REGULATORY COMPLIANCE UPDATE

AML/CTF REGULATION

01.2024

ECOVIS ProventusLaw

Corruption Perception Index

LINK

The 2023 Corruption Perceptions Index reveals a global prevalence of corruption, with over two-thirds of 180 countries scoring below 50 out of 100 (0 is highly corrupt, 100 is very clean), indicating serious corruption issues. The global average is 43, and the majority of countries have shown no improvement or have declined in the past decade. Furthermore, 23 countries reached their lowest scores this year.

FAQ of Financial Crime Investigation Service

LINK

The Financial Crime Investigation Service has begun posting frequently asked questions in its website.

In 2023 the Activity of Financial Fraudsters Grew by a Third, Using the Pandemic Habits of Consumers

LINK

Data from the Centre of Excellence for Money Laundering Prevention shows that financial fraud was on the rise in 2023, with financial institutions recording more than 10,000 fraud cases per year, 33% more than in 2022. Compared to 2022, the amount defrauded by fraudsters increased by 3.9% to EUR 12.3 million last year, but financial institutions managed to recover almost EUR 900,000 of this amount, resulting in real losses of EUR 11.4 million.

Guidelines Published by the EBA for Crypto-Asset Service Providers Concerning Their Management of Exposure to Money Laundering and Terrorist Financing Risks.

LINK

The European Banking Authority has extended its guidelines on money laundering and terrorist financing risk factors to crypto-asset service providers. CASPs are required to implement preventive measures, as the risk of misuse can be significant, not only because of the speed of crypto asset transfers, but also because some products contain features that conceal the user's identity. These new guidelines will apply from December 30, 2024.

Regulation (EU) 2024/163 of 12 December 2023 amending Delegated Regulation (EU) 2016/1675 as regards the deletion of the Cayman Islands and Jordan from the table in point I of the Annex

LINK

The European Commission has updated its list of high-risk third countries. As of 7 February 2024, the Cayman Islands and Jordan will no longer be a part of the list of high-risk third countries.

Anti-Money Laundering: Council and Parliament Strike Deal on Stricter Rules

LINK

The Council and Parliament have reached a provisional agreement on the AML Regulation and the sixth AML Directive. This provisional agreement will make it possible for the first time to harmonize the rules exhaustively throughout the EU.

EBA Consultation on Guidelines on Preventing the Misuse of Money Transfers and Certain Crypto-Assets for Anti-money Laundering and Combating the Financing of Terrorism (Guidelines on Travel Rules)

LINK

The European Banking Authority has launched a public consultation on new guidelines to prevent the misuse of money transfers and certain crypto assets for money laundering and terrorist financing purposes.

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

01.2024

Publication by the Bank of Lithuania

LINK

The European Supervisory Authorities (ESAs) are publishing public consultations on the measures contained in the second package of Digital Operational Resilience Act (DORA) documents. The overall aim of this is to raise supervisory awareness of the cyber risks and information and communication technology (ICT) incidents that financial institutions may face. The package consists of four sets of draft Regulatory Technical Standards (RTS), one set of draft Implementing Technical Standards (ITS) and two sets of guidelines. Please note that the deadline for the submission for comments is 4 March 2024. All contributions received will be published following the end of the consultation, unless requested otherwise.

Publication of final draft technical standards for the Digital Operational Resilience Act (DORA).

LINK

The three European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) published the first set of final draft technical standards under the DORA, which is aimed at enhancing the digital operational resilience of the EU financial sector by strengthening financial entities' Information and Communication Technology (ICT) and third-party risk management and incident reporting frameworks.

The final general drafts of the technical standards comprise four sets of technical standards:

1. Regulatory Technical Standard (RTS) on ICT risk management.
2. RTS on incident classification.
3. RTS defining policy content for contracts related to ICT services supporting essential or critical functions.
4. Technical Implementing Standard (ITS) on the register of information relating to contractual arrangements for the use of services provided by ICT service providers. This standard establishes templates for a register of information covering ICT service providers at individual, consolidated and sub-consolidated levels.

Bank of Lithuania's inspection plan

LINK

The Bank of Lithuania has published this year's financial market participants inspection plan which targets 34 financial institutions. The inspections will mainly focus on:

- anti-money laundering and counter terrorist financing;
- information and communication technology (ICT) and cybersecurity risk management;
- prudential requirements.

In addition to the areas mentioned, the Bank of Lithuania will carry out inspections of credit risk management, implementation of international sanctions, provision of investment services, offering of investment products and compliance with internal control requirements.

According to this year's inspection plan, the Bank of Lithuania experts intend to carry out inspections of the following financial market participants:

- 17 electronic money and payment institutions;
- 5 insurance companies;
- 4 banks;
- 3 independent mortgage brokers;
- 2 issuers;
- 1 credit union;
- 1 financial brokerage company;
- 1 management company.

REMINDER ON REPORTING

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

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

info@proventuslaw.lt

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 REGULATION 01.2024

ECOVIS ProventusLaw

French Data Protection authority fined Amazon France Logistique EUR 32,000,000 for monitoring of employees.

LINK

According to the data protection authority, the company issued scanners to employees for performance documentation. These scanners included indicators for idle time, stow machine gun, and latency under ten minutes, signalling interruptions, downtime of ten minutes or more, and errors during rapid item scanning. This was deemed a breach of the data minimization principle. The DPA also highlighted failures in transparency obligations and personal data security by the data controller. Notably, the CNIL ruled setting up a system measuring work interruptions with such precision was illegal. This system potentially required employees to justify every break, deemed excessive for retaining all data and statistical indicators for all employees and temporary workers for 31 days.

Dutch Supervisory Authority for Data Protection fined International Card Services B.V. EUR 150,000 for failure to carry out a Data Protection Impact Assessment.

LINK

The violation: data controller operating in the financial services sector initiated remote customer identification in the Netherlands in 2019. Since then, they have conducted identity checks on approximately 1.5 million individuals. According to the data protection authority, the company, in addition to collecting customers' names, addresses, telephone numbers, and emails, also requested customers to submit facial pictures, which were subsequently compared with their photo IDs. The authority emphasizes that while financial institutions are obligated to perform identity checks, they must also handle this data with extreme care, making a Data Protection Impact Assessment (DPIA) potentially mandatory. Before commencing large-scale processing, the data controller was required to conduct a DPIA but failed to do so. As a result, a fine of EUR 150,000 was issued.

EDPB adopted a report on the findings regarding the role of Data Protection Officer.

LINK

The news: in 2023, 25 data protection authorities across the European Economic Area launched coordinated action to investigate compliance regarding the role of Data Protection Officers (hereinafter - DPOs). The report highlights key findings, most notably the most common mistakes, such as:

- Not appointing a DPO in cases where this is mandatory.
- Not allocating sufficient resources to the DPOs.
- Insufficient DPO knowledge or inadequate training.
- Not entrusting DPOs with tasks required under the GDPR or failing to assign key roles to them.
- Insufficient involvement.
- Conflicts of interest.
- Lack of independence.
- Lack of reporting by the DPOs to the organizations' highest management level.

Recommendations for legal department of organisations:

If your organisation has a DPO or is required to have a DPO, review whether this role is implemented appropriately. If unsure whether a DPO is needed, or if their role is implemented as is required, consider consulting with data protection experts.

State Data Protection Inspectorate released an overview of personal data security breaches in 2023.

LINK

According to data published by the State Data Protection Inspectorate (VDAI), there were 254 notifications regarding personal data security breaches, impacting over half a million data subjects. These numbers reflect a decrease compared to 2022. The data reveals that human error remains the primary cause of reported breaches to VDAI. However, cyber incidents, constituting only 15% of all reported breaches in 2023, affected 49% of all data subjects impacted, indicating their heightened significance. The predominant type of breach continues to be a breach of confidentiality, accounting for 76% of all reported breaches. Human error caused 72% of all breaches.

EDPB publishes OSS case digest on security of processing and data breach notification.

LINK

The news: the casebook published by EDPB offers valuable insight into how data protection authorities have interpreted and applied the GDPR's provisions in various scenarios, such as hacking, ransomware or accidental data disclosure, personal data breaches caused by human error, insufficient company practices, etc. With the inclusion of practical examples, this document can be used by data controllers to review their own practices and improve their procedures for personal data breaches.

info@proventuslaw.lt

Detailed and full Regulatory Compliance report on PERSONAL DATA PROTECTION REGULATION can be found here:

Our recommendations and details are in this file

REGULATORY COMPLIANCE UPDATE

FINANCIAL AND ECONOMIC SANCTIONS 01.2024

ECOVIS ProventusLaw

The Bank of Lithuania Reminds: Russian Citizens Cannot Participate in the Management of Crypto-Property Companies

LINK

The Financial Crimes Investigation Service points out that one of the restrictions in the European Union's (EU) 12th sanctions package comes into force on January 18, 2024. This restriction prohibits Russian citizens or natural persons living in Russia from acting, controlling or holding, directly or indirectly, any position in a legal person, entity or organization established or registered under the law of a Member State and providing crypto-currency wallet, account management or storage services, or in management bodies.

Guatemala: Council establishes dedicated framework of restrictive measures in support of democracy

LINK

On 12 January 2024, the Council established a special restrictive measures regime to support democracy and a peaceful and orderly transition of power in Guatemala.

Council establishes specific sanctions framework and lists six individuals linked to Hamas and Palestinian Islamic Jihad

LINK

On 19 January 2024, The Council established a specific framework of restrictive measures that will enable the European Union to hold accountable any person or entity that supports, facilitates, or enables violent actions by Hamas and Palestinian Islamic Jihad (PIJ). This new framework will apply until January 19, 2025.

Commission publishes new Guidelines for the annual report on dual use export controls

LINK

On 17 January 2024, the Commission published new Guidelines in view of the preparation of its annual report on dual-use export controls. The goal is to increase transparency through more information sharing on Member States' licensing decisions in the area of export controls.

Support to Dutch action against violation of export sanctions to Russia: three arrests

LINK

Eurojust and Europol collaborated with Dutch, German, Latvian, Lithuanian, and Canadian authorities to conduct a coordinated action against the alleged violation of export sanctions to Russia. This joint effort resulted in the arrest of three suspects and the search of 14 locations, as part of an investigation into the illegal export of technological and laboratory equipment with potential military applications. These exports were in violation of EU-wide sanctions imposed after the outbreak of the war in Ukraine.

Council adds person and entity to EU sanctions list concerning Russia's war of aggression against Ukraine

LINK

The Council introduced additional restrictive measures against PJSC Alrosa (the world's largest diamond mining company) and its CEO Pavel Alekseevich Marinychev, responsible for actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine.

Regional Approach to Ensure Uniform Customs Controls And Information Exchange for Implementation of the EU Restrictive Measures

LINK

The heads of Lithuanian, Latvian, and Estonian customs authorities reached an agreement to implement consistent regional customs controls, aiming to create hurdles for Russia's war efforts in finding avenues to evade EU sanctions.

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

01.2024

ECOVIS ProventusLaw

Draft Resolution of BoL

LINK

The Bank of Lithuania (BoL) prepared a project for amendments of the Rules for the Out-of-Court Procedure of Settlement of the Disputes between Consumers and Financial market participants (BoL resolution No. 03-23) (hereinafter – Project).

The Project was prepared in order to make the procedure for out-of-court settlement of disputes between consumers and financial market participants more effective at the Bank of Lithuania. For this purpose, the rules of the procedure for out-of-court settlement of disputes between consumers and financial market participants in the Bank of Lithuania added to the obligation of financial market participants in their branch, website, standard terms of contracts and in the response to a consumer claim, among other information, to provide a link to the Bank of Lithuania's electronic consumer dispute settlement system.

The Rules also stipulate that applications submitted electronically to the Bank of Lithuania must be signed with a qualified electronic signature or submitted through the Bank of Lithuania's electronic consumer dispute handling system.

Our recommendation:

A financial market participant should fully embrace and adhere to all proposed amendments set forth by BoL. Furthermore, we recommend to be active participation in the remark process initiated by BoL when a new project regarding possible amendments on legal acts or resolutions are issued.

BoL news feed

LINK

Cooperation agreement between the BoL and the State Consumer Rights Protection Service (SCRPS) was signed.

In order to ensure maximum effective protection of consumers' interests, the BoL and the SCRPS will cooperate by exchanging information and sharing experience, developing consumers' financial literacy.

The institutions agreed to actively exchange information and best practices regarding the handling of consumer complaints and disputes, other issues of protecting their rights, sharing knowledge about risk factors and international practice. It was also agreed to increase consumer education through joint initiatives related to financial solutions, products and services, rounding of cash payments.

Our recommendation:

It should be noted that the SCRPS is a regulatory Authority and out-of-court dispute resolution body regards most of consumer goods and services. Taking this into account, a company that offers these types of services should follow information from SCRPS.

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

EMPLOYMENT

01.2024

ECOVIS ProventusLaw

Information from the State Labour Inspectorate

LINK

It has been more than a year since the amendments to the Labour Code were put into effect, which prohibit violence and harassment at work, and require employers to take preventive measures. The State Labour Inspectorate (VDI) is reminding employers of their responsibilities in this regard.

As a reminder, violence and harassment is any unacceptable behaviour or threat thereof, regardless of whether it is intended to have a physical, psychological, sexual or economic impact on an individual either once or repeatedly, or whether it causes or threatens to cause such an effect, or whether it violates the dignity of a person or creates an intimidating, hostile, degrading or offensive environment, and/or has caused or threatens to cause physical, material and/or non-material damage.

Article 30 of the Labour Code specifies the minimum obligations and preventive measures that employers must take to ensure a psychologically safe working environment for their employees. These include:

- eliminating or controlling potential risks of violence and harassment;
- establishing a procedure for reporting and handling reports of violence and harassment;
- providing staff with training on prevention measures, risks, and their rights and responsibilities regarding such incidents.

Employers with more than 50 employees must also adopt a policy on the prevention of violence and harassment.

Our recommendation:

If your organization has not yet taken the necessary steps to prevent violence and harassment at work, we highly recommend seeking legal advice.

Decision of the Supreme Court of the Republic of Lithuania

LINK

Last month, the Supreme Court of Lithuania (LAT) heard a case regarding the separation of work and rest time during on-call duty.

Article 118 of the Labour Code defines 3 types of on-call duty:

- active on-call duty;
- passive on-call duty;
- passive on-call duty at home.

In this case, the employer and employee agreed on passive on-call duty at home. According to Article 118(4) of the Labour Code, such duty is not considered working time, and the employee should be paid at least 20 percent of their average monthly remuneration unless performing job functions.

However, the employee argued that their passive on-call home duty should be considered working time. The Supreme Court held that the main criteria for distinguishing between working time and rest time are 1) the intensity of the restrictions imposed on the employee and 2) the content of the restrictions imposed on the employee.

Passive on-call duty will be considered working time if the restrictions imposed by the employer have a greater impact on the employee's personal and social interests and on their ability to dispose of their time freely. This means that the employee must be present at the place indicated by the employer and be ready to start carrying out the functions of their job without delay if necessary.

Passive on-call duty at home is defined as an employee's home duty where the employee is not obliged to be present at the place designated by the employer but is available during normal rest periods when away from the workplace. Such restrictions have only a slight effect on the employee's ability to use their free time, and consequently, this time does not fall within the definition of working time.

Therefore, it is important to distinguish and determine, in each individual case, whether the employee's on-call duty time constitutes passive on-call duty or passive on-call duty at home, by applying the above criteria. If the parties to an employment contract identify passive on-call duty at home but set the intensity of the restrictions at a level that is typical of working time but not of rest time, such on-call duty cannot be qualified as rest time.

REGULATORY COMPLIANCE UPDATE

CRYPTO

01.2024

ECOVIS ProventusLaw

Consultation Paper on the draft guidelines on reverse solicitation under the Markets in Crypto Assets Regulation (MiCA)

LINK

ESMA – reverse solicitation for CASP services

ESMA previously underlined that the provision of crypto-asset services or activities by a third-country firm is strictly limited under MiCA to cases where such service is initiated at the own exclusive initiative of a client (the so called “reverse solicitation” exemption). This exemption should be understood very narrowly and as such must be regarded as the exception; and it cannot be assumed, nor exploited to circumvent MiCA.

ESMA, and national competent authorities, through their supervisory and enforcement powers, will take all necessary measures to actively protect European Union (EU)-based investors and MiCA-compliant crypto-asset service providers from undue incursions by non-EU and non-MiCA compliant entities.

In order to provide more guidance on the conditions of application of the reverse solicitation exemption and the supervision practices that national competent authorities may take to prevent its circumvention, ESMA is therefore considering the adoption of guidelines attached and has prepared a consultation paper to that effect.

Our recommendation:

Please familiarize yourself with the consultation paper and be aware of the possible implications it could have on your business, especially in cases where your services are provided in EU from companies based outside of the EU.

Consultation paper on the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments

LINK

ESMA – Crypto-asset classification as financial instruments under MiFID

The different approaches to the national transposition of MiFID across Member States mean that there is no commonly-adopted application of the definition of ‘financial instrument’ under MiFID in the EU. Whilst this issue has been noted as a concern since the implementation of MiFID/MiFID II, the issue is exacerbated with the MiCA regulation that exempts certain crypto-assets that have the characteristics of financial instruments.

In order to provide guidance on the qualification of crypto-assets as financial instruments that national competent authorities and market participants should consider, ESMA is therefore considering the adoption of guidelines and a consultation paper on them.

Our recommendation:

Please familiarize yourself with the consultation paper and have a clear understanding of how your crypto-assets could be classified and whether they do not fall under the definition of financial instruments.

Commission proposal on the AML regulation

LINK

New AML requirements for CASPs

The EU Commission has proposed an updated AML regulation forming part of the new EU AML regulatory package. The Council and the Parliament found a provisional agreement on stricter AML rules.
The provisional agreement expands the list of obliged entities to new bodies. The new rules will cover most of the crypto sector, forcing all crypto-asset service providers (CASPs) to conduct due diligence on their customers. This means that they will have to verify facts and information about their customers, as well as report suspicious activity.
According to the agreement, CASPs will need to apply customer due diligence measures when carrying out transactions amounting to €1000 or more. It adds measures to mitigate risks in relation to transactions with self-hosted wallets.

Our recommendation:

Please be aware of the developing narrative in regard to the new AML standards that could affect your activities and attempt to implement the necessary infrastructure beforehand.

info@proventuslaw.lt

REGULATORY COMPLIANCE UPDATE

CORPORATE

01.2024

ECOVIS ProventusLaw

Decision of The Supreme Court of the Republic of Lithuania of 2024-01-17

LINK

The Supreme Court of Lithuania examined an administrative offence case in which the CEO of a company was penalized under Paragraph 1 of Article 119 of the Code of Administrative Offenses for failing to convene an Annual General Meeting of Shareholders in violation of the requirements of the Law of the Republic of Lithuania on Joint Stock Companies.

The representative of the CEO argued that he had been unjustly penalized because he had not been able to fulfill his obligation to convene the Annual General Meeting of Shareholders due to the pending legal dispute concerning the approval of the company's financial statements for the previous year.

Having examined the case, the Supreme Court stated that to decide whether the penalization for failing to convene an Annual General Meeting of Shareholders within the time limit prescribed by the law is correct, it is necessary to establish the reasons why such a statutory duty of the CEO was not fulfilled. The fact that the previous CEO, submitted financial statements for the preceding financial years which had not been approved by the general meeting of shareholders and was punished administratively for that, does not justify the failure to comply with the obligation to convene the meeting, since no legal process had been followed which would have led to the removal of the statements not approved by the General Meeting of Shareholders from the database of the Centre of Registers or to any other action being taken. The errors made in the preparation of the company's financial statements should have been corrected in accordance with the procedure laid down in the Law on Corporate Reporting of the Republic of Lithuania.

The current CEO did not make use of this opportunity, although he had the right to do so, and is therefore rightly fined.

Our recommendation:

ECOVIS ProventusLaw would like to stress the importance of ensuring the timely convening of the Annual General Meetings of Shareholders.

In companies which have a Board, the Agenda of the Annual General Meeting of the Shareholders must be prepared by the Board. In cases provided for in the Paragraph 3 of Article 23 of the Law on Companies, the obligation falls to the CEO of the company.

As seen from the described example, failure to fulfill this statutory duty can even result in administrative proceedings and penalization. Furthermore, unfulfilled fiduciary duties can be the basis for civil liability of the members of the management bodies.

Additionally, proactive approach to address mistakes made in the financial statements should be taken in accordance to the Law on Corporate Reporting.