included, or has obtained explicit consent from that individual.

EU law obliges online marketplace operators to assume responsibility for personal data in ads published on their platform under the GDPR. This includes implementing appropriate technical and organizational measures to identify listings with sensitive data before publication and to verify that the user posting the ad has the right to do so. If consent cannot be confirmed or another GDPR exception does not apply, the operator must refuse to publish the listing.

EDAPP Publishes New Guidelines for AI System Risk Management

LINK

The European Data Protection Supervisor (Hereinafter - EDPS) has published new guidance to help data controllers assess and manage data protection risks when developing, acquiring, and deploying Artificial Intelligence (AI) systems under the EUDPR (Regulation 2018/1725).

The guidance provides practical recommendations for managing key risks related to fairness, accuracy, data minimisation, security, and data subjects' rights. It highlights technical measures that can be used to mitigate these risks, though organizations are still responsible for assessing their specific AI systems.

VDAI Issues Reprimand for Delayed Response to Data Subject Request

LINK

The Lithuanian Data Protection Authority (hereinafter - VDAI) has issued a new decision concerning a company that failed to respond to a data subject's access request within the one-month deadline required by the GDPR.

The individual stated that they had contacted the Lithuanian company several times, requesting information on whether their personal data was being processed, on what legal basis, and how its security was ensured. The company did not respond in time.

During the investigation, the organisation acknowledged that it had received the access request on 14 May 2024 but replied only on 10 September 2024 due to a human error.

The DPA confirmed that the organisation breached GDPR Article 12(3) by failing to respond within one month. Since the company ultimately provided the required information and the violation concerned only one data subject, the authority considered the case minor and issued a formal reprimand under Article 58(2)(b) GDPR rather than stricter corrective measures.

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 11.2025

ECOVIS ProventusLaw

The Council of the European Union

LINK

The EU adopted Council Decision (CFSP) 2025/2032 introducing additional restrictive measures in response to actions by the Russian Federation destabilising Ukraine. The measures include prohibitions on the import of Russian LNG, a transaction ban on specified Russian energy companies, expanded restrictions on petroleum products and liquefied-petroleum gas, sanctions targeting Russia-linked banks and payment systems, and limitations on certain crypto-asset and fintech services.

According to the High Representative's statement, a number of non-EU countries have formally aligned themselves with this Decision. These countries are North Macedonia, Montenegro, Albania, Bosnia and Herzegovina, Iceland, Liechtenstein, Norway, Ukraine, Georgia and Moldova. By aligning, they commit to implementing the restrictive measures in their respective national frameworks.

As a result, the territorial scope of the restrictive regime extends beyond the EU, and the aligned third-country jurisdictions are expected to enforce equivalent prohibitions on relevant imports, financial transactions and services connected to Russian energy, financial and technology sectors.

The Council of the European Union

LINK

On 20 November 2025, the Council of the European Union adopted Council Decision (CFSP) 2025/2357, amending Council Decision (CFSP) 2024/1484 concerning restrictive measures in view of the situation in Russia. The amendment adds ten further natural persons to the EU sanctions list. The newly designated individuals are associated with serious human-rights violations in the Russian Federation, including torture and other cruel or degrading treatment within detention and penal facilities, systemic repression of civil society and media actors, and politically motivated prosecutions targeting activists, journalists and opposition representatives.

The restrictive measures apply immediately upon publication of the amendment. The listed individuals are subject to an asset freeze and a prohibition on EU persons and entities making funds or economic resources available to them. They are also subject to a travel ban, preventing their entry into or transit through EU territory.
This expansion forms part of the EU's broader human-rights restrictive-measures framework, initiated in 2024 and progressively extended to address continued violations of fundamental freedoms and the rule of law in Russia.

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

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

11.2025

ECOVIS ProventusLaw

Changes to the Income Tax Act (GPMĮ)

LINK

The Seimas has approved significant changes to personal income taxation. New amendments to the Personal Income Tax Act (GPM) adopted by the Seimas will come into force as of January 1, 2026. These changes will affect many residents, especially those who earn above-average incomes or are self-employed.

Progressive rates:
• Up to 36 VDU (average wage) – 20 %;
• 36–60 VDU (average wage) – 25 %;
• More than 60 VDU (average wage) – 32 %.

The following are included in the annual income:
• Income from employment;
• Income from individual activities according to a certificate;
• Royalties and remuneration for activities in management bodies;
• Royalties from the employer;
• Income of an MB manager who is not a member of that community for management activities;
• Income from the sale of waste – over 12 VDU (average wage) of the annual portion;
• Income from a business certificate – over EUR 50,000 of the annual portion;
• Annual income from non-employment relationships exceeding 12 VDU (average wage).

Non-taxable income amount (NPD) from 2027:
• €1,044 additional annual NPD for each child – for employees working under an employment contract;
• €208.80 – additional tax credit for each child for parents engaged in individual activities;
• The relief applies only after the end of the tax period, when declaring annual income.

The government proposes that the Seimas wait for the European Commission's decision on the right to disconnect from work after hours

LINK

Following the European Commission's launch of consultations on the right of employees to disconnect from computers and other digital devices after working hours, the Government is proposing that the Seimas refrain from rushing into decisions on this issue.

The Cabinet of Ministers urges to wait for the future European Commission directive, which Lithuania, together with other Member States, will have to transpose into national law.

VDI: Psychological violence in the workplace is not a personal conflict, but a violation of labour law

LINK

Psychological violence is considered to be constant or repeated humiliating, hostile, or offensive behaviour aimed at intimidating, belittling, or pushing an employee into a helpless position. Such behaviour is prohibited not only during working hours, but also during breaks, on the way to and from work, during work-related events, and during communication, including communication via information and electronic communication technologies.

It is very important that the first step an employee takes when experiencing unacceptable behaviour from a colleague or even their immediate supervisor is to contact their employer. The company manager must take measures to resolve the situation, and if they fail to do so or themselves engage in psychological abuse of the employee, then the employee can contact the State Labor Inspectorate.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

CRYPTO

11.2025

ECOVIS ProventusLaw

IOSCO

LINK

On 11 November 2025, IOSCO published its final report on the tokenisation of financial assets. The report notes that while the concept of tokenising traditional financial assets (such as securities or funds), using distributed ledger technology (DLT), is gaining interest, actual adoption remains limited. The potential benefits of tokenisation include faster settlement cycles, increased collateral mobility, and theoretical operational efficiencies. However, IOSCO warns that tokenisation also introduces new and evolving risks. These include legal uncertainties, operational and cybersecurity vulnerabilities related to DLT-based infrastructure, and possible challenges in ensuring true asset ownership or claim over the underlying assets. Because tokenised assets may rely on third-party issuers or custodians, token holders might not have the same rights as holders of traditional assets, creating counterparty risks and potential investor confusion about what is actually being purchased. Finally, IOSCO highlights that tokenisation could create "spill-over" effects if tokenised assets become more deeply tied to crypto-asset markets. Failures or disruptions in the tokenisation infrastructure could thus impact broader financial-market stability if not properly managed.

European Commission

LINK

The EU has adopted DAC8, introducing a mandatory tax-reporting framework for crypto-asset service providers. All CASPs, including exchanges, brokers, custodial wallet providers and platforms facilitating crypto transfers, must report customer holdings and transactions to EU tax authorities in a standardised digital format. A new EU-wide registry will assign each operator a unique ten-digit identifier to facilitate cross-border supervision and ensure visibility of entities operating within or into the EU. Data-retention duties are strengthened, requiring CASPs that cease activities or are delisted to retain relevant customer information for twelve months after removal from the registry. The regime applies to both EU-established and non-EU CASPs serving EU residents, thereby preventing the use of offshore structures to circumvent reporting obligations. The rules take effect on 1 January 2026, creating a short transition window for firms to upgrade systems and integrate DAC8 reporting into broader MiCA, AML/CFT and FATF Travel Rule compliance frameworks. The scope and depth of mandatory reporting raise concerns regarding data security and proportionality, but the EU considers DAC8 essential to closing the tax-compliance gap in the crypto sector.

ESMA

LINK

The ESMA Q&A clarifies that under MiCA the classification of a crypto asset service provider's activity, whether exchange of crypto assets, execution of orders, or reception and transmission of orders, depends on the actual operational handling of client orders and not on contractual labels. When a CASP acts as agent, executing orders on behalf of clients, it provides execution services; if it merely forwards orders, it provides reception and transmission of orders. When the CASP trades with its own capital as counterparty, it provides exchange services and must comply with relevant transparency, pricing, and execution obligations. The determination requires fact specific analysis and in cases of doubt, particularly with retail clients, a conservative presumption treats the CASP as acting as agent, triggering best execution and investor protection requirements. Operational practices must therefore align with the authorised service type and documentation should accurately reflect order flows and counterparty relationships.

ESMA

LINK

The Q&A clarifies the allocation of responsibilities under MiCA Regulation for crypto assets (other ARTs and EMTs) that were admitted to trading before 30 December 2024. For such legacy tokens the following regime applies. First, where persons issued or sought admission to trading these tokens (i.e. offerors or applicants), there is no obligation to produce a new MiCA compliant white paper; they need only comply with the MiCA marketing communication rules (Articles 7 and 9) for communications issued after 30 December 2024. Second, operators of trading platforms must, by 31 December 2027, ensure that, for those legacy tokens for which a white paper is required under MiCA, a white paper is drawn up, notified, and published in compliance with Articles 6, 8, 9 and updated under Article 12. Third, other CASPs referenced in Article 66(3) of MiCA (i.e., non platform CASPs providing services such as trading, advisory, portfolio management) have no obligation to prepare a white paper; they must only provide a hyperlink to any existing registered white paper, if one exists. If no white paper exists, for example, for tokens not listed on any trading platform, they are not required to produce one themselves, even after the 31 December 2027 deadline.

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:

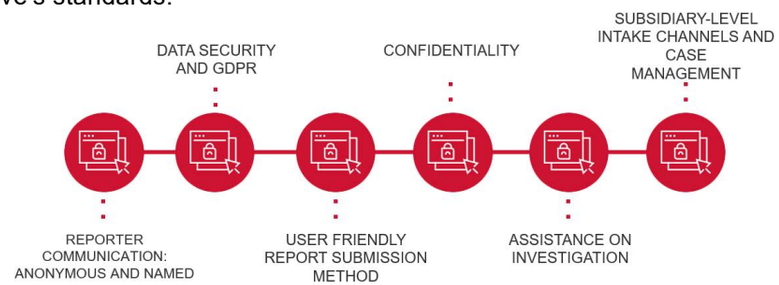
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors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