REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

09.2024

ECOVIS ProventusLaw

Treasury Takes Coordinated Actions Against Illicit Russian Virtual Currency Exchanges and Cybercrime Facilitator

LINK

The U.S. Department of the Treasury has taken coordinated actions to disrupt Russian cybercrime activities. FinCEN identified PM2BTC, a Russian virtual currency exchanger linked to Sergey Ivanov, as a "primary money laundering concern." Simultaneously, OFAC sanctioned Ivanov and the virtual currency exchange Cryptex for facilitating cybercrime and laundering millions for ransomware actors.

As set out in the order, PM2BTC facilitates the laundering of convertible virtual currency (CVC) associated with ransomware and other illicit actors operating in Russia. PM2BTC provides direct CVC-to-ruble exchange services using U.S.-sanctioned financial institutions, otherwise facilitates sanctions evasion, and has failed to maintain a credible and effective anti-money laundering and know your customer (KYC) program.

The EU boosts the certification of the EU Digital Identity Wallets

LINK

The European Commission has requested ENISA, the EU Agency for Cybersecurity, to provide support for the certification of European Digital Identity Wallets. European Digital Identity Wallets will allow everyone in Europe to securely identify themselves when accessing public and private services as well as store and display digital documents like mobile driving licenses and education credentials — all from their mobile phones. They will also enhance privacy by only sharing the exact information agreed to.

FinCEN Withdraws Finding and Notice of Proposed Rulemaking Regarding ABLV Bank, AS

LINK

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has submitted a notice to the Federal Register withdrawing its finding that ABLV Bank, AS (ABLV) is a financial institution of primary money laundering concern, as well as the related notice of proposed rulemaking (NPRM) seeking to impose special measure. The ECB subsequently withdrew ABLV's banking license, and the Luxembourg subsidiary was ordered dissolved. Thus, ABLV no longer operates as a depository institution.

The bank is in the advanced stage of an irrevocable liquidation process supervised by the Government of Latvia, which ensures anti-money laundering/countering terrorist financing (AML/CFT) compliance. Furthermore, Latvian authorities have undertaken significant efforts to identify and address past illicit activity facilitated by the bank, resulting in criminal charges against owners of the bank and its senior managers. As a result, FinCEN has determined that ABLV is no longer a financial institution of primary money laundering concern.

Swedish Court Sends Ex-CEO of Swedbank to Prison

LINK

The former CEO of Swedbank, Birgitte Bonnesen, has been sentenced to prison for her involvement in the bank's extensive money laundering scandal. The Stockholm District Court found her guilty of fraud for misleading investors regarding the seriousness of the bank's anti-money laundering measures and its exposure to high-risk clients.

FinCEN Issues In-Depth Analysis of Check Fraud Related to Mail Theft

LINK

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) reported over $688 million in suspicious mail theft-related check fraud in the six months following its 2023 alert on the issue. During this period, 841 financial institutions filed 15,417 reports under the Bank Secrecy Act (BSA).

FinCEN, working with the U.S. Postal Inspection Service, stressed the critical role financial institutions play in identifying and reporting these crimes. Financial institutions are encouraged to continue filing Suspicious Activity Reports (SARs) and direct affected customers to the Postal Inspection Service for assistance.

Detailed and full Regulatory Compliance report on AML/CTF regulation can be found here:

Our recommendations and details are in this file

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

EMI, PI REGULATION

0≈ .2024

ECOVIS ProventusLaw

Recommendations of the Bank of Lithuania on the publication of standardized information to the public

LINK

Bank of Lithuania has publishes a list of standard information that electronic money and payment institutions should make public about their activities and risk management. Such information include:

- ∇ Activity Information
- ∇ Contact Information
- ∇ Language of Information
- ∇ Information about the terms of payment services provided to the payment service users
- ∇ Information about Complaints Handling
- ∇ Information about Customer Fund Protection
- ∇ Electronic Money Token (EMT) Whitepaper
- ∇ Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Prevention

Event organized by the Bank of Lithuania

LINK LINK

On September 26, 2024, Bank of Lithuania organized consultation event regarding DORA RTS ICT risk management.
The event focused on:

- Legal Framework Overview
- Enhancements to ICT Risk Management
- Simplified ICT Risk Management System
- Mandatory Compliance
- Scope of DORA Regulation
- Significance of Training and Awareness
- Communication Policies
- Monitoring and Reporting Requirements

REMINDER ON REPORTING

Please be aware that the third quarter has ended, meaning that quarterly reports have to be submitted to the Bank of Lithuania.
This includes:

- Report on statistical payment data;
- Reports for supervision of the implementation of money laundering and terrorist financing prevention measures;
- Financial reports (at all times be aware of the capital adequacy requirements).

Consultation event organised by the Bank of Lithuania

LINK LINK

On September 11, 2024, Bank of Lithuania organised consultation event regarding DORA regulation. The DORA regulation aims to enhance digital operational resilience across the financial sector by establishing requirements for ICT risk management and incident reporting.

During the event participants were updated on the adoption of Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) that will guide how institutions manage significant cyber incidents and classify threats.

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

Our recommendations and details are in this file

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

PERSONAL DATA PROTECTION AND ICT REGULATION

09.2024

ECOVIS ProventusLaw

Dutch Supervisory Authority imposes a fine on Clearview because of illegal data collection for facial recognition

LINK

The Dutch Data Protection Authority (Dutch DPA) imposes a fine of 30.5 million euro and orders subject to a penalty for non-compliance up to more than 5 million euro on Clearview AI. Clearview is an American company that offers facial recognition services. Among other things, Clearview has built an illegal database with billions of photos of faces, including of Dutch people. The Dutch DPA warns that using the services of Clearview is also prohibited.

The European Data Protection Board's data protection guide for small businesses is published

LINK

The European Data Protection Board (EDPB) has published translations of the EDPB's Data Protection Handbook (the Handbook) in 17 languages. As one of the key initiatives of the EADB's 2021-2023 strategy, the Handbook aims to help small businesses better comply with data protection requirements.
The Handbook aims to raise awareness of the GDPR and to provide small and medium-sized enterprises (SMEs) with practical information on GDPR compliance in an accessible and easy-to-understand format.

Personal data protection: the supervisory authority is not obliged to exercise a corrective power in all cases of breach and, in particular, to impose a fine

LINK

In Germany, a savings bank found that one of its employees had consulted a customer's personal data on several occasions without being authorised to do so. The savings bank did not inform the customer of this, as its data protection officer had taken the view that there was no high risk for him. The employee had confirmed in writing that she had neither copied nor retained the data, that she had not transferred them to third parties and that she would not do so in the future. In addition, the savings bank had taken disciplinary measures against her.

Our recommendation

In light of the recent case regarding unauthorized access to personal data by an employee of a German savings bank, financial market participants should take the following steps to ensure compliance with GDPR and minimize regulatory risk:

- Strengthen Internal Data Access Controls
- Enhance Incident Response Procedures
- Conduct Thorough Risk Assessments
- Ensure Full Cooperation with Supervisory Authorities
- Training and Disciplinary Measures

Danske Bank pays $7M to settle final probe over Estonia money laundering scandal

LINK

Danske Bank has agreed to pay the equivalent of $7 million in a settlement with French authorities over its failure to stop money-laundering at its former branch in Estonia.

The settlement: Danske Bank, the largest in Denmark, said Wednesday it had cooperated with French authorities and agreed to pay 6.33 million euros in a settlement with France's national financial prosecutor, ending that country's investigation into the bank.

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 09.2024

ECOVIS ProventusLaw

EU Best Practices for the Effective Implementation of Sanctions: Key Takeaways for Financial Market Participants

LINK

The Council of the European Union (Council) has updated its EU Best Practices for the Effective Implementation of Restrictive Measures. Published on 3 July 2024, the new version clarifies the threshold for the ownership test in relation to EU asset freeze restrictions and provides valuable guidance on EU sanctions concepts such as “control” over and “acting on behalf or at the direction” of an entity, amongst other updates.

US, UK and EU announce new measures against Iran and Russia

LINK

In September 2024, the US, UK, and EU announced coordinated sanctions against Iran and Russia in response to Iran's provision of ballistic missiles to Russia for use in Ukraine.

To ensure compliance with the latest regulatory developments:

- Review and update compliance procedures
- Conduct enhanced due diligence
- Monitor ongoing sanctions updates

EU updates list of items subject to Dual-Use Export Controls

LINK

The European Commission published a Delegated Regulation, updating the list f dual-use items contained in Annex I to Regulation (EU) 2021/821 (the “EU Dual Use List“)

- Review and update compliance frameworks
- Conduct enhanced due diligence
- Monitor regulatory changes

G7 Announces Industry Guidance on Preventing Evasion of Export Controls and Sanctions Imposed on Russia

LINK

Today, the United States, Canada, France, Germany, Italy, Japan, the United Kingdom, and the European Union (the G7) published, for the first time ever, **joint guidance** for industry on preventing evasion of the export controls and sanctions imposed on Russia.

The joint guidance outlines the following priority areas:

- Items that pose a heightened risk of being diverted to Russia;
- Red flag indicators of potential export control and/or sanctions evasion
- Best practices for industry to use to address these red flags and conduct enhanced due diligence.

German authorities seize cryptocurrency exchanges used for sanctions circumvention

LINK

The Frankfurt am Main Public Prosecutor's Office - Central Office for Combating Internet Crime (ZIT) - and the Federal Criminal Police Office (BKA) have shut down 47 exchange services hosted in Germany that were being used for criminal purposes. These were platforms on which conventional currencies and cryptocurrencies could be exchanged.

Our recommendation:

- Enhance Know-Your-Customer (KYC) Procedures
- Strengthen Monitoring of Crypto Transactions
- Conduct Regular Risk Assessments
- Collaborate with Authorities

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

Our recommendations and details are in this file

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

CONSUMER PROTECTION

09.2024

ECOVIS ProventusLaw

The Bank of Lithuania Addresses Payment Cancellation and Tracing Procedures:

LINK

Main concern: Misunderstandings between financial institutions and fraud victims often occur due to payment cancellation and tracing procedures.
Key recommendations:
1) Financial institutions should promptly respond to customer requests to cancel payments.
2) Institutions should provide clear information about the status of "reserved funds" and whether they can be recovered.
3) Customers should be informed about the payment process, especially for card transactions, including when a payment is considered completed and how to cancel or trace it.
Best practices observed:

- Priority handling of cancellation/tracing requests.
- 24/7 staff availability for such requests.
- Real-time status updates for customers.
- Multiple channels for submitting requests (email, online account, chat, phone, in-person).

The Bank of Lithuania Proposes Amendments to the Payment Law:

LINK

Main objective: Prevent payment service providers from including additional non-payment services in payment service packages without consumer consent.
Key points:
1) Ensure consumers can choose payment services relevant to their needs.
2) Providers cannot unilaterally impose unwanted products or services.
3) Consumers must always have the option to use a payment account and services separately, without tied non-payment products.
4) Providers must clearly present pricing information for both bundled and separate services.
5) Providers cannot unilaterally start offering tied or grouped services without consumer consent.

The Lithuanian Ministry of Finance

LINK

The Lithuanian Ministry of Finance has prepared draft legislation to enhance consumer protection for remote financial service agreements.
Key changes include:
1. Increased information requirements for service providers.
2. Mandatory access to human specialists for customer consultations.
3. Simplified contract cancellation processes, making it as easy to cancel as to sign up.
4. Prohibition of misleading or manipulative interface designs ("dark patterns").
5. Detailed explanations of contract terms and additional services.
6. Stricter sanctions for non-compliance with regulations.
7. Integration of technical functions for easy contract cancellation in electronic interfaces.

Detailed and full Regulatory Compliance report on Consumer Protection Regulation can be found here:

Our recommendations and details are in this file

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

09.2024

ECOVIS ProventusLaw

Administrative Case No eA-1670-575/2024

LINK

The Supreme Administrative Court of Lithuania (SACL) is reviewing a case involving the Migration Department's annulment of a temporary residence permit application from a dual Canadian-Russian citizen.

Despite entering Lithuania visa-free as a Canadian, the Migration Department cited the Law on Restrictive Measures, which mandates that Russian citizens must present a valid visa or residence permit when applying for a temporary residence permit.

The applicant argues that this requirement violates the Comprehensive Economic and Trade Agreement (IEPA) between Canada and the EU.

The court has posed two questions to the Court of Justice:

1. Can a dual citizen of Canada and Russia rely on the IEPA in national court for a temporary residence permit appeal?

2. Does Regulation (EU) 2018/1806 permit national laws to require a visa for Russian nationals, despite their entry under a visa waiver as Canadian citizens?

The court seeks clarity on the interplay between national law and international agreements in this context.

Description of the Procedure for Allocating and Paying Benefits to Employers Who Hire Employees from Abroad.
Description of the Conditions and Procedures for the Implementation of Employment Support Measures.

LINK LINK

The Employment Service provides subsidies for employers and employees:

1. High Value-Added Qualifications and Competencies:

Employees can receive subsidies for acquiring qualifications listed in the High Value-Added Qualifications and Competencies List.

Subsidy limits are:

- Up to €8,316 (9 minimum monthly wages) for a high value-added qualification.
- Up to €4,620 (5 minimum monthly wages) for upgrading a qualification or acquiring a competency.

2. Attracting Highly Qualified Employees from Abroad:

Since July 1, 2022, employers can apply for a one-time subsidy of up to €6,652.8 (7.2 minimum monthly wages) when hiring highly qualified employees from abroad. This does not apply to the hiring of Ukrainian citizens.

We recommend checking if your company is eligible for a subsidy.

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

CRYPTO

09.2024

ECOVIS ProventusLaw

ESMA, List of Central Counterparties authorised to offer services and activities in the Union

LINK

ESMA's updated list of CCPs authorized to offer services in the Union relating to crypto-assets

The list provides guidance on the companies that are allowed to provide certain activities as central counter parties that relate to crypto-assets.

EBA, Public hearing: Joint-ESA Guidelines under Article 97(1) MiCAR

LINK

ESA publishes slides from a public hearing on the guidelines on crypto-asset classification

The slides provide an informative summary of the guidelines relating to the classification of crypto-assets and differentiation of asset-referenced tokens from other crypto-assets.

European Council, Policy titled "Crypto-assets: how the EU is regulating markets"

LINK

European Council's general overview of crypto-asset regulation in the EU

The European Council published an entry-level overview of the European Union's regulation relating to crypto-assets in the Union.

EBA, Final report on guidelines on liquidity stress testing under MiCAR

LINK

EBA Publishes final report on guidelines on liquidity stress testing under MiCAR

The final report concerns the stress testing of asset-referenced tokens and electronic money tokens and is now available in all official EU languages, and a list of regulators with their compliance timelines regarding these new requirements.

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

REGULATORY COMPLIANCE UPDATE

EU WHISTLEBLOWING DIRECTIVE

ECOVIS ProventusLaw

Whistleblowing Directive Implementation

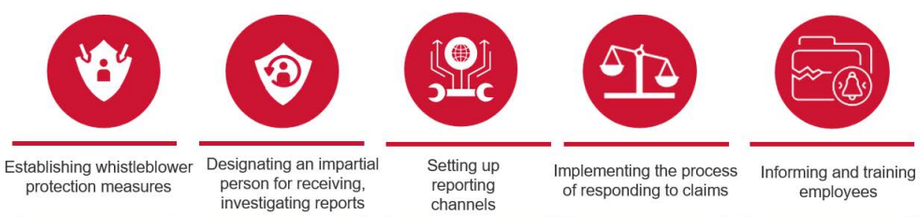
LINK

The EU Whistleblower Directive is mandatory for all organisations with more than 50 employees. **For financial institutions this legislation is mandatory regardless of number of employees** and is designed to protect individuals who report 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. This directive underscores transparency, accountability, and responsible conduct, aligning with broader ESG objectives to promote sustainable and ethical business practices across the European Union and beyond.

This Directive introduces several key provisions, including:

1. Scope: The directive covers many areas where EU law applies, including public procurement, financial services, product safety, environmental protection, public health, consumer protection, and more.
2. Reporting Channels: Member states and certain private entities must establish secure and confidential reporting channels for whistleblowers. These channels must be easily accessible and capable of handling reports effectively.
3. Protections: The directive prohibits retaliation against whistleblowers, including dismissal, demotion, harassment, and discrimination. It also requires member states to provide effective remedies for whistleblowers who experience retaliation.
4. Confidentiality: Whistleblowers' identities must be kept confidential throughout the reporting process unless disclosure is necessary for investigation or legal proceedings.
5. Follow-Up: Once a report is submitted, the relevant authorities or organisations must acknowledge receipt and provide feedback to the whistleblower within a reasonable timeframe.

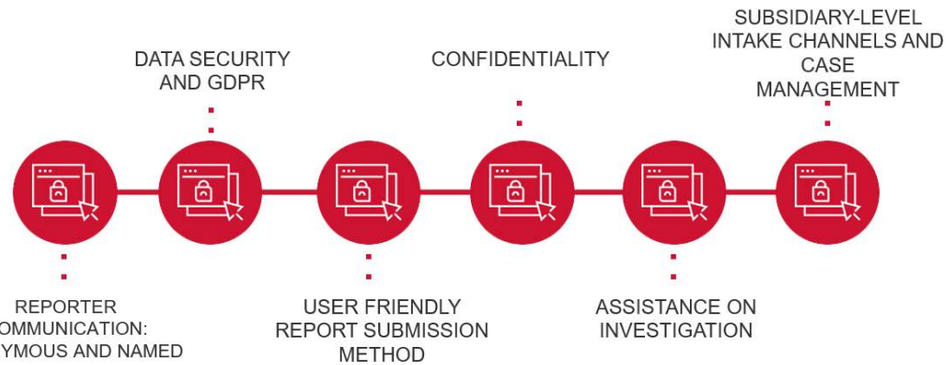
Under the EU Whistleblower Directive, organisations must establish secure and confidential reporting channels for whistleblowers. The reporting process is designed to ensure the protection of whistleblowers and the effective handling of reports of wrongdoing.



WHISTLEBLOWING SOLUTION BY ECOVIS
Outsourcing solution for companies

LINK

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. This allows organisations to focus on their core activities while effectively managing whistleblowing cases.



Discover how Ecovis Whistleblowing'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.

Whether companies require a reporting channel only or a comprehensive investigative service, Ecovis Whistleblowing provides a reliable solution tailored to their needs, fostering transparency and compliance with the EU Whistleblower Directive. Contact us at vilnius@ecovis.lt, and we will ensure compliance with the Whistleblowing Directive tailored to your specific situation and available resources.