REGULATORY COMPLIANCE UPDATE

EU WHISTLEBLOWING DIRECTIVE

ECOVIS ProventusLaw

Whistleblowing Directive Implementation

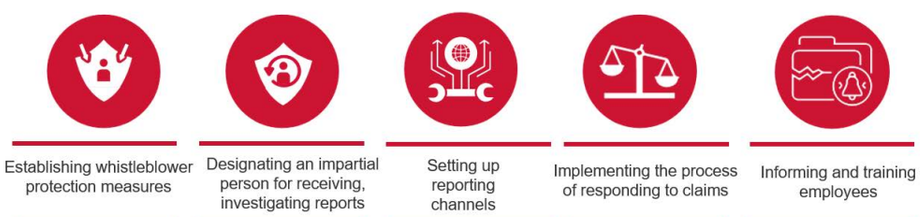
LINK

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.

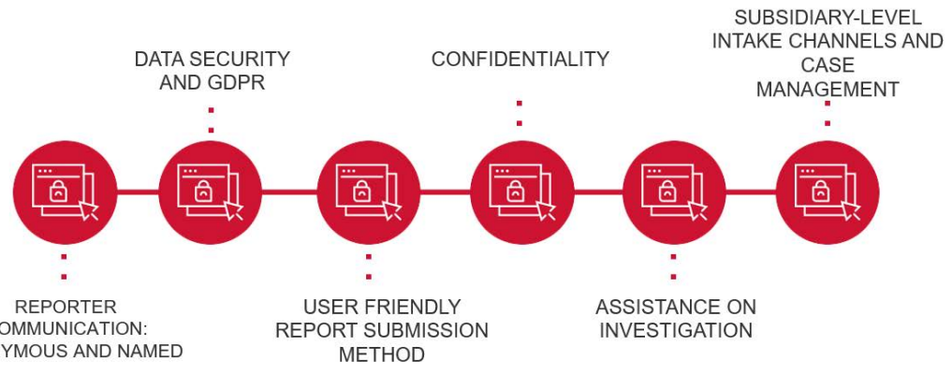
Under the EU Whistleblower Directive, organisations must establish secure and confidential reporting channels for whistleblowers. The reporting process is designed to ensure the protection of whistleblowers and the effective handling of reports of wrongdoing.



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.

REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

07.2024

ECOVIS ProventusLaw

On approval of the description of unacceptable risk criteria for potential and existing holders of an addressable BIC of the Bank of Lithuania payment systems

LINK

The Board of the Bank of Lithuania has approved a new description of unacceptable risk criteria applicable to potential and existing holders of addressable BICs of the Bank of Lithuania's payment systems. This resolution is aimed at ensuring that payment service providers (PSPs) are of good repute and comply with all requirements for the prevention of money laundering, terrorist financing and the implementation of international sanctions.

Expectations of the Bank of Lithuania regarding the provision of cryptocurrency and related services

LINK

The Bank of Lithuania has updated its stance on crypto-assets and related services, in line with the European Parliament and Council Regulation (EU) 2023/1114 (MiCA). This regulation came into effect in Lithuania on June 30, 2024, with the Bank of Lithuania designated as the supervisory authority for this sector. Crypto-asset service providers must adhere to strict requirements to ensure financial stability and prevent money laundering. The Bank of Lithuania aims to ensure that mature and competent participants enter the market, emphasizing a thorough licensing process and the readiness of potential market entrants.

Effective Suspicious Activity Reporting by Wolfsburg Group

LINK

The Wolfsberg Group's statement on effective monitoring of suspicious activity highlights the evolving strategies financial institutions (FIs) should adopt to combat financial crime was released on 1st July 2024. The statement underscores the importance of transitioning from traditional methods to more sophisticated, technology-driven approaches, particularly through the use of machine learning (ML) and artificial intelligence (AI).

New Guidelines for Financial Market Participants to Avoid Unjustified De-Risking and Properly Inform Consumers

LINK

To enhance the user experience of payment service consumers and improve the application of anti-money laundering risk management measures by financial institutions, the Board of the Bank of Lithuania has established new requirements for financial market participants – banks, credit unions, electronic money institutions, and payme institutions. These guidelines on financial service accessibility a financial inclusion will take effect from the beginning of next yea, allowing time for preparation.

Inspection of UAB "IBS Lithuania"

LINK LINK

The Bank of Lithuania conducted an inspection of UAB "IBS Lithuania" and found that the electronic money institution did not consistently comply with international financial sanctions, restrictive measures implementation, and customer representative identification requirements.

During part of the review period, the institution's internal policy and internal control procedures did not include adequate quality assurance and testing process measures related to the implementation of international financial sanctions and restrictive measures, and these measures were not applied sufficiently in practice. Deficiencies were also identified regarding the institution's information technology system, including the verification of information concerning clients, client representatives, and beneficial owners in the context of implementing international financial sanctions and restrictive measures, as well as identifying the identities of client representatives (additional account users).

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

Our recommendations and details are in this file

Supreme Administrative Court of Lithuania (LVAT) has issued a final and unappealable ruling rejecting the complaint of "Paysera LT''

LINK

The Supreme Administrative Court of Lithuania (LVAT) has issued a final and unappealable ruling rejecting the complaint of "Paysera LT," UAB, regarding the decision of the Bank of Lithuania, which restricted the institution's ability to serve certain clients posing a higher risk of money laundering and terrorist financing.

The court noted that the restrictions imposed on the applicant's activities by the Bank of Lithuania are proportionate, considering the suspicions that the applicant was inadequately implementing measures for the prevention of money laundering and terrorist financing, failing to comply with the instructions given by the Bank of Lithuania, and not taking timely actions to rectify identified deficiencies to prevent further harm to the public interest.

ECB Is Pushing UK Fintech Revolut to Bolster EU Bank Controls Amid Review

LINK

The European Central Bank (ECB) is urging Revolut Ltd. to enhance its financial crime controls and governance after identifying several shortcomings during a review of its EU subsidiary, Revolut Holdings Europe UAB. This scrutiny comes as Revolut seeks a banking license in the UK, a process that has been delayed for over three years, prompting frustration from its founder, Nikolay Storonsky.

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

EMI, PI REGULATION

07.2024

ECOVIS ProventusLaw

Ecovis ProventusLaw DORA services

LINK

The Digital Operational Resilience Act (DORA) is a EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025.
Ecovis ProventusLaw started providing services that include:

- Assessing your current security posture and compliance level with the DORA
- Identifying the gaps and risks in your network and information systems, and providing recommendations for improvement
- Designing and implementing security policies, procedures, and controls that meet the DORA requirements
- Providing training and awareness programs for your staff and stakeholders on the DORA obligations and best practices
- Assisting you in reporting incidents and breaches to the relevant authorities and stakeholders
- Preparing you for audits and inspections by the competent authorities and providing support during the process
- Helping you manage and mitigate the impact of any sanctions or enforcement actions.

If you need assistance ensuring compliance with the Digital Operational Resilience Act (DORA) and strengthening your IT security, Ecovis ProventusLaw is ready to assist you in any matter related to DORA regulation.
We invite you to complete the DORA Regulation Compliance Questionnaire. This questionnaire helps us to understand your level of DORA compliance. Your participation will provide insights and feedback on your compliance practices and challenges regarding the DORA Regulation.

Supervisory decisions for financial market participants

LINK

The Bank of Lithuania has published an overview of the activities of electronic money and payment institutions, which analyzes the structure of this sector, significant changes, participants, and their financial results, as well as providing information on supervisory actions and other relevant issues (such as customer fund protection).
For an overview of the activities of electronic money and payment institutions, click *here*.

LINK

Due to the emerging threat to the safe and reliable activities of the electronic money institution Foxpay UAB (hereinafter – Foxpay) and the interests of users, Bank of Lithuania restricted the activities of Foxpay and appointed a temporary representative to oversee the institution's activities.
In its decision, the Bank of Lithuania instructed Foxpay:

- Not to start new business relationships and not to provide financial services to customers related to the institution's shareholder Ieva Trinkūnaitė;
- Not to start new business relationships and not to provide financial services to customers classified as a higher risk group of money laundering and terrorist financing, to customers providing investment (Forex, spreads), gambling, information technology, marketing and virtual currencies services.

Publication by the Bank of Lithuania

LINK

Electronic Money Institutions (EMIs) and Payment Institutions (PIs) providing payment services will be able to gain direct access to payment systems managed by the central banks of the Eurosystem, including the TARGET payment system. However, these institutions will not be provided with the service of safeguarding client funds in central banks.
In the payment system account opened for EMIs and PIs, there can be own and/or client funds as necessary to perform payments. However, client funds that must be protected according to legal requirements must be kept in a safeguarding account at a bank or credit union operating in the European Union or invested in safe, liquid, and low-risk assets, as currently required by law.

The Bank of Lithuania has been given a 9-month period to adapt to the Eurosystem's policy. This means that EMIs and PIs that do not have a safeguarding account at a credit institution must open one within 9 months.

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

07.2024

ECOVIS ProventusLaw

2,385,276 euro fine received by company operating online second-hand clothing trading and exchange due to non-compliance with the General Data Protection Regulation

LINK

The Lithuanian State Data Protection Inspectorate (VDAI) imposed a €2,385,276 fine on Vinted, UAB, the company behind the online second-hand clothing platform "Vinted." This decision followed an investigation triggered by complaints from French and Polish supervisory authorities.

The VDAI identified breaches of the General Data Protection Regulation (GDPR), specifically regarding articles on lawfullness, fairness and transparency, accountability as well as transparent communication and user rights.

Additionally, the investigation uncovered Vinted's use of "shadow blocking," a practice where users suspected of violating platform rules were covertly blocked without their knowledge, violating principles of fairness and transparency. This affected users' ability to exercise other GDPR rights.

The VDAI concluded that Vinted failed to implement sufficient technical and organizational measures to demonstrate compliance with the accountability principle, especially regarding data access rights.

Account of personal data breaches in Lithuania (first half of 2024)

LINK

In the first half of 2024, Lithuania's State Data Protection Inspectorate (VDAI) received 151 reports of personal data security breaches, affecting approximately 402,446 individuals, an increase from 130 reports and 328,929 affected individuals in the same period in 2023.

ESMA Highlights Risks in Global Crypto Firms and Advances DORA Implementation

LINK

The European Securities and Markets Authority (ESMA) has recently issued significant updates relevant to participants in the financial markets, focusing on the challenges posed by global crypto firms and the advancement of the Digital Operational Resilience Act (DORA).

Addressing Global Crypto Firms Under MiCA

ESMA has published an Opinion highlighting the risks associated with global crypto firms seeking partial authorization under the Markets in Crypto-Assets (MiCA) regulation. The concern arises from these firms conducting substantial parts of their operations, such as intra-group execution venues, outside the European Union's regulatory scope. Such practices could lead to reduced consumer protection and create an uneven playing field compared to EU-authorized venues. ESMA urges National Competent Authorities (NCAs) to rigorously assess these firms' business structures during the authorization process to ensure compliance with MiCA's requirements. This Opinion is part of ESMA's broader effort to ensure effective application of MiCA across the EU.

Advancing Digital Operational Resilience

In parallel, ESMA, along with the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA), has released the second batch of policy products under DORA. These include regulatory and implementing technical standards aimed at enhancing the EU financial sector's digital operational resilience. Key areas covered include ICT-related incident reporting, threat-led penetration testing, and guidelines on subcontracting for critical functions. The ESAs emphasize the importance of these measures in ensuring the continuity of financial services and safeguarding customer data against emerging cyber threats.

Market participants are encouraged to stay informed about these developments, as they signal the EU's ongoing efforts to strengthen financial stability and operational resilience in the face of evolving technological risks.

Artificial Intelligence Act

LINK

The EU's AI Act aims to regulate artificial intelligence systems, ensuring they align with fundamental rights and values. It covers a range of AI applications, including facial recognition and predictive policing.

Key Points:

- The AI Act is directly applicable across all EU member states, requiring them to establish national authorities and enforce penalties for violations.
- It has extraterritorial reach, affecting AI providers outside the EU that impact EU markets.
- AI systems are categorized based on risk levels:
  - **Unacceptable Risk**: Banned systems (e.g., social scoring).
  - **High Risk**: Subject to strict requirements (e.g., in health and law enforcement).
  - **Limited Risk**: Must inform users they are interacting with AI (e.g., chatbots).
  - **Minimal Risk**: Few obligations, encouraged to follow voluntary guidelines (e.g., video games).

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 07.2024

ECOVIS ProventusLaw

The Financial Crimes Investigation Service (FCIS) imposed a record fine of over €8.23 million on the Lithuania-registered virtual currency wallet operator and virtual currency exchange operator (VASP)

LINK

The Financial Crimes Investigation Service (FCIS) imposed a record fine of over €8.23 million on the Lithuania-registered virtual currency wallet operator and virtual currency exchange operator (VASP) company “Payeer” for violations of international sanctions.
An additional fine of more than €1.06 million was issued to the company for violations of the Law on the Prevention of Money Laundering and Terrorist Financing.

Sanctions Implementation Commission found that since the actual start of operations, UAB “Payeer” has been linked to the cryptocurrency platform “Payeer.com,” allowing its clients, primarily from Russia, to conduct transactions in Russian rubles, transferring them to and from EU-sanctioned Russian banks. Russian individuals and legal entities were also provided with the opportunity to obtain cryptocurrency wallets and account management or custody services.

According to legal regulations, the company, when providing VASP services, was required to conduct customer identity verification, ensure that services were not provided to sanctioned clients, close existing accounts, suspend the entities' access to funds or economic resources, and inform the FCIS of such suspensions.
It was established that the company had been violating international sanctions laws for over 1.5 years. During this period, UAB “Payeer” reportedly had no less than 213,000 clients, with revenues exceeding €164 million. The violations committed by the company were assessed as severe, and the company did not cooperate or provide explanations, resulting in the imposition of the monetary fine of over €8.236 million.

Moreover, violations of the Prevention of Money Laundering and Terrorist Financing were identified. It was found that the company did not report to the FCIS on customer operations or transactions involving virtual currency that equaled or exceeded €15,000. Deficiencies were recorded in the internal policies and internal control procedures related to the identification and verification of clients and beneficial owners, risk assessment, risk management, and reporting and information submission to the FCIS, among others.
Considering the scale and nature of the Prevention of Money Laundering and Terrorist Financing violations, the company was fined €1.06 million.
This is currently the largest monetary penalty imposed by the FCIS for violations of international sanctions.

Updated FAQs on Services Published by the European Commission on July 2, 2024

LINK

European Commission Updates FAQs on EU Sanctions Compliance
On July 2, 2024, the European Commission (EC) released an updated set of FAQs, providing critical updates and clarifications on the application of EU sanctions. The key updates cover service provisions, business withdrawal from Russia, the "No Russia" clause, and other essential areas.

Treasury Maintains Pressure on Houthi Illicit Shipping and Finance Schemes

LINK

On July 18, 2024, OFAC imposed sanctions on a dozen individuals and vessels that played a crucial role in financing the destabilizing activities of the "Houthis" in the region as part of the Sa'id al-Jamal network.
Sanctions were imposed on Mohammad Roslan Bin Ahmad, a Malaysian and Singaporean citizen residing in Indonesia, and Zhuang Liang, a Chinese citizen residing in the People's Republic of China (PRC), who helped the network conduct illicit transfers and participated in money laundering.

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 07.2024

BoL newsfeed

LINK

Bank of Lithuania: consumer experience must continue to improve.

The Bank of Lithuania's assessment indicates that most payment service providers in the country are working to improve the consumer experience, though some need significant improvements. Over 100 financial institutions were evaluated on their efforts to meet consumer expectations. BoL emphasizes the necessity for financial institutions to ensure quality and accessible services, continuously monitor customer needs, properly handle complaints, and take corrective actions. The assessment revealed that many institutions actively strengthen customer relations, measure satisfaction, monitor feedback (including on social media), and involve relevant employees and senior management in resolving systemic issues highlighted by complaints.

The Bank of Lithuania has issued guidelines to improve consumer protection and standardize the distribution of investment life insurance products

LINK

The guidelines outline best practices and highlight risky activities that may lead to consumers purchasing unsuitable products. For example, distributors must accurately assess a consumer's needs and provide clear, objective information about insurance products. This enables consumers to make informed decisions.

Recognizing the need for time and resources to implement certain provisions, the Bank has allowed a one-year period for market participants to comply with guidelines requiring substantial investments, such as adapting information technology systems. This phased approach aims to ensure a smooth transition to the new standards.

Decision of the State Consumer Rights Protection Authority of Lithuania

LINK

100 000 Eur fine to Membershop.

The State Consumer Rights Protection Authority of Lithuania (VVTAT) found that UAB "BALTIJOS DIDMENA" (one of the biggest e-shop in Baltic states) on their website www.membershop.lt displayed misleading advertisements. These ads compared product prices with the manufacturer's recommended retail price (RRP), giving the false impression of discounts when no discounts were actually applied.

VVTAT emphasized that sale prices should be compared with the previous prices of the products, not misleading reference prices like RRP. Despite multiple warnings and recommendations from VVTAT between 2020 and 2023, the company did not fully comply and continued to mislead consumers until June 2023.

As a result, VVTAT concluded that the advertising practices from 2020 to 2024 were incorrect and misleading, violating the Advertising Law. Consequently, a fine of 100 000,00 euros was imposed.

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

Our recommendations and details are in this file

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

07.2024

ECOVIS ProventusLaw

Amendments to Labour Code od Republic of Lithuania

LINK

Effective June 21, 2024, significant updates to the Lithuanian Labor Code (DK) and Civil Procedure Code (CPK) are now in effect. The amendments to the Labor Code introduce new requirements for employee documentation. Employees are now responsible for providing proof of entitlements, such as disability benefits or family leave. Employers are no longer required to proactively identify these entitlements.

The changes also allow employees to terminate their contracts and receive severance if they cannot work due to illness or caregiving responsibilities, focusing on the need for time rather than the caregiving location. Additionally, disabled employees can work night or overtime shifts only with medical clearance and their consent.

In the Civil Procedure Code, new limits on wage deductions have been set. From July 1, 2024, deductions are capped at 10% for wages up to the minimum wage, 30% for wages between the minimum wage and twice the minimum wage, and 50% for wages exceeding twice the minimum wage.

Employers should update their policies and payroll systems to comply with these changes.

Press Release from the State Labor Inspectorate

LINK

In the first half of 2024, the State Labor Inspectorate received reports of 4 fatal and 18 serious workplace accidents.

In response, the Chief State Labor Inspector has ordered unplanned inspections from August 1 to October 1 in sectors including forestry, agriculture, wholesale trade, wood products and furniture manufacturing, warehousing, and construction. The focus will be on fall prevention and ensuring compliance with safety regulations, with special attention to:

- The prevention of falls from heights
- Ensuring that personal protective equipment and work tools used by self-employed individuals comply with occupational safety and health regulations
- Verifying the implementation of appropriate collective fall protection measures.

At least 260 additional inspections are planned.

Violations will result in the strictest administrative sanctions. Non-compliance at construction sites will lead to additional administrative offense protocols for construction managers.

Press release of the State Lobour Inspectorate

LINK

Considering the opinions expressed by representatives of trade unions and employers' organizations in the Tripartite Council, the proposal from the Bank of Lithuania, and the updated economic fore[illegible] the Ministry of Social Security and Labor proposes that the Governm[illegible] a compromise decision and apply a minimum monthly salary (MMA) [illegible] euros (before taxes) in 2025, instead of the currently set 924 euros.

The MMA would increase by 114 euros, or 12%. Accordingly, the minimum hourly wage would increase to 6.35 euros (currently 5.65 euros).

The MMA for 2025 will be approved by a Government resolution, the public consultation process for which has just begun.

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

CRYPTO

07.2024

ECOVIS ProventusLaw

Bank of Lithuania's letter of expectation regarding the requirements for EMT and ART issuers in light of MiCA regulation

LINK

Bank of Lithuania's expectations for EMT and ART issuers

The Bank of Lithuania published its expectations for EMT and ART issuers in light of the newly implemented MiCAR requirements. The expectations go beyond the requirements of MiCAR and provide insight into the regulator's views on certain practical aspects of adhering to MiCAR's requirements. For example, the BoL does not practically foresee that an EMI could also hold a CASP license.

EBA Statement for the attention of persons issuing to the public, offering to the public, or seeking admission to trading of asset-referenced tokens (ARTs) and e-money tokens (EMTs) and for consumers

LINK

EBA Highlights MiCAR Compliance for Crypto-Asset Issuers

The European Banking Authority (EBA) has issued a statement urging issuers and consumers to adhere to the new Markets in Crypto-assets Regulation (MiCAR) requirements for asset-referenced tokens (ARTs) and e-money tokens (EMTs). The EBA emphasizes supervisory priorities for 2024/2025, including governance, financial resilience, technology risk, and financial crime management, aiming to ensure consistent application and high holder protection standards across the EU.

European Supervisory Authorities' consultation paper on the Draft Guidelines on templates for explanations and opinions, and the standardised test for the classification of crypto-assets, under Article 97(1) of Regulation (EU) 2023/1114

LINK

ESAs Seek Feedback on Crypto-Assets Regulation Guidelines

The European Supervisory Authorities (ESAs) have launched a consultation on guidelines under the Markets in Crypto-Assets Regulation (MiCA). The guidelines propose standardized tests and templates for explaining the classification of crypto-assets. Stakeholders can submit comments by October 12, 2024. A public hearing is scheduled for September 23, 2024, to discuss these proposals, aimed at ensuring a consistent approach across the EU.

ESMA Opinion on global crypto firms' use of their non-EU execution venues

LINK

The European Securities and Markets Authority (ESMA), the EU's financial markets regulator and supervisor authority, issued an opinion to address the risks presented by global crypto firms seeking authorisation under the Markets in Crypto Assets (MiCA) Regulation for part of their activities (crypto brokerage) while keeping a substantial part of their group activities (intra-group execution venues) outside the European Union (EU) regulatory scope.

Final Draft Implementing Technical Standards amending Commission Implementing Regulation (EU) 2021/451 on supervisory reporting referred to in Article 430 (7) of Regulation (EU) No 575/2013 concerning output floor, credit risk, market risk, operational risk, crypto assets and leverage ratio

LINK

The European Banking Authority (EBA) has updated its supervisory reporting framework to align with new regulatory changes from CRD VI/CRR3, effective January 1, 2025. This includes amendments for Basel III reforms and specific reporting requirements for operational risks and crypto assets. A consultation process is ongoing to finalize these technical standards, with the first reporting due by June 2025. The EBA's roadmap outlines the timeline and implementation steps for these updates.
In December 2022, the Basel Committee on Banking Supervision published the final prudential standard on the treatment of institutions' crypto-asset exposures to address potential risks for institutions caused by these exposures that are not sufficiently covered by the existing prudential framework. The standard is applicable from 1 January 2026, although some technical elements are still being further developed.

EBA Draft Guidelines on templates to assist competent authorities in performing their supervisory duties regarding issuers' compliance under Titles III and IV of Regulation (EU) 2023/1114

LINK

EBA launched a consultation on draft Guidelines on reporting requirements to assist competent authorities and the EBA in performing their duties under MiCAR. These Guidelines should ensure that Competent Authorities have sufficient comparable information to supervise compliance of issuers with MiCAR requirements and provide the EBA with the information necessary to conduct the significance assessment under MiCAR. The consultation runs until 15 October 2024. Includes templates and instructions.

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

Our recommendations and details are in this file