REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

12.2025

Anti-Money Laundering Authority (AMLA)

LINK

On 16 December 2025, the Anti-Money Laundering Authority (AMLA) adopted two final RTS that establish binding EU-level methodologies for (i) the assessment of inherent and residual ML/TF risk under Article 40(2) of the AML Directive, and (ii) the risk-based selection of obliged entities for direct AMLA supervision pursuant to Article 12(7) of the AML Regulation.

The RTS transform ML/TF risk assessment from a principles-based exercise into a standardised, rule-driven supervisory process. Supervisory authorities are required to apply a single EU risk model, using predefined indicators, data inputs and scoring logic, without national variation. Risk scores are generated through the aggregation of granular data relating to customer profiles, products and services, transaction volumes, geographic exposure, delivery channels and the effectiveness of internal controls. The framework strictly limits the extent to which weak controls may offset inherent risk and constrains supervisory adjustments to narrowly defined, documented circumstances. Review cycles are also formalised, with higher-risk entities subject to more frequent reassessment.

The RTS governing selection for direct AMLA supervision introduces an objective, data-based filtering mechanism. Only entities meeting defined cross-border activity thresholds enter the selection pool, with final designation determined by residual ML/TF risk scores calculated under the harmonised methodology. Group-wide risk is assessed through weighted aggregation rules designed to reflect, rather than dilute, higher-risk exposures, while national supervisory discretion is intentionally curtailed to prevent regulatory divergence.

The European Commission

LINK

The European Commission adopted a delegated act adding Russia to the EU list of high-risk third countries presenting strategic deficiencies in their AML/CFT frameworks.

The Commission's assessment was conducted independently of the FATF process, reflecting the fact that Russia is not currently subject to FATF grey- or black-listing, following the suspension of its FATF membership. Based on a technical analysis drawing on publicly available information, input from Member States and assessments by the European External Action Service, the Commission concluded that Russia meets the criteria for designation as a high-risk jurisdiction under EU AML rules. The delegated regulation is subject to scrutiny by the European Parliament and the Council, which may object within the prescribed scrutiny period before the measure enters into force.

European Securities and Markets Authority (ESMA)

LINK

ESMA published its annual report on Suspicious Transaction and Order Reports (STORs), presenting aggregated data on market abuse reporting across the European Economic Area.

The report indicates a decline in the overall number of notifications, with approximately 6,763 submissions, including 5,981 STORs, representing a decrease of around ten per cent compared to the previous year. ESMA emphasises that this reduction should not be interpreted as a corresponding decrease in market abuse risk, but may instead reflect differences in detection capabilities, escalation practices, or reporting thresholds across firms and jurisdictions. Investment firms continue to account for the majority of reports, underlining their central role in identifying suspicious activity. Equity instruments remain the primary area of concern, with insider dealing constituting the most frequently reported form of suspected abuse. The report also highlights the continued significance of cross-border cases, requiring cooperation between EU and third-country authorities, and notes that a relatively limited number of firms account for most STOR submissions.

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

12.2025

ECOVIS ProventusLaw

EMI and PI Sector Grows as Licensing Income Exceeds EUR 300 Million

LINK

According to the Bank of Lithuania, in the first half of this year the licensing-related income of the electronic money institutions (EMIs) and payment institutions (PIs) sector increased by 13%, while the value of payment transactions grew by more than one fifth.

At the end of the first half of 2025, the market comprised 75 EMIs and 41 PIs. Total licensing income reached EUR 311 million (EUR 275 million in the same period of 2024), while the value of payment transactions amounted to nearly EUR 161 billion (EUR 132 billion a year earlier).

The ten largest institutions by licensing income generated EUR 192 million, accounting for around 62% of total sector income. Similarly, the ten largest EMIs and PIs by transaction value generated approximately 60% of total sector turnover - slightly more than EUR 99 billion.

Updated Complaint Handling Rules

LINK

The Board of the Bank of Lithuania has adopted a decision introducing a revised framework for how financial market participants should handle customer complaints.
The changes aim to ensure consistent practices across the sector and reflect recent legal and regulatory updates.

Key updates include:

- Clarification of the definition of a complaint to prevent varying interpretations;
- Complaints must be handled objectively and impartially, ensuring that the employee involved in the issue is not responsible for processing the complaint. Adequate staff resources and regular training of complaint-handling personnel are required;
- Updated reporting templates for submitting information on complaints to the Bank of Lithuania, enabling classification by service type, nature, and reason, in addition to recording complaint numbers;
- All complaint data must be submitted through the Bank's REGATA information system.

Payment Habits Survey: Lithuanian Residents Value Accessibility Most and Try Digital Innovations

LINK

The latest survey by the Bank of Lithuania on payment habits shows that the vast majority of residents prefer digital payments, increasingly using smart technologies, and more than half of respondents would like to try the digital euro.
In addition, the demand for receiving payment services remotely is growing, and the choice of service provider is determined by its accessibility.

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

12.2025

French data protection authority fines Israeli AdTech company

LINK

France's data protection authority, CNIL, imposed a 1 million EUR fine on Optimove, an Israeli AdTech company, for GDPR violations discovered during an investigation.

In November 2022, an EU-based platform notified the CNIL of a major data breach. Data from 12.7 to 21.6 million EUR users (including 9.8 million in France) - including names, ages, email addresses, and listening habits - had been posted on the dark web.

The platform identified its former subcontractor, which had provided personalized advertising services, as the source of the breach. The CNIL conducted checks in 2023 and 2024, followed by an investigation in 2025, which uncovered multiple GDPR violations by the subcontractor.

Key GDPR Violations Identified by the CNIL

- Failed to delete data after contract termination.
- Processed data beyond controller instructions.
- Lacked records of processing activities. The company failed to maintain a required register of processing activities under Article 30 GDPR.

EDPB gives recommendations to make online shopping more respectful of users' privacy

LINK

The EDPB adopted recommendations on the legal basis for requiring the creation of user accounts on e-commerce websites.
As a general rule, users should have the option to engage with e-commerce websites, including the ability to make purchases, without creating an account. In such cases, the EDPB recommends that e-commerce websites offer a choice: either a 'guest' mode, allowing users make purchases without creating an account, or the option to voluntarily create an account. This approach minimises the collection and processing of personal data, and therefore aligns with the GDPR's principle of data protection by design and by default.
However, mandatory account creation can be justified in a limited number of cases, including for example, offering a subscription service or providing access to exclusive offers.

Strengthening data protection worldwide: EDPB meets with the countries and organisation with an adequacy decision

LINK

As part of its December's plenary meeting, the European Data Protection Board (EDPB) held an online meeting with Commissioners and representatives of Data Protection Authorities (DPAs) from the countries and the organisation with an EU adequacy decision. An adequacy decision is a key-mechanism in EU data protection legislation which allows free flow of personal data from Europe to third countries or an international organisation offering an adequate level of data protection.* To date, the following countries and organisation benefit from this: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom, Uruguay, United States, and the European Patent Organisation.

Commission fines X 120 million EUR under the Digital Services Act

LINK

The European Commission issued its first-ever fine for a violation under the Digital Services Act (DSA), penalizing Elon Musk's social media platform X 120 million EUR (approximately $140 million) for breaching transparency obligations.

The Commission found X violated the DSA in three key areas:

- the deceptive design of its blue checkmark verification system, which allows anyone to purchase "verified" status without meaningful identity verification.
- an inadequate advertising repository that lacks critical information about ad content and advertiser identity.
- and failure to provide researchers with effective access to public data.

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 12.2025

ECOVIS ProventusLaw

The Council of the European Union

LINK

On 22 December 2025, the Council of the European Union renewed and extended the European Union's economic restrictive measures against the Russian Federation in response to its ongoing war of aggression against Ukraine, prolonging the current sanctions regime for a further six months, until 31 July 2026. The extended measures form part of a long-standing suite of restrictive instruments first introduced in 2014 and significantly expanded following Russia's full-scale invasion of Ukraine in 2022. The economic sanctions encompass a broad range of sectoral restrictions, including constraints on trade, finance, energy, technology and dual-use goods, industry, transport and luxury goods; a ban on the import or transfer of seaborne crude oil and specified petroleum products from Russia to the EU; measures restricting access to EU financial messaging systems ("de-SWIFTing") for designated Russian banks; and the suspension of broadcasting activities and licences within the EU of certain Kremlin-linked outlets. The Council underscored that, so long as the Russian Federation continues actions that destabilise Ukraine and violate fundamental rules of international law, the sanctions will remain in force and additional restrictive measures may be adopted as needed.

The Council of the European Union

LINK

On 18 December 2025, the Council of the European Union adopted a new package of restrictive measures targeting Russia's maritime "shadow fleet" in connection with its ongoing war of aggression against Ukraine, designating 41 vessels and their beneficial owners for inclusion under the EU's economic sanctions framework. The measures extend and reinforce existing maritime related restrictions aimed at preventing the circumvention of EU sanctions, particularly those intended to limit Russia's ability to export energy by sea. The designated vessels, forming part of a so called "shadow fleet" used to obscure ownership, flagging or transactional history, are now subject to an EU asset freeze, and EU persons and entities are prohibited from providing them with funds, economic resources or related services, including port access and insurance or reinsurance services. The Council decision also targets the beneficial owners and operators associated with these vessels, applying the same asset freeze and transaction prohibition obligations. This action is intended to close gaps that allow sanctioned commodities, including crude oil and petroleum products, to reach global markets through opaque maritime arrangements designed to evade EU controls. The decision underscores the EU's commitment to strengthening enforcement of its economic sanctions regime and addressing sanctions evasion practices.

The Council of the European Union

LINK

On 15 December 2025, the Council of the European Union adopted significant extensions to the EU's restrictive measures in response to hybrid threats emanating from the Republic of Belarus and the Russian Federation. The Council's actions target persons and entities involved in information manipulation, cyber operations and other destabilising activities that pose risks to the security, democratic processes and stability of EU Member States. In respect of Russia, the Council designated twelve individuals and two entities for their roles in disseminating disinformation and engaging in cyber activities detrimental to EU interests. Under the extended measures, these designated persons and entities are subject to an EU asset freeze, and EU persons and entities are prohibited from making funds or economic resources available to them directly or indirectly. In parallel, the Council broadened the scope of the sanctions regime applicable to Belarus to expressly cover hybrid activities directed against the EU. The expanded measures extend existing asset freeze and transaction prohibition obligations to include individuals and entities engaged in disinformation, cyber interference and other activities aimed at undermining the security, democratic integrity and societal cohesion of EU Member States. Together, these measures form part of the EU's comprehensive approach to countering hybrid threats, underscoring the Union's determination to hold accountable those engaged in manipulative information operations and malicious cyber conduct, regardless of whether they are directly linked to traditional territorial conflict.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

12.2025

ECOVIS ProventusLaw

VDI: From January 1, 2026 – higher minimum wage

LINK

The minimum wage in Lithuania will change on January 1, 2026. As of this date, the minimum hourly wage (MVA) must be at least €7.05, and the minimum monthly salary (MMA) will be €1,153. It is important to note that this is a gross wage, i.e., before taxes so that the actual take-home pay may vary depending on the amount of taxes paid, the applicable tax-free income amount, tax breaks, and other individual circumstances.

When does the old minimum wage apply, and when does the new one apply?

It should be noted that when paying wages for December 2025 in January 2026, the minimum wage applicable in 2025 will apply, i.e., €1,038 per month or €6.35 per hour. This means that the salary amount is determined according to the period for which the wages are calculated, not according to the date of payment.

Minimum wage – only for unskilled work

We would like to remind you that the minimum wage applies only to unskilled work, either for one hour of work or for the standard working time for a calendar month. According to Article 141(2) of the Labour Code, unskilled work is work that does not require any special qualifications or professional skills. If skilled work is performed, the wage must be higher than the minimum wage, and the specific amounts are determined according to the wage system applied at the workplace.

VDI: Year-end bonuses: when are they just motivation, and when are they the employer's responsibility

LINK

Article 142(1) of the Labor Code provides that bonuses may be awarded for two purposes: to reward the employee for work performed under an employment contract in the cases, amounts, and manner specified in the employment contract, the remuneration system, or other labour legislation, or at the employer's initiative to encourage the employee for good work, activities, or results achieved.

Even after the termination of the employment relationship, the employer may still be obliged to pay the bonus. Article 142(3) of the Labour Code provides that an employee must be paid a bonus proportional to the time actually worked during the period for which it is awarded, unless the parties have agreed otherwise.

Another type of bonus is an incentive bonus, which is awarded at the employer's initiative. It is paid at the employer's discretion to motivate the employee for good work, performance, or results achieved. However, the awarding of such a bonus is the employer's right, not an obligation.

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

Our recommendations and details are in this file

European Securities and Markets Authority

ESAs strengthen consumer defenses against AI-enabled online fraud and crypto scams

As digital finance expands, EU supervisors warn that fraudsters are exploiting AI and emerging technologies to deceive consumers. New ESA factsheets outline practical steps to recognise scams, avoid common traps, and respond effectively, reinforcing investor protection across the EU through clear, accessible guidance.

The European Supervisory Authorities (EBA, EIOPA and ESMA) have jointly released two consumer-focused factsheets addressing the rising sophistication of online frauds and scams, particularly those linked to crypto-assets and AI-enabled deception.

While fraud itself is not new, the ESAs highlight how tools such as AI-generated voices, videos, and deepfakes, combined with the perceived complexity of blockchain-based products, make scams more convincing and harder to detect. The publications explain typical scam techniques, including phishing, impersonation, investment fraud, and Ponzi schemes, supported by concrete examples.
They also outline warning signs and behavioural red flags, while promoting preventative actions such as verifying message sources, avoiding impulsive decisions, and never sharing sensitive personal or banking information.
To maximise reach and impact, the factsheets will be translated into all official EU languages and disseminated by national authorities, underscoring the ESAs' coordinated approach to consumer and investor protection.

LINK

Our recommendation

Firms in the financial and crypto-asset ecosystem should align client communications, compliance training, and control frameworks with the ESA guidance.
Integrating AI-related fraud risks into risk assessments, enhancing staff awareness of emerging scam typologies, and reinforcing clear consumer warnings can help meet regulatory expectations on investor protection.

Legal, audit, and compliance teams should also review disclosure practices and incident response processes to ensure they support timely detection, escalation, and reporting of suspected fraud, while demonstrating a proactive and well-governed approach to consumer protection.

REGULATORY COMPLIANCE UPDATE

CRYPTO

12.2025

ECOVIS ProventusLaw

European Securities and Markets Authority (ESMA)

LINK

On 8 December 2025, the European Securities and Markets Authority (ESMA) published a Questions and Answers document clarifying the interpretation of Article 78(5) of the MiCA Regulation concerning the execution of crypto-asset orders outside a trading platform. ESMA clarified that, for the purposes of Article 78(5) MiCA, the concept of a trading platform is limited to crypto-asset trading platforms authorised under Article 59 MiCA, as defined in Article 3(1)(18) MiCA. As a result, the execution of client orders through alternative arrangements, including over-the-counter trading, third-country trading venues, or decentralised exchanges, is considered to take place outside a MiCA-authorised trading platform.
Where a CASP's order execution policy allows for such execution, the provider must inform clients accordingly and obtain their prior express consent, which may be obtained either on a general basis or on a transaction-by-transaction basis. ESMA noted that this requirement reflects the differing regulatory standards and investor protection levels applicable outside MiCA-authorised trading platforms.

European Securities and Markets Authority (ESMA)

LINK

The European Securities and Markets Authority (ESMA) issued a statement on the expiry of transitional periods under the MiCA Regulation, addressing the supervisory treatment of CASPs that are not yet authorised. ESMA emphasised that MiCA transitional arrangements are coming to an end across Member States, with several jurisdictions having already concluded their national transition periods. CASPs operating without MiCA authorisation in those jurisdictions are therefore expected to cease regulated activities and implement orderly wind-down measures.
ESMA clarified that wind-down planning must prioritise client protection and the orderly return or transfer of crypto-assets, irrespective of whether an authorisation application is pending. The statement further notes that late or incomplete authorisation applications should be assessed with heightened supervisory caution and that national competent authorities should take enforcement action where unauthorised activity persists.
ESMA also underlined the importance of cross-border supervisory coordination and encouraged investors to verify the regulatory status of CASPs using ESMA's MiCA registers.

Bank of Lithuania

LINK

The Bank of Lithuania announced the issuance of two CASP licences under the MiCA Regulation to UAB Nuvei Liquidity and UAB Decentralized, marking further implementation of MiCA's licensing regime in Lithuania and the EU.
Nuvei Liquidity UAB was authorised to provide regulated crypto-asset services including custody, administration, transfer and exchange services, and additionally received a payment institution licence for operations with e-money tokens. Decentralized was granted authorisation to offer custody and administration of crypto-assets, transfer services, exchange of crypto-assets for funds and other crypto-assets under the MiCA framework.
These licences reflect Lithuania's continued leadership in the national implementation of MiCA's licensing regime, at a time when the transitional period for CASPs to obtain formal authorisation is approaching its expiry. The new licences demonstrate that only authorised entities may lawfully provide crypto-asset services in Lithuania and across the European Economic Area once MiCA's transitional arrangements conclude.

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:

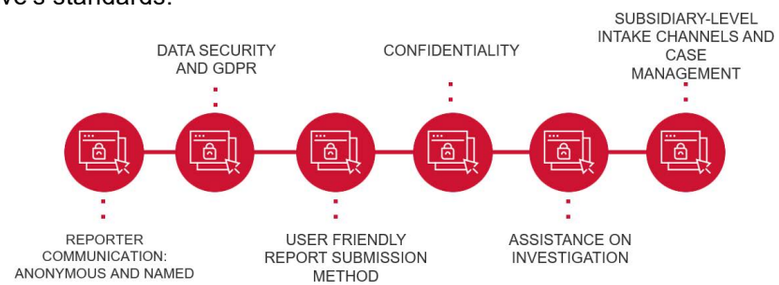
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors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