



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.



Establishing whistleblower protection measures



Designating an impartial person for receiving, investigating reports



Setting up reporting channels



Implementing the process of responding to claims



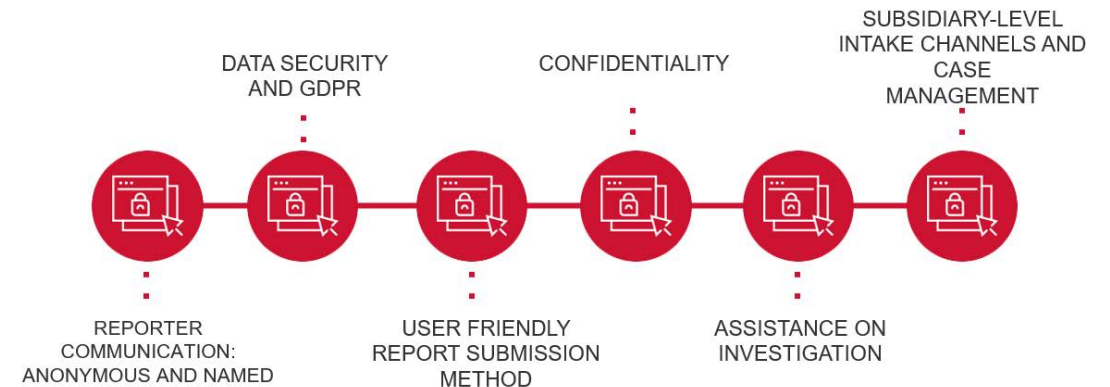
Informing and training employees

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.



The increased risk of terrorist financing: now is the right time to review CTF programs



LINK

In response to the events in Israel in October the last year, the U.S. Financial Intelligence unit (FINCEN) released a warning regarding potential threats, related to financial flows intended to finance terrorist activities of HAMAS.

Financial Crimes Investigation Service (FCIS) and the Bank of Lithuania warned financial market participants and other obliged entities under the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania about the increased risks of terrorist financing activities in Israel and the Gaza Strip.

Terrorist financing is difficult to spot

Creating effective risk management scenarios for monitoring terrorist financing is a significant challenge, even for well-established financial institutions. Terrorist groups often receive funding in small, seemingly legitimate amounts, making it challenging to differentiate these transactions from regular financial activities.

The market faces an uneven risk of terrorist financing

Regarding defense mechanisms for the terrorist financing, compliance with existing regulation is a necessary and non-negotiable aspect. However, the tactics used by criminals also change with time, so the internal review of prevention programs helps to more accurately assess in which direction to improve. The effectiveness of the defensive mechanisms – the procedures used, and the tools used – is the common denominator that binds both the experienced financial market players and newcomers, since all market participants are potentially at risk of finding themselves in the chain of supporting terrorists.

Guidance on Beneficial Ownership and Transparency of Legal Arrangements



LINK

Following the February 2023 revisions to FATF Recommendation 25 on Beneficial ownership and transparency of legal arrangements, the FATF has updated its risk-based guidance for this Recommendation.

The guidance complements the existing guidance on Recommendation 24 on legal persons and aims to help stakeholders from the public and private sectors to implement the new requirements more effectively.

Guidance on Beneficial Ownership and Transparency of Legal Arrangements



LINK

The EU Council has unveiled a comprehensive set of measures to strengthen the protection against money laundering and terrorist financing within the bloc. This new package, announced on January 18, 2024, introduces significant changes to AML regulations, particularly focusing on enhancing transparency in the disclosure of beneficial ownership information related to property located in EU Member States. The proposal recognizes that beneficial ownership is based on two components; that of ownership of a significant proportion of the shares in property-holding entity, and control of the entity due to ability to exert significant influence over those who make decisions on behalf of entity.

Companies in the VASP sector can now provide mandatory information to the FCIS



LINK

Depository virtual currency wallet operators and virtual currency exchange operators (companies in the VASP sector) can now provide mandatory information to the Financial Crimes Investigation Service (FCIS).

Impact measures imposed by the Bank of Lithuania



LINK

The Bank of Lithuania has carried out an inspection of "Secure Nordic Payments", UAB, and found violations of the legal acts, for which, the Bank of Lithuania imposed a fine in amount of 210 000 Eur.

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

Our recommendations and details are in this file



info@proventuslaw.it





Consultative event organised by the Bank of Lithuania



LINK

On 20 March 2024, the Legal and Licensing Department of the Bank of Lithuania organised a consultative event on the topic "Current Licensing News".

During the consultative event, the latest developments in the licensing of financial market participants were presented, best practices and recommendations were shared.

Agenda of the event:

- A reminder of the licensing process.
- The latest statistics on licensing processes.
- Developments in legislation.
- Preparation for MiCA licensing.
- Necessary conditions for a smooth licensing process.
- The most frequently occurring significant deficiencies in licensing processes with real examples.
- Other relevant information.

Key aspects of the event

1. Changes in legislation:
2. The most frequently occurring deficiencies in licensing processes:
 - Insufficient preparation
 - Weaknesses of managers
 - Weaknesses of Shareholders:
 - Weaknesses in internal control:

Decisions of the Financial Market Supervision Committee of the Bank of Lithuania



LINK

Sanctions - Nordstreet UAB

The Bank of Lithuania has carried out an inspection of UAB Nordstreet, the operator of a crowdfunding platform, and found violations of the legal acts regulating crowdfunding activities, for which it has imposed sanction. After assessing that the company acknowledged the identified violation and took measures to eliminate it so that it would not be repeated in the future, the Bank of Lithuania imposed UAB Nordstreet 16 000 Eur fine.

REMINDER REGARDING REPORTING

Due to the end of the first quarter, the following reports shall be submitted to the Bank of Lithuania:

- financial and activity reports for supervisory purposes;
- reports for supervision of the implementation of money laundering and/or terrorist financing prevention measures;
- statistical Payment data.

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



Our recommendations and details are in this file

info@proventuslaw.it





Italian Data Protection Authority fines Medtronic Italia EUR 300,000



[LINK](#)

The violation: on March 7, 2024, the Italian Data Protection Authority (Garante) announced issuing two fines totaling EUR 300,000 to a medical device company. The first fine resulted from the company's use of CC instead of BCC in emails, exposing hundreds of recipients, including diabetes patients, to personal data disclosure. Due to the sensitive nature of health data, this violation was deemed severe. The second fine was imposed for incomplete information provided to patients, emphasizing that lack of transparency and cooperation, even after a violation, can exacerbate consequences.

Italian Data Protection Authority fines Enel Energia S.p.A over 79 million euros



[LINK](#)

The violation: the Italian Data Protection Authority, on the 29 February 2024 announced that it has fined Enel Energia over 79 million euros for "serious shortcomings in the processing of the personal data of numerous electricity and gas supply customers, as carried out for telemarketing purposes". According to DPA, the controller obtained 978 contracts from four companies not affiliated with the energy company's sales network. Enel Energia failed to implement necessary measures to prevent unauthorized agents from engaging in illicit activities, including nuisance calls, service promotions, and signing contracts without real economic benefits for customers. Due to the grave violations, involving the activation of at least 9,300 contracts, the Authority imposed a record fine of EUR 79,107,101 on Enel Energia.

EDPS finds that European Commission's use of Microsoft 365 infringes data protection law



[LINK](#)

The news: following an investigation, the EDPS has found that the European Commission's use of Microsoft 365 violated data protection requirements. Several notable violations were found including those related to the unauthorized disclosure of personal data due to the use of Microsoft 365, unlawful data transfers outside the EU/EEA, as well as those related to failure to limit the processing operations to the stated purposes of processing, such as failing to assess whether the purposes for processing are compatible with the purposes for which the data was initially collected. As a result of the investigation, the Commission, among other things, was ordered to suspend all data flows to Microsoft and its affiliates and sub-processors located outside the EEA and not covered by an adequacy decision, bring processing operations resulting from the use of Microsoft 365 into compliance, carry out a transfer mapping exercise identifying what personal data are transferred to which recipients in which third countries, and more.

European Parliament approves the Artificial Intelligence Act



[LINK](#)

The news: European Parliament approved the Artificial Intelligence Act on March 13 to balance AI advancements with regulation. The landmark legislation awaits finalization and will be effective 20 days after publication in the EU's Official Journal. The AI Act is currently undergoing linguistic approval, before being published in the EU's Official Journal.

Icelandic data protection authority fines Stjórnuna ehf EUR 10,000



[LINK](#)

The violation: the fine resulted from employee monitoring. Following a complaint, the DPA conducted an investigation and discovered that the data controller had installed video surveillance in a restaurant without legal basis or necessity. The DPA noted that the store manager took screenshots of the complainant from the surveillance cameras and recorded their activities without proper consent. Furthermore, employees were inadequately informed about the video surveillance.



info@proventuslaw.it

Detailed and full Regulatory Compliance update on PERSONAL DATA PROTECTION Regulation can be found here:

Our recommendations and details are in this file





EU, G7 indirect Russian diamond ban comes into effect



[LINK](#)

The 27-member EU agreed to ban non-industrial Russian diamonds in December last year when it passed its 12th package of sanctions on Russia in response to its invasion of Ukraine in 2022.

Article on: Lithuanian firms involved in schemes to circumvent Russia sanctions – intelligence



[LINK](#)

Lithuanian intelligence agencies have reported that some Lithuanian companies are aware that they are helping Russian entities to circumvent sanctions but continue to cooperate with them. Russian entities often involve Russian and Belarusian companies with a long-time presence in Lithuania in schemes to circumvent international sanctions.

Directive (EU) on the definition of criminal offences and penalties for the violation of EU restrictive measures and amending Directive (EU) 2018/1673



[LINK](#)

EU parliament has approved new rules to harmonize the enforcement of EU sanctions across EU Member states.

Council of the EU press release: Russia's war of aggression against Ukraine: EU individual sanctions over territorial integrity prolonged for a further six months



[LINK](#)

The Council has decided to extend for a further six months, until September 15, 2024, the restrictive measures targeting individuals responsible for undermining or threatening the territorial integrity, sovereignty, and independence of Ukraine.

Lithuanian Intelligence Agencies published the National Threat Assessment 2024



[LINK](#)

Lithuanian Intelligence Agencies published the National Threat Assessment for 2024.

Article: EU agrees to sanction 30 Russians over Alexei Navalny's death



[LINK](#)

Meeting in Brussels, European Union foreign ministers decided to impose new sanctions on some 30 Russian officials in response to the death of political opponent Alexei Navalny. The decision follows Navalny's death in February in a Russian prison, which the EU blames on Vladimir Putin and his inner circle.

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.it



BoL newsfeed

The Bank of Lithuania provided statistics of 2023 on examined consumer disputes.



[LINK](#)

The Bank of Lithuania examined almost 740 disputes last year, a fifth more than in 2022. A record number of disputes was made up of disputes between consumers and banks due to money defrauded by fraudsters, disputes with insurers increased, and disputes with other financial market participants decreased.

Our recommendation:

It is recommended enhancing fraud prevention measures through robust authentication processes and advanced detection technologies. In addition, educating customers about common fraud schemes to empower them to recognize and report suspicious activity. Financial institutions should strengthen transaction monitoring systems to detect and prevent unauthorized transactions in real-time and fostering collaboration with regulatory authorities.

EP newsfeed



[LINK](#)

The European Parliament has approved a directive to establish a system of prior verification of environmental marketing claims to protect consumers from misleading advertising.

The directive would require companies to provide evidence of their environmental claims before promoting products as environmentally friendly.

It provides for 30-day verification deadlines, with simplified procedures for less complex products, and would exempt micro-enterprises, while SMEs would be given an additional period to comply.

Our recommendation:

We highly recommend that you remain vigilant to future legislative developments in order to adapt quickly and maintain your regulatory compliance.

EC newsfeed



[LINK](#)

The European Commission recently unveiled its annual report on Safety Gate, the EU's rapid alert system for dangerous non-food products, covering events in 2023. Cosmetics were most frequently reported as posing health risks, making 2023 the year with the highest number of alerts since the system was launched in 2003, underlining its growing effectiveness and crucial importance.

In 2023, authorities in the 30 participating countries issued 3,412 alerts and took 4,287 follow-up actions. Each member state responded proactively to alerts, exchanging information to ensure consumer safety. Cosmetics were the most frequently reported products, followed by toys, motor vehicles, electrical appliances and clothing. Alerts mainly concerned chemical, injury, choking and environmental hazards.

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.it



The Supreme Administrative Court of Lithuania

[LINK](#)

The Supreme Administrative Court of Lithuania (SACC), in its ruling of 20 March 2024, recognised that the State Labour Inspectorate was justified in fining The company EUR 4 340 for infringement of the Law on Employment by failing to ensure, in the presence of the elements of an employment contract, that the employees (the four female dancers and the person who distributed the promotional leaflets for the nightclub) were working in the way laid down by the law, by notifying the territorial office of the State Social Insurance Fund Board (SSSIFB) of the recruitment of the persons concerned, and by signing the contracts.

SACC identified 3 criteria to distinguish between employment and civil contract:

1. Under employment contract the employee is obliged to the employer to perform a job function. The employee undertakes to perform a job function defined in terms of types not to perform a specific task or to achieve a specific result. Thus, the relationship resulting from an employment contract is characterised by continuity. On the opposite, under civil (e.g. service) contract the contractor undertakes to complete specific task, achieve result etc.
2. Employment relationships are generally characterised by the periodicity and continuity of payment of wages, which means that the payment of wages is usually linked to a certain period of time (e.g. monthly, weekly, etc.). In the case of a specific task under a civil contract, payment is usually made upon satisfactory completion of the contract and acceptance of the final result of the work.
3. The third feature of an employment contract is the subordination of the employee to the employer in the performance of the job function. This feature distinguishes the employment relationship from other similar relationships, in particular those based on civil contracts, in which there is an obligation to perform work in return for remuneration, but this is done independently, without the right of the other party to regulate the process of performing the work on its own.
The subordination inherent in the employment relationship means that the performance of the functions of the job is inseparable from the employer's control and the execution of his lawful instructions: in this case, it is not sufficient to have a certain subordination between the parties, which is the result of the specific nature of the activity carried out, or to have a fixed payment for the results of the activity, as payment for the performance of the work is not unique to the employment relationship, nor is it abnormal for the establishment of a relationship governed by a civil contract.

Our recommendation:

It is worth assessing your contracts with service providers for signs of an employment contract.

ESMA – third draft consultation paper of MiCAR



LINK

This consultation package covers one draft RTS and three draft guidelines on: (i) arrangements, systems and procedures for detecting and reporting suspected market abuse (RTS); (ii) suitability requirements applicable to the provision of advice on crypto-assets and portfolio management of crypto-assets and the format of the periodic statement referred to in Article 81(14) of MiCA (guidelines); (iii) the procedures and policies, including the rights of clients, in the context of transfer services of crypto-assets (guidelines); and (iv) maintenance of systems and security access protocols in conformity with appropriate Union standards (guidelines).

Our recommendation:

Acquaint yourself with the latest draft consultation paper in relation to certain regulatory technical standards of MiCAR. The regulatory technical standards provide guidance on the methods of how certain services should be provided in compliance with MiCAR. Therefore, it is essential to make room for the incorporation of those requirements if they are applicable to the envisaged services.

ESMA – 1st draft technical standards on MiCA CASP requirements



LINK

The draft technical standards cover a range of hot topics for crypto-asset service providers that have not been detailed by MiCAR including:

- notifications by certain financial institutions to provide CASP services;
- required documents in CASP authorization application;
- complaints handling procedures;
- CASP qualifying holding acquisition;
- ESMA's approach on the extent of information that should be included in the RTS and ITS in regard to the application's documentation;
- Clear draft technical standards on the extent of the information that should be provided by applicant CASPs during the licensing process and standard forms that should be submitted to the local competent authorities.

In general, with these technical standards ESMA is seeking to eliminate any possibility of jurisdictional arbitrage in relation to MiCAR's implementation by detailing what specific information needs to be provided by each applicant (non-/ financial institution) for each of the generally "high-level" requirements that may be ambiguous so that the application process is clear across the EU and that the local regulators would not implement extensively restrictive measures to curb the number of applicants.

Our recommendation:

For all companies that seek to provide crypto-asset services (CASP), it is crucial to get acquainted with these draft technical standards. This is because they not only explain the rationale of ESMA's harmonization efforts with MiCAR, but also provide a clear picture of the requirements that the local regulators together with the applicants will be subject to.

EBA – draft RTS on complaints handling



LINK

The European Banking Authority (EBA) published the final draft Regulatory Technical Standards (RTS) that set out the requirements, templates and procedures for handling complaints received by issuers of asset referenced tokens (ARTs). The draft RTS set out requirements related to the complaints management policy and function, the provision of information to holders of ARTs and other interested parties, templates, recordings, languages, the procedure to investigate complaints and to communicate the outcome of the investigations to complainants, and specific provisions for complaints handling involving third-party entities.

EBA – draft RTS on redemption plans for ART and EMT issuers



LINK

The European Banking Authority (EBA) launched a consultation on the Guidelines for the plans to orderly redeem asset-referenced or e-money tokens in the event that the issuer fails to fulfil its obligations under the Markets in Crypto assets Regulation (MiCAR). The Guidelines specify the content of the redemption plan, the timeframe for review and the triggers for its implementation. The Guidelines are addressed to issuers of asset-referenced tokens (ART) and of e-money tokens (EMT), and to competent authorities under MiCAR. The consultation run until 10 June 2024.

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



Our recommendations and details are in this file

info@proventuslaw.it