REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

12.2024

ECOVIS ProventusLaw

Basel Institute on Governance

LINK

The Basel Institute on Governance has released the December 2024 edition of the Basel AML Index, along with updates to its methodology.

Key 2024 Basel AML Index Findings:

- Myanmar was ranked as the highest-risk jurisdiction globally for money laundering, with a score of 8.17.
- Other high-risk countries include Haiti, Democratic Republic of Congo, Chad, and Venezuela.
- Low-risk jurisdictions include San Marino, Iceland, Finland, Estonia, and Andorra.
- Australia, Israel, U.S., and U.K. ranked relatively low risk, with notable gaps in compliance areas still visible for improvement.

Methodology Updates:

- Corruption and Fraud Risks: Two new indicators, sourced from the Global Organized Crime Index, added to assess fraud risk better.
- Financial Transparency: Relocation of the Financial Secrecy Index under this category for clarity.
- Removal of three indicators due to outdated or discontinued data sources.
- Rebalancing of indicator weights to enhance index accuracy.

Global Observations:

- Asia, Africa, and South America remain high-risk regions due to corruption, regulatory gaps, and financial opacity.
- European nations like Iceland and Finland continue to lead in robust AML/CTF compliance.

The Bank of Lithuania

LINK

Bank of Lithuania: the fight against financial fraud needs to be taken to the highest level of government

The Bank of Lithuania has proposed the creation of a comprehensive national system for the prevention and suppression of financial fraud. This vision, presented to law enforcement, regulatory authorities, and financial market associations, emphasizes the need for a coordinated, state-level strategy involving both public and private sectors. The Bank of Lithuania highlighted challenges such as fragmented regulations, insufficient data-sharing due to privacy laws, and uneven engagement by market participants in fraud prevention efforts. It stressed the need for enhanced legal frameworks and a unified approach to effectively combat financial fraud.

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

12.2024

ECOVIS ProventusLaw

Changes to Resolution of the Bank of Lithuania

LINK

Changes to Resolution of the Bank of Lithuania No. 03-181 on the Approval of the Guidelines for the assessment of members of the management body and key function holders of financial market participants supervised by the Bank of Lithuania. The main amendments include the following:

- the Resolution is now applicable to crypto asset service providers and asset-linked token issuers;
- before selecting or appointing a person as member of the management body or key function holder, financial market participants must assess whether he or she meets the requirements set out in legal acts and record the assessment process and results.
- in terms of circumstances for assessing reputation, a criminal record or an initiated pre-trial investigation will be taken into consideration, regardless of when it was carried out and its outcome, with particular attention to a criminal record or an initiated pre-trial investigation for breaches indicated in the Resolution, additionally pointing out new circumstance to be assessed – history of administrative violations – their nature, repetition, systematicity.
- it will be required to provide an assessment of the collective suitability of all members of the collegial body after the appointment of the person being assessed.

The above-mentioned changes came into force from 30-12-2024.

On the consideration of a draft Resolution of the Board of the Bank of Lithuania

LINK

The Bank of Lithuania has prepared draft resolution (Draft Resolution) to update Resolution of the Bank of Lithuania No 247 of 30 December 2009 "On the approval of the description of the requirements for the management system of electronic money institutions and payment institutions and for the safeguarding of received funds".
This Draft Resolution has been prepared to address the most frequent deficiencies in practice in the operation of electronic money institutions and payment institutions (Institutions) and to implement the latest legislative requirements. It is proposed to introduce more detailed requirements to ensure proper governance of the Institutions and to enhance the risk culture in the Institutions as well to establish specific and further detail the existing requirements for effectively creating an internal control system in Institutions, while ensuring the principle of proportionality.

Requirements for the Electronic Money License and/or Payment Services Termination Plan (winding up plan) will come into effect on April 9, 2025.

The remaining provisions of the Draft Resolution will come into effect on May 1, 2025, with the exceptions indicated in the Draft Resolution.

Changes to Resolution of the Bank of Lithuania

LINK

Changes to Resolution of the Bank of Lithuania No 03-138 on the approval of the rules for the submission of notifications on the acquisition and disposal of a qualifying holding of the authorised capital and/or voting rights in financial market participants under supervision of the bank of Lithuania. The main amendments include the following:

- the Resolution is now applicable to acquisition and disposal of a qualifying holding in the authorized capital and/or voting rights of crypto asset service providers and asset-linked token issuers, central depository;
- detailing the documents to be provided.

The above-mentioned changes came into force from 30-12-2024.

REMINDER ON REPORTING

Please make sure you submit the quarterly and yearly reports as per deadlines. This includes:

- Statistical Payment data and Statistical data on Fraudulent Payments;
- Reports for supervision of the implementation of money laundering and terrorist financing prevention measures;
- Financial reports and activity (at all times be aware of the capital adequacy requirements);
- Reports to State Tax Inspectorate.

Detailed and full Regulatory Compliance Report on EMI, PI regulation can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

PERSONAL DATA PROTECTION AND ICT REGULATION

ECOVIS ProventusLaw

12.2024

Cyber Resilience Act enters into force

LINK

The Cyber Resilience Act (“CRA”) (Regulation (EU) 2024/2847Opens in new window) entered into force on 10 December 2024, and provides companies with a three-year grace period to put compliant products on the EU market (i.e. by 11 December 2027). It complements the NIS 2 Directive by introducing cybersecurity requirements for manufacturers of "products with digital elements" (“PDEs”), such as hardware and software products that are connected, whether directly or indirectly, to another device or network.

Commission Implementing Regulation laying down implementing technical standards for the application DORA with regard to standard templates for the register of information

LINK

On December 2, 2024, the Official Journal of the European Union published the EU Commission Implementing Regulation (EU) 2024/2956, dated November 29, 2024. This regulation establishes implementing technical standards for the application of the Digital Operational Resilience Act (DORA) in the financial sector, specifically regarding standard templates for the information register.

The Implementing Regulation outlines standard templates for an information register, which tracks all contractual arrangements regarding ICT services from third-party providers. Information gathered from that register is essential for the financial entities’ internal ICT risk management, for the effective supervision of the financial entities by their competent authorities, and for the establishment and conduct of oversight of the critical ICT third-party providers.

The Implementing Regulation came into effect on December 22, 2024.

Inspection by the State Data Protection Inspectorate (VDAI) on compliance with data protection requirements

LINK

Inspection by the State Data Protection Inspectorate (VDAI) on compliance with data protection requirements in the short-term vehicle rental sector.

Baltic data protection supervisory authorities conducted a joint preventive inspection to evaluate how the short-term vehicle rental sector adheres to the General Data Protection Regulation (GDPR) requirements. The inspection aimed to identify and mitigate risks associated with personal data processing in this rapidly growing industry.

Key findings included:

- Insufficient transparency;
- Failure to provide essential information to data subjects;
- Incorrect selection of legal grounds for data processing.

EDPB opinion on AI models: GDPR principles support responsible AI

LINK

The European Data Protection Board (EDPB) has adopted an opinion on using personal data to develop and deploy AI models. This opinion looks at 1) when and how AI models can be considered anonymous, 2) whether and how legitimate interest can be used as a legal basis for developing or using AI models, and 3) what happens if an AI model is developed using personal data that was processed unlawfully. It also considers the use of first and third-party data.

Commission adopts DORA Delegated Regulation on RTS specifying the criteria for determining the composition of the joint examination team

LINK

The European Commission has adopted a Delegated Regulation with regard to regulatory technical standards (RTS) specifying the criteria for determining the composition of the joint examination team ensuring a balanced participation of staff members from the European Supervisory Authorities (ESAs) and from the relevant competent authorities, their designation, tasks, and working arrangements under Regulation (EU) 2022/2554 (the Digital Operational Resilience Act or DORA).

These teams ensure balanced participation from the European Supervisory Authorities (ESAs) and relevant competent authorities. The act specifies criteria for team composition, member designation, tasks, and operational procedures to enhance supervisory consistency across the EU.

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 12.2024

ECOVIS ProventusLaw

The European Council of the European Union

LINK

Russia's war of aggression against Ukraine: EU adopts 15th package of restrictive measures.

On 16th December, the Council adopted a 15th package of economic and individual restrictive measures with the objective of further limiting Russia's ability to wage its illegal, unprovoked and unjustified war of aggression against Ukraine. These measures are designed to address the circumvention of EU sanctions through targeting of Putin's shadow fleet and weaken Russia's military and industrial complex.

The Council agreed on a significant package of 84 listings, which consists of 54 persons and 30 entities responsible for actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. Key targets include:

- Military units involved in attacks on Ukrainian civilians.
- Managers in Russian energy companies.
- Individuals linked to child deportations and propaganda.
- Senior officials in North Korea and non-EU actors supporting Russia militarily (e.g., Chinese entities).

The Council is adding further vessels to the list of those subject to a port access ban and ban on provision of a broad range of services related to maritime transport. This measure is intended to target non-EU tankers that are part of Putin's shadow fleet circumventing the oil price cap mechanism or support the energy sector of Russia, or vessels that are responsible for transporting military equipment for Russia or involved in the transport of stolen Ukrainian grain. 52 vessels originating from third countries were targeted today on these grounds, bringing the total of designated vessels to 79.

The European Council of the European Union

LINK

EU agrees first listings in response to destabilising activities against the EU, its member states and partners. For the first time ever, on 16th December 2024, the Council decided to impose restrictive measures against 16 individuals and three entities responsible for Russia's destabilising actions abroad. These measures are in response to Russia's malicious actions and its lack of respect for a rules-based international order and international law.

The relevant framework for restrictive measures was set up on 8 October 2024 to target those engaged in actions and policies by the government of the Russian Federation, which undermine the fundamental values of the EU and its member states, their security, stability, independence and integrity, as well as those of international organisations and third countries through hybrid activities of various kinds, including the use of coordinated information manipulation and interference.

Key Sanctioned Entities and Individuals:

- GRU Unit 29155: Known for foreign assassinations, bombings, and cyber-attacks in Europe.
- African Influence Networks:

- Groupe Panafricain pour le Commerce et l'Investissement and its founder, Harouna Douamba, involved in pro-Russian covert influence campaigns in Africa.
- African Initiative news agency, spreading propaganda and disinformation, and its editor-in-chief Artem Kureev.
- A GRU official overseeing Wagner Group operations in Africa post-Prigozhin.

- Doppelganger Campaign Leaders:

- Sofia Zakharova (linked to Russian government disinformation campaigns).
- Nikolai Tupikin (responsible for digital propaganda infrastructure).

- Espionage and Influence Operations:

- Vladimir Sergiyenko: Involved in intelligence operations against Germany.
- Visa Mizaev and his wife: Key figures in Russian espionage targeting German intelligence.

Sanction Mechanisms:

- Asset freezes for designated individuals and entities.
- Travel bans preventing entry or transit through EU territories.
- Prohibition on making funds or economic resources available to sanctioned individuals/ entities.

The sanctions reflect the EU's commitment to countering hybrid activities undermining EU and global stability, including disinformation, espionage, and cyber operations.

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

CONSUMER PROTECTION

12.2024

The European Commission

New EU General Product Safety Regulation (GPSR) Takes Effect.

The European Union's new General Product Safety Regulation (EU) 2023/988 (GPSR) came into force on December 13, 2024, replacing the previous General Product Safety Directive 2001/95/EC. This landmark regulation aims to enhance consumer protection and modernize product safety standards across the EU market.

Key aspects of the GPSR include:

- The regulation now covers new technologies, online marketplaces, and products sold through distance selling
- Manufacturers must conduct internal risk analyses and prepare technical documentation for products.
- Safety assessments now consider factors such as cybersecurity features.
- Products must bear identifying elements like type, batch, or serial numbers.
- Mandatory reporting of accidents through the Safety Business Gateway.
- Specific safety requirements for online platforms to protect consumers from dangerous products.
- Standardized recall notices and improved communication channels for consumer complaints.
- Modernized rapid alert system for dangerous products, enhancing information exchange between authorities.

The GPSR applies to products placed on the EU market from December 13, 2024, onward.

LINK

Our recommendation:

Businesses operating in or selling to the EU market should thoroughly review the new General Product Safety Regulation (GPSR) to understand its implications for their operations. Updating product safety assessment procedures, implementing robust traceability measures, and ensuring compliance with new documentation and reporting requirements are crucial. Online marketplaces and e-commerce platforms must pay special attention to their new obligations regarding product safety checks and consumer communication.

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

12.2024

ECOVIS ProventusLaw

Labour Code Amendments

LINK

Amendments to the Labour Code come into force on **1 January 2025**.
The main changes include:

- **Specify arrangements for additional work**. Agreements must specify the procedure for granting additional rights or obligations in order to ensure clearer regulation and reduce the risk of potential disputes (Article 35(4) of the Labour Code).
- **Employment of the general manager.** Employers must notify Sodra of the employment of the general manager at least one working hour before the scheduled start of work (Article 42(2) of the Labour Code).
- **Long-term service allowance.** In the event of termination of employment due to the employer's bankruptcy, employees are entitled to a seniority allowance calculated on the basis of uninterrupted service (Article 62(5) of the Labour Code).
- **Overtime**. Overtime work is now permitted only with the written consent of the employee, except in cases provided for by law (Article 119(2) of the Labour Code).
- **Parental leave.** The duration of the non-transferable two-month part of parental leave has been clarified as 62 calendar days (Article 134(3) of the Labour Code).
- **Overtime pay on public holidays and night shifts.** It has been explicitly stated that work during holidays and night shifts shall be compensated at a rate of no less than 2.5 times the regular wage (Article 144(4) of the Labour Code).

Order of the Chief State Labor Inspector On approving the description of measures for preventing violence and harassment at work No. EV-221

LINK

A description of measures to prevent violence and harassment at work, approved by a decree of the Chief State Labour Inspector of the Republic of Lithuania, has entered into force. description is intended to implement the provisions of Article 30(4) of the Labour Code on preventing violence and harassment at work. It sets out a list of necessary preventive measures to reduce the risks of violence and harassment at work, their impact on employees, and the procedures for implementing these measures. The following obligations are imposed on employers:

- **Implementation of the prevention policy.** Employers are obliged to develop and implement a clear policy on the prevention of violence and harassment.
- **Training for employees.** Provide regular training to employees on the prevention and recognition of violence and harassment.
- **Reporting system.** Ensure that an anonymous reporting system is in place where employees can report incidents of violence or harassment.
- **Investigation procedures.** Establish clear procedures for investigating reports of violence or harassment.
- **Psychological support.** Provide psychological support to employees who are victims.
- **Liability for violations.** Ensure that appropriate action is taken against employees who violate the prevention policy.

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

Our recommendations and details are in this file

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

CRYPTO

12.2024

ECOVIS ProventusLaw

The European Banking Authority (EBA)

European Banking Authority Consultation on CASPs' Central Contact Points (CCPs)

LINK

The EBA released a Consultation Paper amending regulatory technical standards for CASPs operating in multiple EU Member States. CASPs exceeding EUR 3 million in cumulative services per year in a host Member State may need to appoint a CCP to oversee AML/CFT compliance. CCPs will liaise with host Member State authorities, reducing compliance discrepancies across jurisdictions.

The European Commission

European Commission Guidance on MiCA and PSD2 Interplay

LINK

The European Commission has issued a formal communication addressing the regulatory complexities arising from the interaction between the MiCA and the Payment Services Directive (PSD2), particularly concerning e-money tokens (EMTs). EMTs are identified as having a dual nature, functioning both as crypto-assets under MiCA and as electronic money or funds under PSD2. As a result, CASPs offering payment services involving EMTs must either obtain a payment service provider (PSP) license or collaborate with an already licensed PSP.

The European Commission highlighted the risks posed by diverging interpretations of these regulatory frameworks across EU Member States, which could lead to instances of non-compliance. It underscored the importance of reducing redundant dual licensing requirements, streamlining authorization procedures, and enhancing operational efficiency for CASPs operating within the European Union.

While the EC acknowledged that forthcoming legislative developments, such as the Payment Services Regulation (PSR) and PSD3, aim to harmonize these regulatory obligations, it recognized that such measures may take up to three years to implement. To address the interim regulatory uncertainty, the European Commission proposed that the European Banking Authority and the European Securities and Markets Authority issue a "no-action letter." This letter would classify EMTs as "funds" under PSD2, clarifying that CASPs facilitating the storage, transfer, or exchange of stablecoins would not require a PSP license unless such activities are explicitly used for payment purposes.

This communication reflects the EC's commitment to fostering regulatory clarity, minimizing operational burdens, and ensuring a unified approach to the oversight of EMTs within the EU.

The European Securities and Markets Authority

LINK

On December 17, 2024, the European Securities and Markets Authority published its final package of Regulatory Technical Standards (RTS) and guidelines in preparation for the full implementation of the MiCA. This comprehensive package outlines key measures to enhance regulatory clarity and promote investor protection in the crypto-asset market.

The RTS on market abuse establishes specific systems, procedures, reporting obligations, and coordination measures designed to detect and prevent abuse within crypto markets. The reverse solicitation guidelines reaffirm this exemption's limited and exceptional scope, applying strictly to client-initiated services. Furthermore, guidelines on suitability require crypto-asset service providers (CASPs) offering advisory or portfolio management services to adhere to rules aligned with MiFID II when recommending crypto-assets.

The package also includes guidelines for crypto-asset transfer services, which aim to safeguard investor interests by defining detailed policies and procedures for CASPs involved in such transfers. Additional guidelines address the qualification of crypto-assets as financial instruments, providing clear conditions under which crypto-assets may fall within the scope of MiCA and MiFID II. Lastly, ESMA introduced principles for entities outside the purview of MiCA or the Digital Operational Resilience Act (DORA) to effectively manage ICT risks through robust system maintenance and security access protocols.

This package underscores ESMA's commitment to fostering a secure, transparent, and well-regulated environment for the crypto-asset market, ensuring both investor protection and regulatory compliance ahead of MiCA's full application.

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