REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

02.2026

ECOVIS ProventusLaw

MONEYVAL Report. Latvia AML/CTF Mutual Evaluation (on-site visit November 2024)

LINK

MONEYVAL published its assessment of Latvia's AML/CTF framework.

Key findings: Latvia demonstrates strong overall performance, well-developed risk understanding and sustained political commitment.

Strengths:

1. solid international cooperation;
2. high-quality FIU analytical outputs;
3. effective risk-based banking supervision;
4. robust beneficial ownership transparency framework;
5. strong asset recovery practices including non-conviction-based confiscation.

Areas for improvement:

1. risk assessment methodology in the non-financial sector (State Revenue Service);
2. fully risk-based supervisory approach by the Latvian Council of Sworn Advocates;
3. prosecution of legal persons not yet commensurate with risk profile;
4. uneven TF awareness in certain non-financial sectors, particularly the legal profession.

Latvia placed under regular follow-up and must report to MONEYVAL by June 2028.

While the report assesses Latvia specifically, it is relevant for all obliged entities operating in Latvia or with Latvian counterparties.

Entities should review their AML/CTF frameworks given identified supervisory gaps.

Adequate TF awareness and training across their operations should be ensured.

MONEYVAL Report, Use of virtual assets for money laundering, terrorist financing and sanctions evasion

LINK

MONEYVAL published an updated horizontal review of virtual asset (VA) and virtual asset service provider (VASP) regulation across 25 jurisdictions.

Key findings: significant progress in regulatory/supervisory frameworks and international cooperation.
However, challenges remain:

1. enforcement against unlicensed VASPs is weak;
2. FATF Travel Rule (Recommendation 16) operationalised in only 46% of jurisdictions;
3. sanctions evasion via virtual assets is a growing concern.

Emerging risks identified: misuse of VAs for sanctions evasion, fraud, proliferation financing and child exploitation.

Further action needed on:

1. integrating sanctions/proliferation financing risks into national assessments;
2. improving suspicious activity reporting quality by VASPs;
3. enhancing investigatory capabilities;
4. cross-border cooperation and capacity building.

VASPs and financial institutions dealing with virtual assets should:

1. ensure full licensing/registration compliance;
2. implement the FATF Travel Rule if not yet operationalised;
3. integrate sanctions evasion and proliferation financing risks into their AML/CTF risk assessments;
4. review and improve the quality of suspicious activity reports.

Institutions should monitor further MONEYVAL guidance given the rapidly evolving VA sector.

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

02.2026

ECOVIS ProventusLaw

Decisions of the Bank of Lithuania Financial Market Supervision Committee

LINK

Four decisions adopted:

1. Tesonet Global UAB approved to indirectly acquire a qualifying holding (>10%, <20%) in e-money institution UAB "Elektroninių pinigų bitė", and approved to indirectly gain decisive influence over peer-to-peer lending platform and consumer credit provider UAB "Finansų bitė".

2. Settlement agreement with Emerchantpay Limited entered into force, the company had challenged the Bank of Lithuania's objection to its acquisition of UAB "PHOENIX PAYMENTS"; under the agreement Emerchantpay waives its claims and may submit a new notification which the Bank of Lithuania will assess based on new factual circumstances; confirmed by the Supreme Administrative Court of Lithuania.

3. Aki Sanne approved as board member candidate of ERGO Life Insurance SE.

4. UAB Inchcape Insurance Broker added to the insurance brokers list (now 106 firms).

Entities planning qualifying holding acquisitions or management appointments should ensure all required notifications and supporting documentation are submitted to the Bank of Lithuania in a timely manner. Firms whose acquisition applications were previously objected to should note that resubmission based on new factual circumstances remains a viable option.

Bank of Lithuania announcement of 2026 consultative events

LINK

The Bank of Lithuania announced 17 consultative events planned for 2026 covering:

1. DORA implementation;
2. AML/CTF;
3. payment services;
4. upcoming Consumer Credit Law amendments;
5. licensing;
6. third-party risk management;
7. resolution and other topics.

Events are held remotely.

Vilnius Regional Administrative Court

LINK

The Vilnius Regional Administrative Court annulled the part of the Bank of Lithuania's resolution revoking the payment institution licence of Majestic Financial UAB, holding the measure unlawful on grounds of disproportionality and insufficient reasoning.

The Bank of Lithuania had revoked the licence following AML/CFT supervisory findings. The court found that the authority failed to establish any real adverse consequences for clients or other financial institutions, did not identify aggravating circumstances, and did not adequately assess the institution's documented remediation efforts — which included updated AML/CFT procedures, exit from high-risk client relationships, additional staff training, and a retrospective transaction review. The court treated these steps as mitigating circumstances that the authority was required to weigh before selecting a sanction.

Drawing on CJEU and ECtHR case law, the court held that licence revocation is an extreme measure equivalent in severity to a criminal sanction and may only be applied where supervisory objectives cannot be achieved through less restrictive means — such as a warning, fine, or operational restriction. The Bank of Lithuania had not demonstrated why such alternatives would have been insufficient. The sanctioning part of the resolution was set aside and the matter remanded to the authority to impose a proportionate measure. The judgment is not yet final and may be appealed to the Supreme Administrative Court of Lithuania.

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

02.2026

ECOVIS ProventusLaw

The State Data Protection Inspectorate (VDAI) has fined Biržai Hospital 6,000 EUR following an investigation into video and audio surveillance at its premises

LINK

VDAI found that while video surveillance in common areas (e.g. entrances, corridors, lobby) was lawful to ensure safety, surveillance in operating theatres, emergency examination rooms and the geriatric day-care unit was unlawful, as it captured patient examination areas and staff workplaces. In these cases, patients' and employees' privacy rights outweighed the hospital's interests. The authority also determined that audio recording inside the hospital, including in operating theatres, violated the GDPR. Audio recording was not considered necessary for safety or work organisation, particularly given the risk of capturing sensitive health data. Additionally, the hospital set unclear and excessive retention periods for recordings, failed to ensure proper access controls, and did not fully cooperate with the authority during the investigation. VDAI ordered corrective measures and, in February 2026, imposed a 6,000 EUR administrative fine. The decision may be appealed within one month.

The State Data Protection Inspectorate of Lithuanias announced its supervisory priorities for 2026

LINK

The State Data Protection Inspectorate of Lithuania (VDAI), acting as the supervisory authority under the EU General Data Protection Regulation (GDPR), has announced its supervisory priorities for 2026.

Planned Inspections and Monitoring Activities

In 2026, the VDAI plans to conduct:

- 15 scheduled inspections in selected public and private sector organisations;
- 10 monitoring activities focusing specifically on technical and organisational security measures;
- Follow-up reviews of 15 organisations previously inspected where deficiencies were identified or corrective measures were ordered.

Lithuanian DPA Orders Company to Provide Call Recording in Direct Marketing Case

LINK

On 10 October 2024, the State Data Protection Inspectorate of Lithuania (VDAI) upheld a complaint against DirectMarketing OU for refusing to provide a data subject with a copy of a call recording in which the company claimed he had consented to direct marketing.

After receiving a marketing call, the complainant asked how his personal data had been obtained and requested confirmation of the data processed, details of the alleged survey, and copies of his consent. The company stated that he had participated in a survey on 9 April 2024 and agreed to receive marketing calls but refused to provide the call recording, arguing that recordings were internal documents and that the individual's identity could not be verified based on name and phone number alone.

State Data Protection Inspectorate: Fewer Personal Data Breaches Reported in 2025, but Over 1.2 Million Data Subjects Affected

LINK

In 2025, the State Data Protection Inspectorate (VDAI) received 223 notifications of personal data breaches (PDBs). The total number of affected data subjects in Lithuania reached 1,249,409. Compared to the previous year, the number of reported breaches decreased. In 2024, VDAI received 273 breach notifications. The number of affected data subjects in Lithuania also decreased by nearly 200,000 (1,467,368 in 2024).

Nature of Breaches

By type, confidentiality breaches statistically dominated in Lithuania of all cases in 2025. Integrity breaches made up 6%, availability breaches 10%, and in 1% of cases the incident was not considered a personal data breach (did not meet the legal definition).

EDPB Report on the Right to Erasure (Article 17 GDPR)

LINK

The European Data Protection Board (EDPB) has published the results of its Coordinated Enforcement Action (CEF) focusing on the right to erasure under Article 17 GDPR.

The EDPB selected this topic because the right to be forgotten is one of the most frequently exercised GDPR rights and one of the areas generating the highest number of complaints to supervisory authorities.

The main objectives of the initiative were:

- to ensure that individuals across Europe can effectively exercise their right to erasure;
- to assess how data controllers implement this right in practice;
- to identify common challenges and highlight good practices;
- to provide further guidance to organisations.

Detailed and full Regulatory Compliance Updates on Personal Data Protection and ICT Regulation can be found here:

Our recommendations and details are in this file

Council Decision (CFSP) 2026/432 amending Decision (CFSP) 2024/1484 - restrictive measures in view of the situation in Russia

The Council designates individuals responsible for the imprisonment and inhumane treatment of Russian political prisoners and activists who spoke out against Russia's war of aggression against Ukraine and criticised Putin's regime.

The new listings target members of the judiciary — two judges, one prosecutor, one investigator, and the heads of penal colonies and a pre-detention centre — who are involved in politically motivated trials. Overall, 8 individuals added to the EU Russia human rights sanctions list:

1. Aleksei Valizer - head of Penal Colony 10, Altai Krai
2. Anton Rychar - head of Pre-trial Detention Centre 1, Jewish Autonomous Oblast
3. Maksim Prilepsky - head of Penal Colony 5, Oryol Oblast
4. Vyacheslav Pisklov - head of Penal Colony 9, Altai Krai
5. Sergei Filichev - prosecutor, Lomonosovsky District Court, Saint-Petersburg
6. Eva Giunter - judge, Moskovsky District Court, Saint-Petersburg
7. Ilya Pleshkov - senior investigator, Moskovsky District, Saint-Petersburg
8. Andrey Shibakov - judge, Lomonosovsky District Court, Saint-Petersburg

All designated persons are subject to asset freeze, prohibition on making funds available, and travel ban.

LINK

Our recommendations:

1. EU companies and individuals must ensure no funds or economic resources are made available to the newly designated persons.
2. Compliance and sanctions screening teams should update internal watchlists accordingly.
3. Firms with exposure to Russian counterparties should conduct enhanced due diligence to identify any links to designated individuals.

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

02.2026

ECOVIS ProventusLaw

Recommendations of Ministry of Social Security and Labour of the Republic of Lithuania for the development and review of the work renumeration system

LINK

In order to help employers prepare for the upcoming changes, the State Labor Inspectorate (VDI), in cooperation with the Ministry of Social Security and Labor (SADM), has prepared recommendations for the development of remuneration systems, which help to assess the current situation in practice and plan the necessary actions.

All Remuneration system

- All employers, regardless of the number of employees, will be required to have a remuneration system in place.
- The remuneration system must be accessible to all employees.
- Before approving or changing the remuneration system, information and consultation procedures must be carried out in accordance with the procedure laid down in the Labor Code.
- In the remuneration system, the positions at the workplace or in the employer's company, institution, or organization must be divided into groups according to objective and gender-neutral criteria, the forms of remuneration for each group of positions or position must be established, wage levels or limits (minimum and maximum), additional remuneration (bonuses and allowances), the basis, amounts, and procedure for awarding bonuses, wage indexation, and criteria and procedures for wage increases. However, employers with fewer than 50 employees will be exempt from the obligation to include criteria and procedures for wage increases in the remuneration system.
- Positions classified as having the same or equal value work must be assigned to the same job group.

Decision of the Civil Division of the Supreme Court of Lithuania of February 19, 2026, in civil case No. e3K-3-10-684/2026

LINK

The Supreme Court of Lithuania ruled on the reduction of wages at the employer's initiative and the termination of the employment contract due to the employee's fault.
The dispute in the case arose after the employee submitted a request to the employer to terminate the employment contract in accordance with Article 56(1)(2) of the Labor Code, i.e., on the grounds that the employer had not paid the employee the full salary specified in the employment contract for more than two months.
The Supreme Court of Lithuania provided important clarifications regarding reduced wages for employees and when such situations are possible only at the employer's initiative.
If an employee is not active and does not defend their violated rights regarding changes to the terms of remuneration, according to the legal regulation established in Article 45(3) of the Labor Code, it is considered that the employee has agreed to work under the changed terms of remuneration.

Decision of the Supreme Court of Lithuania of February 5, 2026, in an administrative offense case No. 2AT-1-648/2026

LINK

The Supreme Court of Lithuania examined a case concerning illegal employment and the separation of employment legal relations from civil legal relations.
The court stated that illegal employment can only be established when: 1) the person has started working; 2) the relationship between the employer and the illegal employee has the characteristics of an employment contract; 3) the rules for concluding an employment contract have not been followed.
An employment contract has essential features that distinguish it from other contracts. First, an employee must have a certain work function rather than specific tasks.
Secondly, when performing their work functions, employees must comply with work procedures and obey the employer's instructions, whereas in civil contracts there is no subordination between the parties.

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

02.2026

ECOVIS ProventusLaw

ESMA Statement, reminder on obligations under CFD product intervention measures

LINK

ESMA reminded firms that perpetual futures/contracts offering leveraged exposure to crypto-assets (e.g. Bitcoin) likely fall within the scope of existing national CFD product intervention measures.

Where the CFD definition is met, firms must comply with:

1. leverage limits;
2. mandatory risk warnings;
3. margin close-out and negative balance protection;
4. prohibition of monetary and non-monetary benefits.

Additionally:

1. a narrow target market and aligned distribution strategy is required given product complexity;
2. appropriateness assessments must be carried out for non-advised services;
3. conflicts of interest must be identified, prevented or managed.

Companies offering perpetual futures or similar leveraged derivatives should:

1. assess whether the product falls within the CFD definition and applicable national intervention measures;
2. ensure full compliance with CFD requirements (leverage limits, risk warnings, margin close-out, negative balance protection, benefits prohibition);
3. define a narrow target market and review distribution strategy;
4. implement appropriateness assessments for non-advised clients;
5. review and update conflicts of interest policies.

TheEBA Opinion on the end of the No-Action Letter transition period, interplay between PSD2 and MiCA (EBA/Op/2025/08) Bank of Latvia

LINK

The EBA published an Opinion advising NCAs on how to proceed once the 9-month PSD2/MiCA transition period expires on 2 March 2026. Three scenarios apply:

1. CASP has obtained PSD2 authorisation or partnered with an authorised PSP, may continue EMT services;
2. CASP has submitted an application but not yet received authorisation, NCA may allow continued EMT services only if:
   2.1. application duly submitted with all required documents;
   2.2. applicant responds to NCA queries exhaustively and expeditiously;
   2.3. NCA has verified no material supervisory measures or MiCA/AML infringements;
   2.4. NCA has no reason to expect non-compliance and approval is expected within a very short timeframe. In this scenario the CASP must cease marketing EMT payment services and must not onboard new clients.
3. CASP has not submitted an application or fails to meet scenario 2 conditions, NCA must require the CASP to cease EMT payment services and offboard relevant clients as of 2 March 2026.

Our recommendation:

CASPs transacting EMTs that qualify as payment services should urgently verify which scenario applies to them.
CASPs in scenario 2 must ensure full cooperation with their NCA and immediately cease marketing and new client onboarding for EMT payment services.
CASPs that have not submitted a PSD2 application must discontinue EMT payment services as of 2 March 2026.

Detailed and full Regulatory Compliance Update on Employment 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:

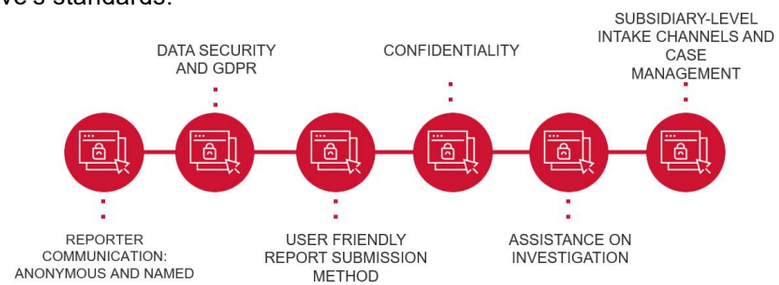
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors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