



Proposal for a Directive of the European Parliament and of the Council on the Mechanisms to Be Put in Place by the Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Repealing Directive (EU) 2015/849



On February 12, 2024, the Council of the European Union and the European Parliament finalized the text of the 6th AML Directive. The AMLD6 establishes a harmonized definition of money laundering offenses, outlining 22 specific activities within categories like organized crime, terrorism, human trafficking, and corruption. It also extends criminal liability to legal entities, holding companies, and partnerships accountable for illegal activities if there's a lack of supervision leading to such actions.

Fraud Prevention Guidelines

The Bank of Lithuania has developed Fraud Prevention Guidelines to encourage financial market participants to enhance their management of financial fraud risk and improve compliance with EU and Lithuanian legislation. These guidelines aim to assist payment service providers in detecting, assessing, and mitigating fraud risk effectively.



Overview of money laundering and terrorist financing prevention 2023



The Bank of Lithuania has published an infographic of supervision of AML/CTF compliance in the first quarter of 2023. The infographic shows the number of supervised financial market participants, supervisory actions, guidelines and reviews for FMPs, overview of clients and payments in the payments sector and priority areas of the BoL.

Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group



Chainalysis has issued a report on crypto crime, according to which, in 2023, illicit addresses sent \$22.2 billion worth of cryptocurrency to services, which is a significant decrease from the \$31.5 billion sent in 2022. Some of this drop may be attributed to an overall decrease in crypto transaction volume, both legitimate and illicit. However, the drop in money laundering activity was steeper, at 29.5%, compared to the 14.9% drop in total transaction volume.

FATF Jurisdictions under Increased Monitoring



On February 23, 2024, the Financial Action Task Force has held a meeting during which it included Kenya and Namibia to the list of jurisdictions subject to increased monitoring (the "Grey List"). The FATF also decided to remove Barbados, Gibraltar, Uganda, and the United Arab Emirates from the Grey List.

Frankfurt to host the EU's new anti-money laundering authority (AMLA)



The Council and European Parliament have agreed that Frankfurt will be the headquarters for the EU's new Anti-Money Laundering Authority (AMLA), set to begin operations in mid-2025 with over 400 staff members. AMLA will play a central role in EU's anti-money laundering efforts, having supervisory powers over obligated entities and the ability to impose sanctions.

After the court satisfied the claim of the General Prosecutor's Office, assets worth more than 700 thousand euros were confiscated for the benefit of the state



The Kaunas District Court has issued a decision to confiscate property valued at 701,998 EUR, including cash, three single-family houses, and an apartment, in favour of the state. The General Prosecutor's Office, in collaboration with the Financial Crime Investigation Service, determined that the individual could not justify the acquisition of these high-value assets with legitimate income. Furthermore, it was revealed that the individual transferred the unexplained property to four other individuals, identified as dishonest acquirers.

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





Publication by the Bank of Lithuania



LINK

The Bank of Lithuania has reached an important milestone of the data management programme: banks operating in Lithuania have started to provide supervisory information to REGATA, a state-of-the-art reporting system. It will reduce the administrative burden on financial market participants and enable more efficient data management.

New rules adopted by European Parliament



LINK

The European Parliament adopted the Regulation amending the Single Euro Payments Area Regulation and the Cross-Border Payments Regulation as regards instant credit transfers in euro.

The new regulation aims to make sure that retail clients and businesses, especially SMEs, will not have to wait for their money, as well as to enhance the safety of transfers. Banks and other payment service providers (PSPs) will have to ensure credit transfers are affordable and immediately processed. The text, already agreed with EU member states, updates the current Single Euro Payments Area (SEPA) rules.

Bank of Lithuania consultancy events



LINK

This year, the Bank of Lithuania plans to organise 16 consultative events for financial market participants. The main focus will be on the regulation of cryptocurrency services, prevention of fraud and money laundering.

Judgment of the European Court of Justice



LINK

EU Court of Justice rules on the difference between payment institutions, e-money institutions and banks. Payment institutions may hold client money much longer than previously thought.

info@proventuslaw.lt



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



Publication by the Bank of Lithuania



LINK

Consumers' ability to choose their preferred payment method is improving, but some people are still faced with situations where they are unable to pay at the point of sale in the way they prefer. Businesses are considering the most convenient way to accept payments.

Judgment of the Regional Administrative Court



LINK

The Regional Administrative Court annulled the resolution of the Bank of Lithuania and ordered the Bank of Lithuania to remove on its website the information on the sanction imposed on shareholder of electronic money institution.

Our recommendations and details are in this file



Dutch Data Protection authority fines Uber B.V. and Uber Technologies Inc. EUR 10,000,000 for breaches of driver information.



[LINK](#)

The violation: the Dutch Data Protection Authority (Dutch DPA), together with CNIL, found that both Uber B.V. and Uber Technologies had committed several notable GDPR violations, including failing to fulfil data subject access requests in an accessible format or ensuring that the exercise of rights form was sufficiently accessible. These weren't the only violations found in terms of data subject rights, as the companies also failed to mention the right to data portability in their privacy statements. They also failed to meet their information obligations, providing information to drivers only in English. Furthermore, the information provided was incomplete, as the retention periods provided were too general and there was insufficient information about data transfers outside the EU. According to the Dutch DPA, the data controllers should have provided better and more thorough information to their drivers.

The Court of Justice of the European Union delivers an opinion in a case concerning the sale of personal data contained in a database.



[LINK](#)

The news: the Advocate General of the Court of Justice of the European Union (hereafter - CJEU) has delivered an opinion in a case C-693/22 concerning the sale of a database in enforcement proceedings. The case raised questions about the processing of personal data, with the Advocate General finding that the actions taken by the court enforcement officer, including retrieving, consulting and using the data to estimate its value, constituted 'processing' under the GDPR. One of the key issues in the case was the lack of consent from the data subjects for the transfer of their personal data. In addition, the AG emphasised the need for consent for the transfer of data, the lawful basis for processing and the balance between the right to property and the protection of personal data. The conclusion suggested that national legislation could allow a judicial officer to sell a database containing personal data without consent if it's considered a necessary and proportionate measure to enforce a civil claim.

EDPB clarifies the notion of main establishment under the GDPR.



[LINK](#)

The news: the EDPB has adopted an opinion on the notion of 'main establishment' and the criteria for the application of the one-stop-shop mechanism. The opinion helps to clarify what the 'main establishment' of a data controller means. This is particularly relevant for data controllers who take processing decisions outside the EU. As explained in the Opinion, the EDPB considers the main establishment of a data controller to be its central administration within the EU. The EDPB also clarified that the one-stop-shop rule only works if it can be shown that an establishment of the data controller in the European Union takes decisions about how and why certain data are processed and has the authority to implement those decisions. Put simply, if the data processing decisions are made outside the EU and there is no main establishment of the controller in the Union, the one-stop-shop rule doesn't apply. The opinion also highlights that data controllers have the burden of proving where processing decisions are made, with relevant elements such as records of processing activities and privacy policies assisting in the assessment of the main establishment. The EDPB also emphasised that supervisory authorities can challenge a controller's claim by objectively examining the facts and requesting further information. While central management in the EU serves as a starting point, a detailed assessment of where data processing decisions are made and implemented within the Union is essential before designating a main establishment.

State Data Protection Inspectorate release 2024 plan for inspections.



[LINK](#)

The news: as part of their functions, the State Data Protection Inspectorate (hereinafter - VDAI) announced that in 2024, VDAI has planned 16 planned inspections and 10 monitoring exercises in both public and private sector organisations. VDAI will conduct planned inspections to assess and improve the personal data processing practices of selected organisations within the sector. The summaries of the inspections, which will be made public, will be available to all organisations, enabling them to assess and improve their own performance on the basis of the findings. The list of organisations subject to the inspections has also been made public.

Recommendations for the legal department of organizations:

- review the list of entities to confirm whether planned inspection will be performed at your organisation;
- even if your organisation is not on the list, ensure that your organisation is fully compliant with data subject rights implementation, especially the right of access.



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 adopts 13th package of individual and economic sanctions against Russia two years after Ukraine invasion

In view of the second-year mark of the beginning of Russia's full-scale invasion of Ukraine - a thirteenth package of restrictive measures against Putin's regime, those who are responsible for perpetuating his illegal, unprovoked and unjustified war of aggression and those who are significantly supporting it.

Individual listings

The Council decided to impose restrictive measures on an additional 106 individuals and 88 entities responsible for actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. The new listings agreed target primarily the military and defence sectors and associated individuals, including those involved in DPRK armament supply to Russia, as well as members of the judiciary, local politicians and people responsible for the illegal deportation and military re-education of Ukrainian children.

Import-export controls and restrictions

The Council added 27 new entities to the list of those directly supporting Russia's military and industrial complex in its war of aggression against Ukraine. They will be subject to tighter export restrictions concerning dual use goods and technologies, as well as goods and technology which might contribute to the technological enhancement of Russia's defence and security sector.

Iron and steel

United Kingdom was added to a list of partner countries which apply a set of restrictive measures on imports of iron and steel from Russia, and a set of import control measures that are substantially equivalent to those of the EU.

Our recommendation:

Please be reminded to fully comply with the restrictive measures imposed by the EU and closely monitor the list of newly designated individuals and entities.

Financial market participants should review and assess their current business activities and relationships with entities and individuals that may be subject to EU sanctions related to Russia's military aggression against Ukraine. This may include conducting due diligence on customers, counterparties, and business partners, monitoring transactions for potential sanctions risks, and implementing appropriate controls to ensure compliance with the sanctions regime.

It is important for financial market participants to have in place effective sanctions compliance programs to help prevent unintended exposure to sanctioned individuals, entities or activities. This may include ongoing training for employees, regular risk assessments and updates to policies and procedures.

Stay up to date with the news on how to implement international 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.it



The European Parliament's ECON Committee



LINK

The European Parliament's ECON Committee voted in favor of full reimbursement for consumers who fall victim to identity theft scams. According to the committee, payment service providers could reimburse consumers directly for all types of payment fraud, and then recover these funds from electronic communications providers if they fail to take action against fraudulent websites or phone number spoofing.

The next steps involve a plenary vote in the European Parliament in April, followed by agreement with national governments in the Council.

Our recommendation:

We recommend that you take note of recent legislative developments concerning the reimbursement of consumers who are victims of identity theft, strengthen your fraud prevention measures, and maintain transparent communication with your customers.

The Council of the European Union



LINK

The Council of the European Union has adopted a directive aimed at strengthening consumer rights in the context of the ecological transition. This directive amends the rules on unfair commercial practices and consumer rights to adapt them to the circular economy. It protects consumers against misleading "green" claims, clarifies the responsibility of traders in the event of information (or lack of information) on early obsolescence, unnecessary software updates or the unjustified obligation to buy spare parts from the original producer.

Finally, it improves the information available to encourage more sustainable choices. For example, throughout the EU, products will carry a harmonized label containing information on the commercial guarantee of durability.

Our recommendation:

We advise you to make these new rules your own in order to comply with the directive, to avoid misleading environmental claims in your commercial operations, and to make your product information more transparent.

European Commission news feed



LINK

On February 17, the EU's Digital Services Act (DSA) began to apply to all online intermediaries in the EU, marking a milestone in online regulation. It aims to make the digital environment safer, fairer and more transparent. EU users benefit from better protection against illegal goods and content, as well as the preservation of their rights on online platforms where they interact with other users, share information or make purchases.

The DSA also applies to hosting services and online intermediaries, with specific obligations. Since August 2023, it has already applied to 19 Very Large Online Platforms (VLOPs), with others to follow, as well as Search Engines (VLOSEs). Three new designated platforms must meet the stricter obligations by the end of April, but all must comply with the general DSA obligations.

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



Employment Service Under the Ministry of Social Security and Labour

The employer located in the Republic of Lithuania has a duty to provide information on foreigners employed under a contract of employment and sent for temporary work in the Republic of Lithuania to the Employment Service (on foreigners employed under an employment contract) and to the State Labour Inspectorate of the Republic of Lithuania under the Ministry of Social Security and Labour (on foreigners sent for temporary employment in the Republic of Lithuania) through the information system of the Sodra EDAS by filling in the LDU form. The LDU form must be filled in all cases including if a foreigner will work remotely in a Lithuanian company (without coming to the Republic of Lithuania). Filling LDU form employer should indicate which country's social insurance system the employee will be subject to.

Our recommendation:

If your company is hiring foreigners, the LDU must be filled out and submitted through the SODRA system.

Decision of the Constitutional Court of the Republic of Lithuania



The Constitutional Court ruled that the provision of Article 7(3) of the Law on Social Insurance of Occupational Accidents and Diseases of the Republic of Lithuania, According to which 'Accidents occurred on the way to or from work shall not be recognised as insured events if the insured person was drunk or under the influence of psychoactive substances', in so far as it excludes from insured events accidents on the way to or from work which occur when the insured person is drunk or under the influence of psychoactive substances and which are not caused by his or her drunkenness or under the influence of psychoactive substances, is contrary to Article 52 of the Constitution of the Republic of Lithuania and to the principle of the rule of law.

So from now on, if an accident occurred on the way to or from work while employee was drunk or under the influence of psychoactive substances, the accident could be considered insured event if it was not caused by employee's state of alcohol or psychoactive substances consumption.

Decision of the Supreme Court of the Republic of Lithuania

**LINK**

The Supreme Court of Lithuania (LAT) heard a case regarding the liability of an outsourced company that provides safety and health specialist services for the employer, after the employer compensated the damage due to the death of an employee at the workplace.

The case establishes that an occupational accident occurred on the premises of the plaintiff's undertaking, in which an employee of the plaintiff was killed.

The plaintiff (the employer) compensated the relatives of the deceased worker for non-material damage and claimed damages from the defendant, with whom it had concluded a contract for the performance of part of the functions of the occupational safety and health service in the plaintiff's undertaking. The plaintiff argued that the damage was caused by the defendant's improper performance of its contractual obligations.

After examining the case, the panel of judges of the Supreme Court of Lithuania noted that although the Law on Occupational Safety and Health establishes an absolute duty of the employer to provide employees with safe and healthy working conditions, and the employer is liable for the actions of a person to whom employer delegated his safety and health enforcement functions, this does not eliminate the liability of this person to the employer for the non-performance of contractual obligations (inadequate fulfilment). In this case the defendant failed to carry out his contractual obligations properly, which resulted in the plaintiff's losses and which the defendant must compensate.

However, the panel of judges of the Supreme Court applied the principle of mixed fault and reduced the damages awarded to the plaintiff by 30 %, since it was established that the accident was partly caused by the unlawful acts of the plaintiff itself, namely that the plaintiff did not properly carry out the duties assigned to it by the regulations in the field of occupational safety and health, which had not been delegated to the defendant by contract.

The defendant's share of the liability (70 %) is higher since, as an entrepreneur providing services in the field of occupational safety and health, the defendant was under a duty to exercise the utmost care and diligence in providing those services, which it failed to do.

ESMA News report on the requirements when posting investments recommendations on social media

[LINK](#)

ESMA published its latest news regarding the requirements when posting investment recommendations on social media. The authority is drawing the attention of the crypto market participants to be wary of the Market Abuse Regulation, which covers instances of unsolicited investment advice that could be subject to penalties.

Our recommendation:

Read the brief news report published by ESMA. Evaluate whether your social media or any other public communications adhere to the requirements of the Market Abuse Regulation.

ESMA Public Statement

[LINK](#)

ESMA clarifies certain best execution reporting requirements under MiFID II.

The MiCA regulation prescribes in its preamble that crypto-asset service providers (CASPs) need to have in place a “best execution” policy that would establish a procedure and methodology yielding the best result for its Clients when executing orders on behalf of its Clients.

Our recommendation:

Familiarize yourself with ESMA’s statement and use it as guidance when compiling / adapting your best execution policy for crypto-assets.

European Commission delegated regulation on the procedural rules for fine imposition by EBA on issuers of ARTs and EMTs

[LINK](#)

The adopted delegated regulation clarifies the procedural rules for the exercise of the power to impose fines or periodic penalty payments by the EBA on issuers of significant ART and EMT issuers.

Our recommendation:

Necessary to review for potential ART and EMT issuers to have a better understanding when the regulatory authorities have the power to impose fines and penalties for ART / EMT issuance misconduct.

European Commission delegated regulation specifying the criteria and factors to be taken into account by the European Securities Markets Authority, the European Banking Authority and competent authorities in relation to their intervention powers

[LINK](#)

According to Article 103(1) of MiCA, the European Securities and Markets Authority (ESMA) may temporarily prohibit or restrict the marketing, distribution or sale of certain crypto-assets other than asset-referenced tokens or e-money tokens or crypto-assets other than asset-referenced tokens or e-money tokens with certain specified features, or a type of activity or practice related to crypto-assets other than asset-referenced tokens or e-money tokens. Similarly, pursuant to Article 104(1) of MiCA, the European Banking Authority (EBA) may temporarily prohibit or restrict the marketing, distribution or sale of certain asset-referenced tokens or e-money tokens or asset-referenced tokens or e-money tokens.

Our recommendation:

Important for all kinds of crypto-asset issuers and crypto-asset service providers operating crypto-asset trading platforms. Necessary to familiarize with the delegated regulation to have a better understanding what kind of powers of intervention the European Supervisory Authorities (ESAs) have and what restrictive measures should be made technically possible for crypto-asset issuers and CASPs operating trading platforms.

European Commission delegated regulation on the criteria classifying ARTs and EMTs as significant

[LINK](#)

The adopted delegated regulation clarifies the criteria regarding the classification of ARTs and EMTs as significant.

Our recommendation:

Important for ART / EMT issuers. Necessary to understand when an ART / EMT can be classified as significant and what reporting data should be provided by ART / EMT issuers for keeping track when the token passes the threshold for being considered as significant.

European Commission delegated regulation specifying the fees charged by EBA to issuers of significant ARTs and EMTs

[LINK](#)

Pursuant to Article 137(1) of MiCA, the European Banking Authority (EBA) is to charge fees to issuers of significant ARTs and EMTs. Those fees are to cover EBA’s expenditure on the execution of its supervisory tasks relating to issuers of significant ARTs and EMTs in accordance with Articles 117 and 119 of MiCA, as well as the reimbursement of costs that the competent authorities might incur when carrying out work under MiCA, in particular as a result of any delegation of tasks by EBA in accordance with Article 138 of MiCA.

Our recommendation:

Important for ART / EMT issuers that could become significant. Necessary to familiarize with the dynamic between significant ART / EMT issuers and the EBA; and take into account the charges associated with the stablecoin issuance and transactions.

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



Decision of The Court of Appeal of the Republic of Lithuania of 2024-01-30



LINK

The Court of Appeal ruled on a significant case involving a dispute over a provision that obliges the person selling the shares to ensure that the new shareholder becomes party to the agreement and share option provisions.

In this instance, the shareholders had concluded an agreement with which they sought to regulate their relations. This agreement had a share option clause which obliged to sell the shares to the other shareholder. Ignoring the clause, one of the shareholders sold off their shares of the company to another person and did not ensure that the new shareholder becomes a party to the shareholder agreement. Due to this, the remaining shareholder lost his option right ensured by the shareholder agreement.

The remaining shareholder initiated the case in court and requested for the share purchase agreement to be recognised as void and to impose a fine on the seller of the shares as provided for in the shareholder agreement.

The Court of Appeal held that the failure to ensure that the new shareholder becomes party to the shareholder agreement is a breach of the agreement, but it does not invalidate the share purchase agreement. However, the Court did note that such breach could be a basis for contractual liability.

While the Court did hold that a fine provided for in the agreement could be awarded, it decided not to award the fine in this instance. The Court justified its decision by noting that the plaintiff found out about the share purchase agreement on the day it was concluded but filed the suit more than 6 months later thus missing the term for bringing a suit to be awarded the contractual.

Our recommendation:

Such disputes are rare in the Lithuanian case law and can be used to learn something new and to incorporate such knowledge into future shareholder agreements or used during disputes.

The dispute illustrates that the breach of contractual clause which obliges the person selling the shares to ensure that the new shareholder becomes party to shareholder agreement is not sufficient to recognise share purchase agreement as void. However, such breach can result in contractual liability.

Shareholders must keep in mind that fines provided for in the shareholder agreements can be enforced in case of breach of contract, but shareholders must be aware of the term for acting and bringing a suit demanding enforcement of the fine. The term is 6 months after the person became aware of the infringement or should have become aware of the infringement.