REGULATORY COMPLIANCE UPDATE

ECOVIS ProventusLaw

EU WHISTLEBLOWING DIRECTIVE

Whistleblowing Directive Implementation

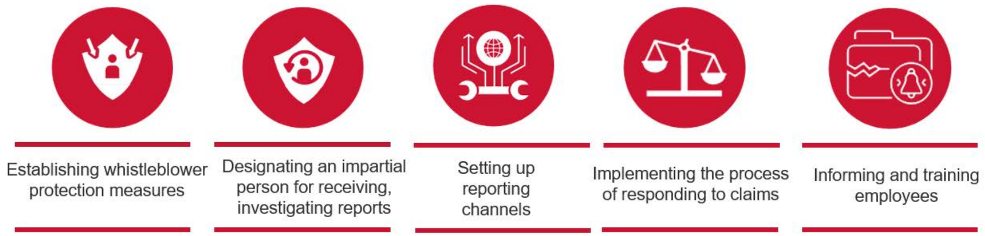
LINK

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.

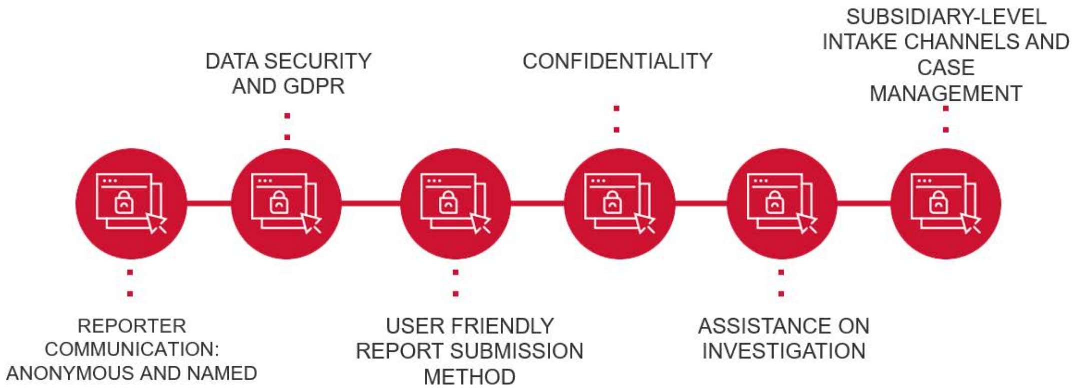
Under the EU Whistleblower Directive, organisations must establish secure and confidential reporting channels for whistleblowers. The reporting process is designed to ensure the protection of whistleblowers and the effective handling of reports of wrongdoing.



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

04.2024

ECOVIS ProventusLaw

Decisions of the Board of the Bank of Lithuania

LINK

The Board of the Bank of Lithuania, having assessed the results of the inspection of UAB NEOCARD, revoked the licence of UAB NEOCARD as an electronic money institution for significant, repeated, systematic and long-lasting breaches of legal acts. The institution can no longer provide any financial services and is obliged to return the funds to its customers.

- During the period under review, NEOCARD UAB did not ensure effective internal controls to prevent money laundering and terrorist financing.
- The institution had not established adequate internal control procedures for the identification and verification of the identity of the client and beneficiary.
- The institution did not adequately analyse alerts generated by the monitoring system and did not carry out investigations into suspicious customer transactions or did so in a formal manner.
- The institution's internal policies and internal control procedures regarding the implementation of international sanctions and restrictive measures were also significantly weak.
- It was found that the institution obstructed the Bank of Lithuania's inspection by submitting fraudulently corrected documents, selected for the inspection, related to the identification of customers.

Update of the list of criteria for identifying possible money laundering and suspicious monetary transactions

LINK

The Financial Crimes Investigation Service (FCIS) has updated the list of criteria for identifying potential money laundering and suspicious monetary transactions FICIS has updated the list of criteria for identifying potential money laundering and suspicious monetary transactions (the List of Criteria), which is intended for financial institutions and other obliged entities implementing anti-money laundering (AML) measures, and will come into force from 1 May 2024.

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

LINK

The Bank of Lithuania has conducted an inspection of the electronic money institution UAB Guru Pay and imposed sanctions. During the inspection, weaknesses were identified in the area of prevention of money laundering and terrorist financing, such as the allocation of functions and the management of conflicts of interest. In addition, the institution's procedures did not always ensure that the identification of customer representatives, the nature of the customer's activities and the assessment of the risks posed by customers were properly identified. The institution's information security monitoring system was also deficient.

Fraud prevention guidelines by the Bank of Lithuania

LINK

The Bank of Lithuania (BoL) has approved the Fraud Prevention Guidelines for Financial Market Participants Providing Payment Services, which will enter into force on 1 May 2024. The aim of the Guidelines is to encourage financial market participants to improve the management of financial fraud risk and to increase the effectiveness of the prevention measures in place.

Payment service providers need to be vigilant about fraud risks related to the customer data they hold and have clearly described processes that are proportionate, accurate, relevant and relevant to the day-to-day provision of payment services.

Amendments to the Republic of Lithuania Law on Prevention of Money Laundering and Terrorist Financing

LINK

Taking into account both the risks posed by the cryptocurrency industry in general and the concerns of their supervisory authority, the Financial Crimes Investigation Service (hereinafter referred to as the " FCIS"), about the negligent attitude of many cryptocurrency companies towards the compliance with the currently established requirements, it has been decided to tighten the requirements for these companies. Stricter requirements for these entities, additional powers for their supervisors and a number of other additional amendments to the Republic of Lithuania law on the prevention of money laundering and terrorist financing, including editorial changes and clarifications, were adopted on 18 April 2024. Law No. XIV-2543 (hereinafter referred to as the "Law on Amendments") was approved by the Parliament of the Republic of Lithuania on the Prevention of Money Laundering and the Financing of Terrorism.

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

ECOVIS ProventusLaw

EMI, PI REGULATION

04.2024

Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro

LINK LINK

On 9 April 2024, the Instant Payments Regulation, approved by the European Union authorities, will come into force and will enable instant payments to take over across Europe. The Instant Payment service allows transfers within 10 seconds on any day of the year, including weekends and public holidays, at any time of the day. The new regulation will ensure that the service is available in all EU countries.

Credit institutions across the EU will be required to provide instant euro payments from 2025 autumn, giving residents and businesses in Lithuania and the rest of the EU more opportunities to transfer funds across borders in seconds, any time of day. Credit institutions and other payment service providers will also have to be prepared to check whether the account specified by the payer belongs to the payee to whom the funds are to be transferred.

The requirement to provide an instant payment service applies first to:

- Credit institutions. Institutions that provide a credit transfer service in euro will have to provide their customers with the possibility to receive instant payments from January 2025 and to initiate instant payments from October 2025.
- Electronic money and payment institutions have a longer lead time, having to provide the service from April 2027.

Another important change is the Regulation's requirement for payment service providers to verify that the account of the recipient referred to in the payment order is held by the person named in the order. Thus, payment service providers will have to:

- check whether the recipient's account number and the name of the recipient match.
- inform the payer, prior to payment confirmation/authorisation, whether the name of the recipient indicated is the same, close to the same or different.
- inform the payer of the name discrepancy but will not be able to reject the authorised payment. It will also have to inform the payer of the possible consequences if the payment is confirmed. The final decision on whether to approve a payment lies with the payer.

This service will have to be provided free of charge to customers for normal transfers and instant payments in euro. Payment service providers have until October 2025 to be ready to offer this service.

Q&A by the Bank of Lithuania

LINK

The Bank of Lithuania has updated its Frequently Asked Questions section with the following question:

Can a Compliance Officer be appointed as a member of the Supervisory Board of an institution if conflicts of interest are identified and managed in the institution? If the Compliance Officer is appointed as a member of the Supervisory Board, should the Compliance Officer continue to be directly accountable to the Management Board of the Institution as provided for in point 9.5 of the Description of the Requirements for the Management System of Electronic Money Institutions and Paying Institutions and for the Safeguarding of the Funds Received, without any delegation of accountability to the Supervisory Board, while acting as Compliance Officer?

In the view of the Bank of Lithuania, the appointment of the Compliance Officer as a member of the supervisory body - the Supervisory Board - would create a potential and permanent conflict of interest.

REMINDER REGARDING REPORTING

Please be aware of the upcoming deadlines for reporting to the State Tax Inspectorate – by 1st of June to submit the reports in terms of:

- accounts where the total annual turnover of all accounts held by the same person with the same financial market participant is at least EUR 15,000;
- the debt obligations owed to a financial market participant as at 31 December of the calendar year;
- balance of accounts at the end of the year, if the total annual balance of accounts of the same person with the same financial market participant at the end of the year is not less than EUR 5,000.

Please note that contributions of supervised financial market participants to the bank of Lithuania for the current year shall be paid by 31st of May.

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

ECOVIS ProventusLaw

PERSONAL DATA PROTECTION REGULATION 04.2024

Croatian Data Protection Authority fines a betting company EUR 20,000 for insufficient legal basis for data processing

LINK

The violation: the controller, operating in the field of gambling and betting sector, has received a fine of EUR 20,000 for cookie related violations.
According to the supervisory authority, the data controller failed to offer data subjects the option to give or withdraw consent in an informed and voluntary manner. In cases involving different categories of cookies, such as marketing and analytical cookies, the consent mechanism, like the cookie banner, must be clearly distinguishable, easily accessible, and use language that is clear and simple to understand. However, the betting company not only neglected to differentiate between cookie categories in the banner but also deposited cookies before obtaining consent.

Moreover, deficiencies were found in terms of fulfilling information obligations. The controller's privacy policy lacked details about the legal basis for processing, the types of cookies used, their purposes, and the duration of storage.

Recommendations for organizations' legal departments:

- review how consent for the use of cookies is obtained, whether it is valid and if it is available before any cookies are deposited;
- ensure that your privacy or cookie policy includes sufficient information about the use of cookies or other similar technologies.

Court of Justice of the European Union publishes Advocate General's Opinion concerning health data

LINK

The news: the Court of Justice of the European Union (CJEU) has released the opinion of the Advocate General (GA) regarding the interpretation of GDPR provisions concerning remedies and 'data concerning health'. Specifically, the opinion examines whether data entered by a customer on an online sales platform, such as Amazon, to purchase non-prescription medication qualifies as processing of 'data concerning health'.
The opinion notes that while other purchases may also hint at special categories of data (e.g., ordering a specific garment suggesting religious beliefs, or a political book indicating political affiliations), such indications are speculative, at least in this context. The Advocate General stresses that any information suggesting the health status of the data subject should be based on a certain degree of certainty rather than speculation.

The State Data Protection Inspectorate issued a Recommendation on records of processing activities and updated the forms of records of processing activities for data controllers and data processors

LINK

The news: the Lithuanian data protection authority (VDAI) has released guidance on Records of Processing Activities (ROPA), along with accompanying formats, accessible to both data controllers and processors.

Spanish Data Protection Authority fines CAIXABANK, S.A EUR 1,200,000 for insufficient legal basis for data processing

LINK

The violation: following an investigation prompted by a complaint, the supervisory authority concluded that the data controller, a company operating in the financial sector, shared forms soliciting personal data from data subjects.

Within these forms, data subjects were asked to consent to the transfer of their personal data to the General Treasury of Social Security but were not provided with an option to refuse such transfer.

info@proventuslaw.lt

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

ECOVIS ProventusLaw

FINANCIAL AND ECONOMIC SANCTIONS 04.2024

OFAC sanctions 13 entities for aiding Russian sanctions evasion via crypto

LINK

On 25 March 2024, the US Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned 13 entities and two individuals for the development and operation of blockchain-based services which aimed to evade sanctions, including BitPapa and NetExchange.

It was stated by OFAC that many of the individuals and entities facilitated transactions or offered other services that helped OFAC-designated entities evade sanctions. Russia is increasingly turning to alternative payment mechanisms to circumvent U.S. sanctions and continue to fund its war against Ukraine.

Council gives final approval to the introduction of criminal offences and penalties for breaches of EU sanctions

LINK

The EU Council has given its final approval to the introduction of criminal sanctions for violations of EU sanctions. This means that certain actions, such as circumventing travel bans or trading in sanctioned goods, will be considered criminal offenses in all member states. Sanctions must be effective and proportionate, with penalties that can include fines and imprisonment for intentional violations.

Member states must ensure that violating EU sanctions is punishable by effective and proportionate criminal penalties, which vary depending on the offence. However, intentional violation of sanctions must give rise to a prison sentence as the maximum penalty. Those who have violated EU restrictive measures may additionally be subject to fines.

Extremist settlers in the occupied West Bank and East Jerusalem

LINK

The Council on 2024-04-19 decided to list four persons and two entities under the EU Global Human Rights Sanctions Regime. The listed individuals and entities are responsible for serious human rights abuses against Palestinians, including torture and other cruel, inhuman or degrading treatment or punishment and for the violation of right to property and to private and family life of Palestinians in the West Bank.

The listed entities are Lehava, a radical right-wing Jewish supremacist group, and Hilltop Youth, a radical youth group consisting of members known for violent acts against Palestinians and their villages in the West Bank.

New reporting requirements for legal persons and the financial sector approved

LINK

The European Union has introduced new reporting requirements through the new Article 5r of Regulation 833/2014, for legal persons and entities with substantial connections to Russia. Article 5r forms part of the EU's 12th package of sanctions (2023, December 18) measures on Russia. The new requirement will provide national competent authorities with more information on the flow of funds from the European Union to entities related to Russia, will allow them to better assess whether certain types of transfers pose a risk of violating Russia-related sanctions and will help them to identify the sources of Russian revenue.

Lithuanian parliament extends national sanctions on Russians, Belarusians for a year

LINK

Lithuania has extended its national sanctions on Russian and Belarusian citizens for another year. Little additional measures have been added, despite proposals such as limiting how often Russian and Belarusian residents could visit home and taking away their residence permits if they express support for Putin. The law adopted last year-imposed restrictions on Russians and Belarusians to obtain Lithuanian visas and e-resident status. Russian citizens also face additional restrictions on entry to Lithuania and acquisition of real estate in the country. Lithuania also temporarily refuses to accept their residence permit applications.

The updated law on national sanctions will be in force until May 2, 2025.

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

04.2024

ECOVIS ProventusLaw

BoL newsfeed

LINK

The Bank of Lithuania examined 55 electronic money and payment institutions' agreements (Terms and Conditions) regarding payment services and found that they only partially comply with the requirements of the Law on Payments.
The most non-compliant contractual provisions were found in relation:

- to the liability of institutions for unauthorized payment transactions.
- shorter deadlines for the payer to report an unauthorized, improperly initiated or executed payment transaction than those laid down in the Law on Payments.
- unjustifiably partially shift responsibility for unauthorized or improperly authorized payment transactions to consumers.
- only a general provision on the liability of the institution for the fulfilment of its obligations or for the reimbursement of direct losses, without distinguishing that the institution is responsible for the proper initiation or execution of the payment transaction as set out in the Law on Payments.
- terms for amendment and termination of the contract which do not comply with the Law on Payments.

Our recommendation:

Recommendation to ensure that contracts with customers regarding payment services are regularly reviewed and updated to comply with the requirements of the Law on Payments.

Parliament adopts "Right to Repair" Directive

LINK

Parliament has adopted the "Right to Repair" directive for consumers, aimed at strengthening manufacturers' obligations to repair goods and encouraging consumers to extend the life of products through repair, in order to reduce waste and support the repair sector.

The new rules require manufacturers to provide fast, cost-effective repair services, offering consumers a one-year extension to the legal warranty for products repaired under warranty. In addition, a European information form could be introduced to facilitate the assessment and comparison of repair services, while a European online platform would be launched to support community repair initiatives.

Cypriot official calls for EU consumer protection regulation amendment

LINK

At an informal meeting of EU consumer protection ministers in Brussels, the Permanent Secretary of the Cypriot Ministry of Energy, Trade and Industry stressed the need to amend EU regulations to better meet the growing needs of consumers and guarantee their protection.

Discussions focused on the implementation of internal market rules and the challenges linked to the digital transition, such as artificial intelligence, e-commerce and the role of influencers on social networks in promoting products. He stressed the importance of a fair and efficient internal market for economic prosperity and sustainable development, underlining the need for close cooperation between all stakeholders.

info@proventuslaw.lt

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

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

04.2024

ECOVIS ProventusLaw

4th April 2024, the Supreme Court of Lithuania ruling in the case No. e3K-3-11-421/2024

LINK

The Supreme Court of Lithuania (LAT) provided a legal interpretation rule in the case No e3K-3-11-421/2024 dated 4 April 2024 regarding the liability of the employer, employer's manager and the company that externally performed occupational health and safety (hereinafter OSH) functions in the event of an accident in the company:

- Assignment of OSH functions to persons appointed by the employer, OSH specialist (internal or external) does not release the employer from responsibility in the field of OSH;

- this principle is absolute and imperative in relation to the employer's obligation to employee but does not in any way affect and does not remove the responsibility of the natural or legal persons performing the functions of the occupational safety and health service for the benefit of the employer in scope of contractual obligations. This means that such persons are responsible to the employer according to contractual obligations.

Our recommendation:

- review contracts with external suppliers providing OSH services, assessing which functions they have taken over and which functions remain the manager's responsibility.

- implement appropriate control measures for OSH functions provided by external companies.

17th April 2024 the Supreme Court of Lithuania ruling in the case No 2K-34-1073/2024

LINK

The Supreme Court of Lithuania was under consideration the case regarding the criminal liability for the disclosure of a commercial secret established in Article 211 of the Criminal Code was considered. Criminal liability arises for a person who discloses information considered a commercial secret, which was entrusted to him or which he learned due to his work, if this act causes significant material damage to the victim.

In this case, the court ruled on the following rules:

- If the confidentiality agreement with the employees does not specify a period for how long after the termination of the employment relationship the employee must protect commercial secrets, the 1-year period provided by the law applies.

- Significant material damage in the context of this article is calculated according to the net profit criteria, whereby the net profit is the portion of the received gross income remaining after deducting the financial costs of operation, special losses, and paid taxes.

Our recommendation:

It is recommended to review the confidentiality agreements, namely:

- the period of the obligation to protect commercial secrets;
- penalty for breach of confidentiality.

ESMA Trends, Risks, Vulnerabilities analysis report on crypto-assets: market structures and EU relevance

LINK

Over the last decade, crypto assets have developed into an extensive system and gained considerable attention, especially due to the risks they pose to consumers and financial stability. ESMA monitors these risks and has repeatedly issued warnings to investors.

The article aims to improve specifically the understanding of crypto-asset trading and the extent to which it resembles or differs from traditional financial markets. It also identifies current and potential areas of risk, not only to consumers but also to market order and financial stability. Finally, the analysis informs and supports the implementation of the EU Markets in Crypto-Assets (MiCA) regulation.

In particular the report provides a comprehensive and well-documented general overview of the crypto asset market such as trading, on-/off- ramping, in-between-the-lines debate on decentralization / globality and effective concentration of the assets i.e. that even though the foundations of crypto-assets stem from the demand on decentralization, market activity reveals that the top 3 crypto-assets account for ~74% of the total crypto market capitalization, while one of them is a Tether’s USDT stablecoin.

Our recommendation:

The report provides a high-level overview of the crypto-asset market and the overall consumer and regulator stance on the industry.

It’s important to familiarize with the findings of the report in order to understand the general view on crypto-assets and their use particularities.