REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

04.2026

ECOVIS ProventusLaw

Lietuvos Bankas (Bank of Lithuania) – Notice inviting participation in AMLA consultations

LINK

The Bank of Lithuania, alongside AMLA, is inviting Lithuanian financial market participants to engage with two ongoing AMLA public consultations on draft AML/CFT instruments (see Entry 2 below for details).

The notice specifically targets banks, credit unions, payment institutions, electronic money institutions, and other obliged entities supervised by Lietuvos Bankas, encouraging them to submit written comments and participate in the public hearings organised by AMLA.

Lithuanian-supervised institutions should treat this as a direct call to action from their national regulator to engage with the AMLA consultation process.
Participation demonstrates regulatory engagement and may help shape rules that will directly affect day-to-day AML/CFT compliance.

AMLA – Draft RTS under AMLR Articles 16(4) & 17(3) (group-wide requirements) and Draft Guidelines under AMLR Article 10(4) (business-wide risk assessment)

LINK

AMLA launched two public consultations on draft instruments defining how obliged entities must identify, assess, and manage AML/TF risks:

1. Draft Guidelines on Business-Wide Risk Assessment (AMLR Art. 10(4)) - minimum expectations for all obliged
entities on conducting a business-wide risk assessment, with proportionality based on si e, business model, and risk profile. Consultation open until 15 July 2026 public hearing on 28 May 2026.

2. Draft RTS on Group-wide Requirements (AMLR Arts. 16(4) 17(3)) - minimum standards for group-wide AML/CFT frameworks, including cross-border situations and third-country operations, requiring groups to maintain a consolidated view of AML/TF risk across the entire organisation. Consultation open until 15 June 2026 public hearing on 20 May 2026.

Additionally, AMLA published an updated data model and taxonomy for its 2027 direct supervision selection exercise, with comments accepted until 10 May 2026.

Obliged entities - especially those operating across multiple jurisdictions or with third-country subsidiaries - should review both instruments carefully and consider submitting responses or attending the public hearings.

Contact the Ecovis team for assistance in assessing the impact on existing AML/CFT frameworks and preparing consultation submissions.

Detailed and full Regulatory Compliance Update on AML/CTF Regulation can be found here: *Our recommendations and details are in this file*

REGULATORY COMPLIANCE UPDATE

EMI, PI REGULATION

04.2026

ECOVIS ProventusLaw

Latvijas Banka - Licensing Framework

LINK LINK

Amendments to the Credit Institution Law (in force 6 January 2026) introduced the specialised credit institution licence with a reduced initial capital of €1M (vs €5M for regular banks). On 9 April, at the Fintech Breakfast "A New Banking Licence for Fintechs in Latvia, Vol. 2," Agnese Alaine, Head of the Licensing and Sanctions Department, introduced the regulatory framework and licensing process for a special credit institution. Eligible models:
(a) cooperative/territorial banks with limited customer base;
(b) fully digital banks/neobanks;
(c) innovative financial services providers.

Key licensing requirements:

- capital adequacy calculation must cover risk-weighted assets for 3 years AND cumulated expected losses for 3 years (the higher of the two applies)
- exit strategy mandatory as part of licensing documentation
- 4-step process (introductory meeting -> pre-licensing ->ECB joint review -> official application)
- up to 3 months possible 1-year extension.

Common pitfalls flagged by Latvijas Banka: unrealistic financial projections, insufficient AML risk assessment, inadequate IT cost forecasting, incomplete management F&P information, and underestimation of ECB involvement timelines. Supervisory message: "Everything can be improved except lack of capital and reputation."

EU Advocate General Opinion in Case C-274/25, Alternative Payments UAB v Lietuvos Bankas

LINK

The Advocate General concluded that a PSP transmitting SEPA direct debit instructions, collecting funds and managing restricted IBAN accounts for merchants may itself be considered to provide a regulated direct debit service under PSD2, even if another PSP performs the actual debit from the payer s account. The opinion also clarified that such activity does not qualify merely as payment acquiring or payment initiation services. Although the opinion is not binding and the final judgment of the CJEU is still pending, payment institutions and fintechs offering merchant collection or recurring payment solutions within the SEPA framework should assess whether their activities could be regarded as regulated direct debit services and whether their current authorisations adequately cover such operations.

Latvijas Banka - Fintech Latvia Newsletter / Licensing

Three new licensed entities entered the Latvian financial market in April:

- NorthernTech SIA received an EMI licence authorising payment transaction execution and payment instrument issuance
- SIA pinyya invest received a licence for investment and ancillary investment services
- SIA Catego received a payment institution licence for account information services.

New licensed players signal continued market growth.

Firms considering entry into the Latvian market or seeking partners in the payment/EMI space should note the expanded competitive landscape.
If you are considering obtaining a licence in Latvia, Contact ECOVIS Team - we advise and provide assistance throughout the entire licensing process.

CJEU Judgment in Case C-744/24, P.W. v Bank Polska Kasa Opieki S.A.

LINK

The CJEU ruled that, under Directive 2008/48/EC, lenders may not apply interest to amounts representing credit-related costs (including insurance premiums and other non-interest credit costs) that form part of the total cost of credit to the consumer. The Court clarified that only the actual amount made available to the borrower may constitute the basis for the borrowing rate. Credit institutions and consumer lenders should review their consumer credit structures, APR calculations and contractual documentation to ensure that interest is not charged on financed credit costs, insurance premiums or similar ancillary charges, as such practices may be incompatible with EU consumer credit rules.

Detailed and full Regulatory Compliance Updates on Payments Systems Regulation can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

PERSONAL DATA PROTECTION AND ICT REGULATION

ECOVIS ProventusLaw

04.2026

Changes to Direct Marketing Rules in Lithuania from July 2026

LINK

On 16 April 2026, Seimas adopted amendments to the Law on Electronic Communications, specifically revising Article 81, which governs the use of electronic communications for marketing purposes. These changes will apply from 1 July 2026. It is important to note that these amendments apply only to direct marketing carried out via electronic communications (e.g. email, SMS) and do not cover other forms of marketing.

B2B Direct Marketing: What's New?

Under the new rules, direct marketing to legal entities may be carried out without prior consent, based on an opt-out model.

Contacts of Natural Persons: Consent Still Required

For natural persons, the rules remain unchanged - prior consent is still required for direct marketing. Consent must be freely given, specific, informed, unambiguous.

Exception: "Soft Opt-In" for Existing Customers

Although prior consent is generally required for marketing to natural persons, the law provides an exception - the so-called "soft opt-in" for existing customers.

EDPB DPIA Template

LINK

The European Data Protection Board (EDPB) has introduced a *new template* to assist organi ations in conducting Data Protection Impact Assessments (DPIAs). This template aims to simplify DPR compliance and promote consistency across Europe by providing a structured format for reporting DPIA processes. It is designed to help organi ations clearly document how they assess and manage risks related to the processing of personal data.The template is currently open for public consultation until June, allowing stakeholders to provide feedback. After this period, Data Protection Authorities across Europe will consider adopting the template either as a common standard or as a framework aligned with national requirements.

Vinted Reprimanded for Failing to Properly Handle Data Access Requests

LINK

The State Data Protection Inspectorate (Lithuania) has issued a decision following a complaint transferred by the erman supervisory authority regarding the handling of data subject access requests by Vinted, UAB. The complainant s account had been blocked due to alleged unfair activity, reportedly based on automated decision-making. The individual subsequently exercised their right of access under Article 15 of the GDPR, requesting information about the logic behind the decision and the recipients of their personal data.

However, the company failed to properly respond to this request. Instead of providing the required information, the complainant was redirected to the privacy policy. The authority found that the request may not have been correctly identified as a GDPR access request, highlighting weaknesses in internal processes.

Lithuanian Data Protection Authority Imposes Fine for Personal Data Breach

LINK

VDAI has imposed a fine of EUR 4,500 on UAB DELS A Lithuania, as the legal successor of UAB "Rakrėjus", for violations related to personal data security. The investigation was initiated in arch 2025 following notifications of personal data breaches linked to a cybersecurity incident that occurred on the public cloud services platform used by UAB "Rakėjus". Upon completing the investigation, the VDAI found that the breach affected the personal data of a large number of data subjects - nearly 3,000 individuals. Some of the data could not be restored, and service provision, including financial services, was temporarily disrupted. The authority classified the breach as of medium severity. The VDAI concluded that the company had failed to implement appropriate technical and organisational measures to ensure the security of personal data, thereby infringing Article 32(1)(b) of the General Data Protection Regulation (GDPR).

EDPB Annual Report 2025

LINK

The European Data Protection Board (EDPB) has released its *Annual Report* for 2025, outlining significant developments in data protection across the European Union. The report highlights the continued enforcement of the eneral Data Protection Regulation (GDPR) and the increasing number of cross-border cases handled by the EDPB. This reflects the growing importance of data privacy and the commitment of EU authorities to uphold citizens rights in an evolving digital landscape.

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

Our recommendations and details

REGULATORY COMPLIANCE UPDATE

FINANCIAL AND ECONOMIC SANCTIONS 04.2026

Council Decision (CFSP) 2026/884 & Council Implementing Regulation (EU) 2026/885 - EU Restrictive Measures for Russia's Destabilising Activities (hybrid threats listing)

LINK

The Council of the EU added two entities to its sanctions list under the Russia hybrid threats regime.
The first is Euromore, a pro-Kremlin media platform that amplifies and legitimises Russian disinformation targeting European audiences, including content justifying Russia's war against Ukraine and undermining EU institutions.
The second is Pravfond (Foundation for the Support and Protection of the Rights of Compatriots Living Abroad), a Russian state-founded and financed body whose legal and analytical output systematically reinforces Kremlin disinformation narratives, including allegations of Ukraine's "nazification" and "Russophobia."
Both entities are subject to an asset freeze; EU persons and companies are prohibited from making funds or economic resources available to them. The total number of designated individuals and entities under this regime now stands at 69 individuals and 19 entities.
EU-based firms and financial institutions should screen their counterparties and transaction flows against the updated sanctions list.

Contact the Ecovis team for support on sanctions compliance screening and risk exposure assessment.

Council Regulation (EU) 2026/506, Council Decision (CFSP) 2026/508 & related acts - 20th Package of EU Restrictive Measures against Russia

LINK

On 23 April 2026, the EU adopted its 20th sanctions package against Russia - the most expansive to date - targeting Russian energy actors, the "shadow fleet," a major maritime insurer, and a Chinese semiconductor manufacturer, alongside mirrored measures under the Belarus regime. The package combines the largest asset free e listing in two years (37 individuals, 80 entities) with wide-ranging sectoral measures across financial services, crypto-assets, energy and maritime, trade and anti-circumvention, and cybersecurity, with effective dates staggered through May 2026 and into January 2027.

This package has direct and immediate implications for any EU firm providing crypto asset services, financial messaging, or trade finance with Russian or Belarusian exposure. Firms should urgently audit their crypto asset platforms and service relationships for compliance with the new sectoral ban and transaction prohibitions.

Contact the Ecovis team for a comprehensive legal review of exposure under the 20th sanctions package, particularly regarding crypto asset services, stablecoin trading, and digital ruble-related activities.

Detailed and full Regulatory Compliance Updates on Financial and Economic Sanctions can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

04.2026

ECOVIS ProventusLaw

Proposed Amendments to the Labour Code: More Flexibility, Clearer Rules and Stronger Collective Relations

LINK

A package of amendments to the Lithuanian Labour Code, currently under consideration in the Seimas and expected to enter into force on 1 November 2026, introduces significant changes to both individual and collective employment relations. The reforms aim to increase labour market flexibility, clarify employment regulation, and strengthen social dialogue.

It includes: greater flexibility for high-earning employees, longer probation period, new grounds for termination, updated settlement rules upon termination, higher penalties for late payments, changes to annual leave rules, more clarity on remote work, and introduction of a clear "termination and employer's discretion" ground.

Implementation of the EU Pay Transparency Directive in Lithuania: plans and how to prepare

LINK

Lithuania is taking concrete steps to implement the EU Pay Transparency Directive, which aims to strengthen the principle of equal pay and increase transparency in the labour market. The upcoming legislative amendments will introduce new obligations for employers and expand employees rights to information and legal protection.

Objectives of the Directive

The main objectives of the Directive are to:

- Ensure equal pay for women and men for the same or work of equal value
- Increase transparency in pay setting and pay levels
- Provide effective remedies for employees who experience pay discrimination

The Pay Transparency Directive is expected to be transposed into Lithuanian national law by 7 June 2026.

Decision of the Supreme Court of Lithuania of April 16, 2026, in Civil Case No. e3K-3-66-1249/2026

LINK

The Supreme Court of Lithuania ruled on the legal provisions governing the classification of an agreement between an employer and an employee regarding compensation for damages to the employer. The court clarified that, for an agreement between the parties to be considered a novation (substitution of an obligation), it is necessary to establish both the original and the new obligation of the parties by which it was replaced, as well as the parties intent regarding the replacement.

Agreements regarding obligations arising from employment legal relationships must be assessed in accordance with the mandatory provisions of labor law.

Court of Justice of the European Union judgement of 16 April 2026, Colombani v EEAS, C-343/23 P

LINK

The Court of Justice of the European Union provided important clarifications on what constitutes psychological harassment.

Psychological harassment is defined as improper conduct , which, first, takes the form of physical behaviour, spoken or written language, gestures or other acts, which takes place over a period and is repetitive or systematic , suggesting that psychological harassment must be understood as a process that occurs over time and presupposes the existence of repetitive or continual behaviour which is intentional , as opposed to accidental . Second, to fall within that concept, such physical behaviour, spoken or written language, gestures or other acts must have the effect of undermining the personality, dignity or physical or psychological integrity of a person.

Psychological harassment may be committed collectively by several people where their actions amount to one and the same conduct of harassment and each of them contributes to it by his individual and personal conduct.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

CONSUMER PROTECTION

04.2026

Latvijas Banka (Bank of Latvia) – Press Release / EU Technical Support Instrument Project (in cooperation with Lietuvos Bankas, OECD, and European Commission)

Latvijas Banka, together with the Central Bank of Lithuania, the OECD, and the European Commission, is developing an action plan to strengthen digital financial literacy and fraud resilience among the populations of Latvia and Lithuania, funded through the EU's Technical Support Instrument.

Research conducted under the project reveals the scale of the problem: 27% of Latvian adults have been victims of financial fraud in the past two years, with purchase fraud (15%), phishing (8%), investment fraud (6.5%), and unauthorised transactions (5.6%) being the most prevalent types. In Lithuania the figure is even higher at 44%. Underreporting remains a significant concern, with 37% of victims failing to report incidents.

A stakeholder workshop was held on 24 April 2026, bringing together the OECD, State Police, Finance Latvia Association, and representatives of at-risk population groups to contribute to the action plan.

Despite the challenges, digital financial literacy in Latvia has improved, reaching an average score of 58/100 -up 10 points since 2023.

The project is set to conclude in November 2026 with publication of research results and the finalised action plan.

LINK

Our recommendation

Financial service providers operating in Latvia and Lithuania should monitor the forthcoming action plan, expected in November 2026, as it may inform or precede regulatory measures targeting consumer protection, fraud prevention obligations, and digital literacy requirements. Firms should review their current fraud reporting and customer education frameworks to ensure alignment with emerging regulatory expectations.

Contact the Ecovis team for guidance on compliance positioning ahead of potential follow-on regulatory action in the Baltics.

REGULATORY COMPLIANCE UPDATE

INVESTMENT AND CRYPTO

04.2026

ECOVIS ProventusLaw

FCA Policy Statement PS26/7 - Progressing Fund Tokenisation (Policy Statement + Guidance, Financial Conduct Authority)

LINK

The FCA published PS26/7 and accompanying guidance clarifying how asset managers can use distributed ledger technology (DLT) for fund tokenisation within existing regulatory rules - no new legislation required. The guidance covers both private and public blockchain models, permitting public chain use where sufficient controls are in place. A new optional Direct to Fund (D2F) model is also introduced, enabling investors to deal directly with a fund (traditional or tokenised), removing intermediary layers and improving dealing efficiency. The FCA positions tokenisation as a means to lower costs and broaden investor access, and the policy statement includes a forward-looking roadmap for how fund tokenisation will develop as part of its wider digital assets strategy.
Asset managers, fund administrators, and firms with UK operations or UK-facing fund structures should review PS26/7 to assess how current or planned tokenisation activities fit within the new framework - particularly regarding public blockchain use conditions and the D2F model.

European Securities and Markets Authority (ESMA) - Statement on the End of Transitional Periods under MiCA (ESMA75-113276571-1679)

LINK

ESMA confirmed that the MICA transitional period expires across the EU on 1 July 2026, after which unlicensed crypto-asset service providers (CASPs) must cease offering services to EU clients.

Key expectations:

- unauthorised CASPs must have operational wind-down plans ready for immediate execution, including orderly client offboarding to authorised CASPs or self-hosted wallets
- authorised CASPs must complete client migration and ensure outsourcing/custody delegation arrangements involve only MiCA-authorised entities
- third-country providers remain prohibited from soliciting or serving EU clients outside the reverse solicitation exception, including in B2B contexts.

NCAs are expected to enforce these requirements actively. ESMA also issued a consumer warning advising investors to verify provider authorisation via the ESMA Interim MiCA Register.

ESMA MiCA Register

LINK

Four crypto-asset service providers received MiCA authorisation or last-update confirmation during April 2026 across five EU home member states:

- Northstake ApS (Denmark) - authorised for custody administration, order execution, and transfer services passporting across the full EEA (30 states).
- Electrocoin Ltd (Croatia) - authorised for custody administration, exchange for funds, and exchange for other crypto-assets full EEA passporting.
- Validvent Technology GmbH (Germany) - authorised for crypto-asset advice passporting to 16 selected EU member states including AT, BE, CY, FR, IE, IT, NL, ES and others.
- ClearBank Europe N.V. (Netherlands) - authorised for order execution, reception and transmission of orders, and transfer services passporting limited to the Netherlands.

This reflects continued momentum in MiCA authorisation activity, with firms now actively using the EU passport to offer regulated crypto services across member states.

Firms operating crypto-asset services in the EU should monitor the ESMA CASP register to track competitive landscape and passporting activity. Those not yet authorised under MiCA should assess their timeline for compliance. Contact the Ecovis team for guidance on MiCA authorisation strategy.

Detailed and full Regulatory Compliance Update on Financial Instruments 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 to 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.