REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

01.2026

ECOVIS ProventusLaw

Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)

LINK

AMLA to launch data collection exercise to test risk assessment models for the financial sector

AMLA will launch a data collection exercise starting in March 2026 to test and calibrate its risk assessment models for the financial sector. These models serve two purposes: to inform the selection of up to 40 entities for AMLA's direct supervision starting in 2028 (selection taking place in 2027), and to ensure money laundering risks of financial institutions are assessed consistently by supervisors across the EU.

The exercise is being conducted in close cooperation with national supervisors and the private sector. It represents a preparatory step towards AMLA's direct supervision and will involve two groups of financial institutions: those that may be eligible for AMLA's direct supervision, and a representative sample of entities likely to remain under national supervision. National supervisors have provided AMLA with lists of both groups, and AMLA has notified those selected to participate.

The exercise will allow participating financial institutions to test and prepare their systems for future data collections, while AMLA will use the insights gained to optimize the data collection planned for the selection process. Once models are fully tested and calibrated, AMLA will establish the final list of entities eligible for direct supervision. National supervisors will collect data points from eligible entities in early 2027, which will inform AMLA's subsequent selection of the 40 directly supervised entities.

Joint announcement by the European Banking Authority (EBA) and the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA); ESAs-AMLA Memorandum of Understanding

LINK

EBA and AMLA complete handover of AML/CFT mandates

The European Banking Authority and the Authority for Anti-Money Laundering and Countering the Financing of Terrorism completed the full transfer of all AML/CFT mandates and functions from the EBA to AMLA on 1 January 2026. This marks a significant milestone in the EU's fight against financial crime and concludes the EBA's stand-alone AML/CFT mandate that began in 2020.

Key EBA tools and expertise, including the EuReCa database, supervisory insights, and risk assessments, have been transferred to AMLA. All existing EBA AML/CFT guidelines and standards remain in force until replaced by AMLA, ensuring regulatory continuity for the industry and supervisors.

Under the new framework, AMLA will complete the EU's Single Rulebook, advance supervisory convergence, and coordinate the work of Financial Intelligence Units (FIUs) to enhance cross-border exchange of financial intelligence. AMLA will directly supervise 40 of the most complex financial institutions or groups in the EU. The EBA will continue to address money laundering risks through prudential regulation, working in coordination with AMLA to maintain a coherent framework.

A formal ESAs-AMLA Memorandum of Understanding has been established to enable regular information exchange, joint initiatives, and consistent engagement with the private sector.

Inspection plan by the BoL

LINK

The Bank of Lithuania announced its 2026 inspection plan

Plan includes around ~20 inspections focusing primarily on AML/CTF compliance:

- 2 banks;
- 1 central credit union;
- 1 e-money institution;
- 1 payment institution
- 1 crowdfunding provider.

Additionally, 15 unplanned inspections will target AML/CTF compliance, fraud prevention, and payment services provision. The regulator published standardized inspection templates to help institutions prepare and reduce administrative burden.

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

01.2026

ECOVIS ProventusLaw

Bank of Lithuania

LINK

The Bank of Lithuania held 14 consultative events in 2025 for financial market participants, attracting over 3,000 attendees (average 223 per event). The most popular topics were Digital Operational Resilience Act (DORA) requirements (nearly 1,000 participants, one-third of all attendees) and Risk Management Process Guidelines for E-Money and Payment Institutions.
Almost 80% of respondents indicated the content met their expectations. The Bank of Lithuania publishes its annual consultative events plan by February each year on its website, based on regulatory developments and industry feedback.

The plan is announced here: https://www.lb.lt/lt/konsultaciniu-renginiu-planas

- Monitor the Bank of Lithuania's website for the 2026 consultative events plan (published by February).
- Use these consultative sessions to clarify regulatory expectations and align internal compliance practices with supervisory guidance

Latvia strengthens its position as an innovation-friendly financial hub

LINK

New Special Credit Institution Licence:
Amendments to the Credit Institution Law came into effect in January 2026, allowing institutions to be licensed as special credit institutions with a minimum initial capital requirement of EUR 1 million. This new licensing category aims to enhance competitiveness in the credit institution sector and support the development of financial market participants.

Strategic Positioning for Fintech:
Latvia has attracted increased attention from Europe's fintech community, particularly among organisations launching innovative financial services. Key advantages include early regulatory consultations that reduce uncertainty, structured and transparent licensing pathways, direct participation in central-bank settlement infrastructure, balanced cost structure with EU regulatory alignment, and crypto-asset service authorisation under MiCA.

Supervision Priorities (2026-2028):
Latvijas Banka has announced its financial market supervision priorities for the next three years, focusing on enhancing the financial and operational resilience of financial market participants, as well as improving the accessibility and transparency of financial services.

Bank of Lithuania

LINK

The Bank of Lithuania (Lietuvos Bankas) approved the acquisition of UAB BLUE EMI LT by UK-based Checkout Payments Group Limited (Checkout.com), one of the world's largest payment solutions providers.

This marks another major international FinTech entering Lithuania's market. The Bank highlighted Lithuania's favorable regulatory environment, including the "Newcomer" program (consultations for potential market entrants), CENTROlink payment system access, and reduced capital requirements (from €1M for specialized banks since 2017).

Over the past 5 years, the Bank granted 100+ licenses and 150+ permits to new financial market participants. Five global institutions entered Lithuania in the past 2 years (Robinhood, Nuvei, DriveWealth, Commerzbank, PKO Bank Polski).

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

01.2026

ECOVIS ProventusLaw

VDAI Decision on Direct Marketing Compliance

LINK

The State Data Protection Inspectorate of Lithuania (VDAI) recently examined a complaint regarding unsolicited direct marketing emails sent by UAB "Topo grupė". The decision highlights once again what requirements apply to email marketing, when exceptions may be used, and why silence is not consent under GDPR and Lithuanian law. Under Article 81(1) of the Law on Electronic Communications, email may be used for direct marketing purposes only with the recipient's prior consent. According to the GDPR, consent must be:

- freely given,
- specific,
- informed,
- unambiguous,
- expressed by a clear affirmative action.

Important: silence, inactivity, or failure to tick an opt-out box does not constitute valid consent.

Marketing without consent:

The law allows one narrow exception (Article 81(2) of the Republic of Lithuania Law on Electronic Communications), where marketing emails may be sent without separate consent only if all of the following conditions are met:

1. the email address was obtained directly from the customer;
2. it was collected in the context of a sale of goods or services;
3. the marketing relates only to the company's own similar products or services;
4. the customer was clearly informed and given a free and easy opt-out option:
   - at the time of data collection, and
   - in every message sent;
5. the customer did not object initially.

EU Court Clarifies Pseudonymized Data as Personal Data

LINK

A long-running case between the EU Single Resolution Board (SRB) and the European Data Protection Supervisor (EDPS) concerning when pseudonymized data counts as personal data has concluded without a final General Court ruling. The dispute arose from SRB's 2017 sharing of pseudonymized stakeholder comments with Deloitte during the resolution of a Spanish bank, which the EDPS had deemed personal data under the GDPR.

The Court of Justice of the EU (CJEU) previously clarified that:

- Individuals' personal opinions can be personal data.
- The risk of reidentification must be assessed case by case.
- Pseudonymized data is not automatically personal data if it effectively prevents identification by others.

EDPB contributes to the LED evaluation and adopts recommendations on the application for Processor BCR

LINK

The European Data Protection Board (EDPB) has adopted a report to support the European Commission's evaluation of the Law Enforcement Directive (LED), which must be submitted to the European Parliament and the Council by 6 May 2026. The report highlights the key role of the LED in protecting personal data in the law enforcement context and points to growing challenges linked to the use of new technologies, including artificial intelligence. The EDPB calls for clearer boundaries between the LED and the GDPR, stronger national implementation across the EU, improved cooperation between competent authorities, and a reinforced role for Data Protection Officers (DPOs).

EU Court of Justice to Examine GDPR Compliance of FATCA-Related Bank Data Transfers

LINK

The EU Court of Justice (CJEU) is set to clarify whether transferring EU residents' banking data to the United States under the Foreign Account Tax Compliance Act (FATCA) complies with the EU's General Data Protection Regulation (GDPR).

The case stems from a complaint by an individual with dual Belgian and US citizenship, alongside the Association of Accidental Americans, challenging the legality of FATCA-mandated transfers. FATCA requires non-US financial institutions to report US persons' account information to the IRS, and non-compliance can trigger a 30% withholding tax on US investment income.

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

REGULATORY COMPLIANCE UPDATE

FINANCIAL AND ECONOMIC SANCTIONS 01.2026

ECOVIS ProventusLaw

The Council of the European Union

Council of the EU imposes sanctions on six individuals for Russian hybrid threats and information manipulation activities

The Council of the EU adopted restrictive measures against six additional individuals in response to Russia's continued hybrid activities, particularly Foreign Information Manipulation and Interference (FIMI) against the EU, its member states, and partners.

The newly sanctioned individuals include:

- television presenters **Dmitry Guberniev, Ekaterina Andreeva, Maria Sittel;**
- propagandist **Pavel Zarubin**;
- actor **Roman Chumakov;**
- and ballet dancer **Sergey Polunin.**

All have been working for or supporting Russian propaganda channels, spreading disinformation about the war in Ukraine, and actively contributing to Russia's war effort, including raising funds for Russian armed forces.

Restrictive measures now apply to 65 individuals and 17 entities. Listed persons are subject to asset freezes, travel bans, and EU citizens and companies are forbidden from making funds or economic resources available to them.

LINK

Our recommendations:

- Immediately screen customer databases and transaction monitoring systems against the updated EU sanctions list to identify any matches with the six newly designated individuals or related entities.
- Freeze all assets and block transactions involving sanctioned persons.
- Update sanctions screening procedures and ensure compliance teams are aware of the expanded scope covering information manipulation and hybrid threat activities.
- Implement enhanced due diligence for customers with potential links to Russian propaganda channels or media outlets.
- Report identified assets or attempted transactions involving sanctioned individuals to national competent authorities.

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

01.2026

ECOVIS ProventusLaw

Lithuania Registers Extensive Labour Code Amendments Strengthening Pay Transparency and Equal Pay Obligations

LINK

On 20 January 2026, amendments to the Labour Code were registered introducing broad pay transparency and equal pay obligations. Employers will no longer be allowed to request salary history from job applicants and must disclose relevant collective agreement provisions during recruitment. All employers, regardless of size, will be required to implement an accessible remuneration system based on objective, gender-neutral job grouping and defined wage structures, including pay ranges and bonus criteria (with limited exemptions for employers with fewer than 50 employees).

Employees will have the right to obtain written information about their own pay and average pay levels by gender within their job group. Employers must inform employees annually of this right. Disclosure of salary data for the purpose of enforcing equal pay cannot be treated as confidential. Employers will also be required to report gender pay gap data, with monthly wage information submitted to the State Social Insurance Fund Board for publication of aggregated statistics.

Our recommendations:

- Review the recruitment process to ensure transparency requirements are met;
- Conduct an assessment of the gender pay gap;
- Review the remuneration system or prepare it, if the employer does not yet have one, taking into account the anticipated new requirements.
- Prepare clear information for employees on wage setting and remuneration procedures.
- Review confidentiality procedures and agreements to ensure that they are consistent with transparency obligations.

Key Employment Law Developments in 2025 – Lithuanian Supreme Court

LINK

Indirect discrimination and disability (C-38/24, Bervidi, 11 September 2025) The CJEU confirmed that protection against indirect discrimination on grounds of disability extends to employees who suffer adverse treatment because they care for a disabled child. Employers must provide appropriate conditions enabling such employees to provide necessary care, unless this would impose a disproportionate burden.

Pre-contractual testing of candidates (LAT, 16 June 2025, No. 3K-3-108-1120/2025) The Supreme Court of Lithuania held that employers may assess a candidate's actual qualifications and abilities before concluding an employment contract. If the candidate's declared qualifications do not match their real capabilities, the employer may lawfully terminate the pre-contractual relationship and refuse to conclude contract.

Conflicts of interest and gross misconduct (LAT, 10 April 2025, No. e3K-3-49-1120/2025) The Court clarified that employers may define conflicts of interest in employment contracts and internal rules. A conflict includes not only actual harm to the employer's interests but also a potential threat of harm. Employees may be held liable for failing to avoid even the risk of a conflict of interest.

Double pay for work on rest days and litigation cost (LAT, 25 September 2025, No. e3K-3-128-1120/2025) Double pay applies where work on a rest day is performed at the employer's request. If the schedule change is initiated solely by the employee, double pay is not due. The employer bears the burden of proof. The Court also confirmed that courts may depart from the "loser pays" principle where strict application would deprive a party of meaningful compensation.

Illegal employment of foreigners and fault (LAT, 13 October 2025, No. 2AT-30-891/2025) Administrative liability for illegal employment requires fault. Where a residence permit expiry was overlooked due to a clerical software error and the employer had generally ensured proper compliance systems, the company director was not found negligent.

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

01.2026

ECOVIS ProventusLaw

European Securities and Markets Authority

LINK

Five crypto-asset service providers receive MiCA authorisation across Europe

European regulators authorised five crypto-asset service providers under the MiCA framework in January 2026:

Germany

ISF Institut Deutsch-Schweizer Finanzdienstleistungen GmbH (authorised 28 January 2026)

- Regulator: Federal Financial Supervisory Authority (BaFin)
- Authorised services: reception and transmission of orders for crypto-assets on behalf of clients

Ireland

Interactive Brokers Ireland Limited (authorised 22 January 2026)

- Regulator: Central Bank of Ireland (CBI)
- Authorised services: reception and transmission of orders for crypto-assets on behalf of clients

Malta

Damex Digital LTD (authorised 29 January 2026, registered 30 January 2026)

- Regulator: Malta Financial Services Authority (MFSA)
- Authorised services: providing custody and administration of crypto-assets on behalf of clients; exchange of crypto-assets for funds; exchange of crypto-assets for other crypto-assets; execution of orders for crypto-assets on behalf of clients; providing transfer services for crypto-assets on behalf of clients

Slovakia

Firefish Europe s.r.o. (authorised 2 January 2026, registered 5 January 2026)

- Regulator: National Bank of Slovakia (NBS)
- Authorised services: providing custody and administration of crypto-assets on behalf of clients; exchange of crypto-assets for funds; exchange of crypto-assets for other crypto-assets; providing transfer services for crypto-assets on behalf of clients

Okazio s.r.o. (authorised 15 January 2026, registered 16 January 2026)

- Regulator: National Bank of Slovakia (NBS)
- Authorised services: providing custody and administration of crypto-assets on behalf of clients; execution of orders for crypto-assets on behalf of clients; providing advice on crypto-assets; providing portfolio management on crypto-assets; providing transfer services for crypto-assets on behalf of clients.

The Bank of Latvia

LINK

Latvia issues two MiCA licences and promotes crypto-asset supervision framework

Latvia issued two MiCA (Markets in Crypto-Assets Regulation) licences in 2025, demonstrating progress in establishing a clear and predictable regulatory framework for crypto-asset service providers.

Latvijas Banka will participate in the event "Crypto Crisis Averted: Explore Alternatives" in Warsaw on February 12, 2026, where Marine Krasovska, Head of the Financial Technology Supervision Department, will speak on the panel "EU Crypto Compliance in Practice" and share insights on crypto-asset supervision and MiCA implementation.

Latvia has positioned itself as an attractive jurisdiction for crypto-asset service providers within the EU, offering early regulatory consultations that reduce uncertainty, structured and transparent licensing pathways, and alignment with EU regulatory frameworks including MiCA.

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:

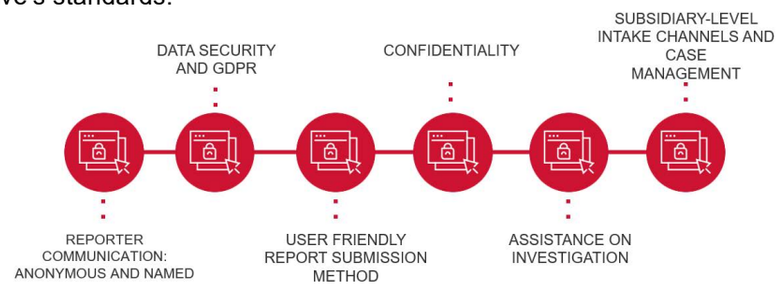
Readiness Assessments – Understand your current compliance gaps. DORA Gap analysis with our compreheni
Implementation of Internal ICT Audits – In line with Article 6 requirements
Incident Response & Reporting Frameworks – Clear, regulator-ready processes
Third-Party Risk Management – Ensure your vendors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