2024/1640

19.6.2024

# DIRECTIVE (EU) 2024/1640 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

## of 31 May 2024

## on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849

**(Text with EEA relevance)**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank ([1]),

Having regard to the opinion of the European Economic and Social Committee ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) Directive (EU) 2015/849 of the European Parliament and of the Council ([4]) constitutes the main legal instrument for the prevention of the use of the Union's financial system for the purposes of money laundering and terrorist financing. That Directive sets out a comprehensive legal framework, which Directive (EU) 2018/843 of the European Parliament and the Council ([5]) further strengthened by addressing emerging risks and increasing transparency of beneficial ownership. Notwithstanding the achievements under that legal framework, experience has shown that Directive (EU) 2015/849 should be further improved to adequately mitigate risks and to effectively detect criminal attempts to misuse the Union financial system for criminal purposes and to further the integrity of the internal market.

(2) Since the entry into force of Directive (EU) 2015/849, a number of areas have been identified where amendments would be needed to ensure the necessary resilience and capacity of the Union financial system to prevent money laundering and terrorist financing.

(3) Significant variations in practices and approaches by competent authorities across the Union, as well as the lack of sufficiently effective arrangements for cross-border cooperation were identified in the implementation of Directive (EU) 2015/849. It is therefore appropriate to define clearer requirements, which should contribute to smooth cooperation across the Union whilst allowing Member States to take into account the specificities of their national systems.

([1]) OJ C 210, 25.5.2022, p. 15.
([2]) OJ C 152, 6.4.2022, p. 89.
([3]) Position of the European Parliament of 24 April 2024 (not yet published in the Official Journal) and decision of the Council of 30 May 2024.
([4]) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).
([5]) Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (OJ L 156, 19.6.2018, p. 43).

(4) This Directive is part of a comprehensive package aiming at strengthening the Union's anti-money laundering and countering the financing of terrorism ('AML/CFT') framework. Together, this Directive and Regulations (EU) 2023/1113 ([6]), (EU) 2024/1624 ([7]) and (EU) 2024/1620 ([8]) of the European Parliament and of the Council will form the legal framework governing the AML/CFT requirements to be met by obliged entities and underpinning the Union's AML/CFT institutional framework, including the establishment of an Authority for anti-money laundering and countering the financing of terrorism (AMLA).

(5) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted at Union level which do not take into account international coordination and cooperation would have very limited effect. The measures adopted by the Union in that field should therefore be compatible with, and at least as stringent as, other actions undertaken at international level. Union action should continue to take particular account of the Financial Action Task Force (FATF) Recommendations and instruments of other international bodies active in the fight against money laundering and terrorist financing. With a view to reinforcing the efficacy of the fight against money laundering and terrorist financing, the relevant Union legal acts should, where appropriate, be aligned with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation adopted by the FATF in February 2012 (the 'revised FATF Recommendations') and the subsequent amendments to those standards.

(6) Specific money laundering and terrorist financing threats, risks and vulnerabilities affecting certain economic sectors at national level diminish the ability of Member States to contribute to the integrity and soundness of the Union financial system. As such, it is appropriate to allow Member States, upon identification of such sectors and specific risks, to decide to apply AML/CFT requirements to additional sectors than those covered by Regulation (EU) 2024/1624. With a view to preserving the effectiveness of the internal market and the Union AML/CFT system, the Commission should be able, with the support of AMLA, to assess whether the intended application by Member States of AML/CFT requirements to additional sectors is justified. In cases where the best interests of the Union would be achieved by taking action at Union level as regards specific sectors, the Commission should inform the Member State intending to apply the AML/CFT requirements to those sectors that it intends to take action at Union level instead and the Member State should abstain from taking the intended national measures, unless those measures are intended to address an urgent risk.

(7) Certain categories of obliged entities are subject to licensing or regulatory requirements for the provision of their services, whereas for other categories of operators access to the profession is not regulated. Regardless of the framework that applies to the exercise of the profession or activity, all obliged entities act as gatekeepers of the Union's financial system and must develop specific AML/CFT skills to fulfil that task. Member States should consider providing training to persons wishing to enter the profession of those entities to enable them to perform their duties. Member States could consider, for example, including AML/CFT courses in the academic offer linked to those professions or cooperating with professional associations to train newcomers to those professions.

(8) Where obliged entities are not subject to specific licensing or registration requirements, Member States should have in place systems that enable supervisors to know with certainty the scope of their supervisory population in order to ensure the adequate supervision of such obliged entities. This does not mean that Member States need to impose AML/CFT-specific registration requirements where this is not needed for the identification of obliged entities, as is the case for example where VAT registration enables the identification of operators that carry out activities falling within the scope of AML/CFT requirements.

([6]) Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (OJ L 150, 9.6.2023, p. 1).

([7]) Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L, 2024/1624, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1624/oj).

([8]) Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (OJ L, 2024/1620, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1620/oj).).

(9) Supervisors should ensure that, with regard to currency exchange offices, cheque cashing offices, trust or company service providers, and gambling service providers, as well as financial mixed activity holding companies, the persons who effectively manage the business of such entities and the beneficial owners of such entities are of good repute and act with honesty and integrity and possess the knowledge and expertise necessary to carry out their functions. The criteria for determining whether a person complies with those requirements should, as a minimum, reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes. In order to foster a common approach to the verification by supervisors that the management and beneficial owners of obliged entities satisfy those requirements, AMLA should issue guidelines on the criteria to assess good repute, honesty and integrity and the criteria to assess knowledge and expertise.

(10) For the purposes of assessing the appropriateness of persons holding a management function in, or otherwise controlling, obliged entities, any exchange of information about criminal convictions should be carried out in accordance with Council Framework Decision 2009/315/JHA ([9]) and Council Decision 2009/316/JHA ([10]). In addition, supervisors should be able to access all information necessary to verify the knowledge and expertise of the senior management, as well as their good repute, honesty and integrity and that of the obliged entity's beneficial owners, including information available through reliable and independent sources.

(11) Investor residence schemes present risks and vulnerabilities, in particular, in relation to money laundering, the evasion of Union restrictive measures, corruption and tax evasion which could ultimately give rise to certain risks for the security of the Union. For example, weaknesses in the operation of certain schemes, including the absence of risk management processes or weak implementation of those processes can create opportunities for corruption, whereas weak or inconsistently applied checks on applicants' source of funds and source of wealth might lead to higher risks that such schemes are exploited by applicants for criminal purposes, aiming to legitimise funds obtained through illicit means. In order to avoid that risks stemming from the operation of such schemes affect the Union's financial system, Member States whose national law enables the granting of residence rights in exchange for any kind of investment should therefore put in place measures to mitigate the associated risks of money laundering, its predicate offences and terrorist financing. Such measures should include an adequate risk management process, including the effective monitoring of its implementation, checks on the profile of the applicants, including obtaining information on their source of funds and source of wealth, and the verification of information on applicants against information held by competent authorities.

(12) The Commission is well placed to review specific cross-border threats that could affect the internal market and that cannot be identified and effectively combatted by individual Member States. It should therefore be entrusted with the responsibility for coordinating the assessment of risks relating to cross-border activities. Involvement of the relevant experts, such as the Expert Group on Money Laundering and Terrorist Financing and the representatives from the Financial Intelligence Units (FIUs), as well as, where appropriate, from other Union-level bodies including AMLA, is essential for the effectiveness of the process of the assessment of risks. National risk assessments and experience are also an important source of information for that process. Such assessment of the cross-border risks by the Commission should not involve the processing of personal data. In any event, data should be fully anonymised. Union and national data protection supervisory authorities should be involved only if the assessment of the risk of money laundering and terrorist financing has an impact on the privacy and data protection of individuals. To maximise synergies between the assessment of risks at Union and national level, the Commission and Member States should endeavour to apply consistent methodologies.

(13) The findings of the risk assessment at Union level can assist competent authorities and obliged entities in the identification, understanding, management and mitigation of the risk of money laundering and terrorist financing, as well as of risks of non-implementation and evasion of targeted financial sanctions. It is therefore important that the findings of the risk assessment are made public.

(14) Member States remain best placed to identify, assess, understand and decide how to mitigate risks of money laundering and terrorist financing affecting them directly. Therefore, each Member State should take the appropriate steps to properly identify, assess and understand its money laundering and terrorist financing risks, as well as risks of non-implementation and evasion of targeted financial sanctions and to define a coherent national strategy to put in

([9]) Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009, p. 33).

([10]) Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23).

place actions to mitigate those risks. Such national risk assessment should include a description of the institutional structure and procedures of the Member State's AML/CFT regime, as well as the allocated human and financial resources to the extent that this information is available. In order to maintain an ongoing understanding of risks, Member States should regularly update their national risk assessment, and should also be able to supplement it with targeted updates and assessments of risks associated with specific sectors, products or services.

(15) Legal entities and legal arrangements can provide a means for criminals to hide behind a veil of legitimacy and might therefore be misused to launder illicit proceeds, whether domestically or across borders. To mitigate those risks, it is important that Member States understand the risks associated with the legal entities and legal arrangements that are in their territory, whether because the entities are established there, or because trustees of express trusts or persons holding equivalent positions in similar legal arrangements are established or reside there, or they administer the legal arrangement from there. In the case of legal arrangements, given the settlor's right as to the choice of the law that governs the arrangement, it is also important that Member States have an understanding of the risks associated with the legal arrangements that can be set up under their law, irrespective of whether their laws explicitly regulate them, or their creation finds its source in the freedom of contract of the parties and is recognised by national courts.

(16) Given the integrated nature of the international financial system and openness of the Union economy, risks associated with legal entities and legal arrangements expand beyond those in the Union territory. It is thus important that the Union and its Member States have an understanding of the exposure to risks emanating from foreign legal entities and foreign legal arrangements. Such assessment of risks does not need to address each individual foreign legal entity or foreign legal arrangement that has a sufficient link with the Union, whether by virtue of it acquiring real estate or being awarded contracts following a public procurement procedure, or because of transactions with obliged entities that allow them to access the Union's financial system and economy. The risk assessment should however enable the Union and its Member States to understand what type of foreign legal entities and foreign legal arrangements enjoy such an access to the Union's financial system and economy, and what types of risks are associated with that access.

(17) The results of risk assessments should be made available to obliged entities in a timely manner to enable them to identify, understand, manage and mitigate their own risks. Those results can be shared in a summarised form and made available to the public, and should not include classified information or personal data.

(18) In addition, to identify, understand, manage and mitigate risks at Union level to an even greater degree, Member States should make available the results of their risk assessments to each other, to the Commission and to AMLA. Classified information or personal data should not be included in those transmissions unless deemed strictly necessary for the performance of AML/CFT tasks.

(19) In order to effectively mitigate the risks identified in the national risk assessment, Member States should ensure consistent action at national level either by designating an authority to coordinate the national response or by establishing a mechanism for that purpose. Member States should ensure that the designated authority or the established mechanism has sufficient powers and resources to perform that task effectively and ensure an adequate response to the identified risks.

(20) To be able to review the effectiveness of their systems for combating money laundering and terrorist financing, Member States should maintain, and improve the quality of, relevant statistics. With a view to enhancing the quality and consistency of the statistical data collected at Union level, the Commission and AMLA should keep track of the Union-wide situation with respect to the fight against money laundering and terrorist financing and should publish regular overviews.

(21) The FATF has developed standards for jurisdictions to identify and assess the risks of potential non-implementation or evasion of the proliferation financing-related targeted financial sanctions, and to take action to mitigate those risks. Those new standards introduced by the FATF do not substitute or undermine the existing strict requirements for countries to implement targeted financial sanctions to comply with the relevant United Nations Security Council resolutions relating to the prevention, suppression and disruption of the proliferation of weapons of mass destruction and its financing. Those existing obligations, as implemented at Union level by Council Decisions

2010/413/CFSP ([11]) and (CFSP) 2016/849 ([12]) as well as Council Regulations (EU) No 267/2012 ([13]) and (EU) 2017/1509 ([14]), remain binding on all natural and legal persons within the Union. Given the specific risks of non-implementation and evasion of targeted financial sanctions to which the Union is exposed, it is appropriate to expand the assessment of risks to encompass all targeted financial sanctions adopted at Union level. The risk-sensitive nature of AML/CFT measures related to targeted financial sanctions does not remove the rule-based obligation incumbent upon all natural or legal persons in the Union to freeze and not make funds or other assets available to designated persons or entities.

(22) In order to reflect developments at international level, particularly the revised FATF recommendations, and to ensure a comprehensive framework for implementing targeted financial sanctions, requirements should be introduced by this Directive to identify, understand, manage and mitigate risks of non-implementation or evasion of targeted financial sanctions at Union level and at Member State level.

(23) Central registers of beneficial ownership information ('central registers') are crucial in combating the misuse of legal entities and of legal arrangements. Therefore, Member States should ensure that the beneficial ownership information of legal entities and legal arrangements, information on nominee arrangements and information on foreign legal entities and foreign legal arrangements are held in a central register. To ensure that those central registers are easily accessible and contain high-quality data, consistent rules on the collection and storing of that information by the registers should be introduced. Information held in central registers should be accessible in a readily usable and machine-readable format.

(24) With a view to enhancing transparency in order to combat the misuse of legal entities, Member States should ensure that beneficial ownership information is registered in a central register located outside the legal entity, in full compliance with Union law. Member States should, for that purpose, use a central database, which collects beneficial ownership information, or the business register, or another central register. Member States can decide that obliged entities are responsible for providing certain information to the central register. Member States should make sure that in all cases that information is made available to competent authorities and is provided to obliged entities when they apply customer due diligence measures.

(25) Beneficial ownership information of express trusts and similar legal arrangements should be registered where the trustees and persons holding equivalent positions in similar legal arrangements are established or where they reside, or where the legal arrangement is administered. In order to ensure the effective monitoring and registration of information on the beneficial ownership of express trusts and similar legal arrangements, cooperation between Member States is also necessary. The interconnection of Member States' registries of beneficial owners of express trusts and similar legal arrangements should make that information accessible, and should also ensure that the multiple registration of the same express trusts and similar legal arrangements is avoided within the Union.

(26) Timely access to information on beneficial ownership should be ensured in ways which avoid any risk of tipping off the legal entity or the trustee or person in an equivalent position concerned.

(27) The accuracy of data included in the central registers is fundamental for all of the relevant authorities and other persons allowed access to that data, and to make valid, lawful decisions based on that data. Therefore, Member States should ensure that the entities in charge of central registers verify, within a reasonable time following submission of beneficial ownership information and on a regular basis thereafter, that the information submitted is adequate, accurate and up-to-date. Member States should ensure that entities in charge of central registers are able to request any information they need to verify beneficial ownership information and nominee information, as well as situations where there is no beneficial owner or where the beneficial owners could not be determined. In those situations, the information provided to the central register should be accompanied by a justification including all relevant

([11]) Council Decision 2010/413/CFSP of 26 July 2010 concerning restrictive measures against Iran and repealing Common Position 2007/140/CFSP (OJ L 195, 27.7.2010, p. 39).
([12]) Council Decision (CFSP) 2016/849 of 27 May 2016 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Decision 2013/183/CFSP (OJ L 141, 28.5.2016, p. 79).
([13]) Council Regulation (EU) No 267/2012 of 23 March 2012 concerning restrictive measures against Iran and repealing Regulation (EU) No 961/2010 (OJ L 88, 24.3.2012, p. 1).
([14]) Council Regulation (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation (EC) No 329/2007 (OJ L 224, 31.8.2017, p. 1).

supporting documents to enable the register to ascertain whether this is the case. Member States should also ensure that the entities in charge of central registers have adequate tools at their disposal to carry out verifications, including automated verifications in a manner that safeguards fundamental rights and avoids discriminatory outcomes.

(28) It is important that Member States entrust the entities in charge of central registers with sufficient powers and resources to verify beneficial ownership and the veracity of information provided to them, and to report any suspicion to their FIU. Such powers should include the power to conduct of inspections at the business premises of legal entities and of obliged entities that act as trustees of express trusts or persons holding equivalent positions in similar legal arrangements, whether carried out by the entities in charge of the central registers or by other authorities on their behalf. Member States should ensure that adequate safeguards are applied where those trustees or persons holding an equivalent position in a similar legal arrangement are legal professionals, or where their business premises or registered office are the same as their private residence. Such powers should extend to representatives of foreign legal entities and foreign legal arrangements in the Union, where those legal entities and arrangements have registered offices or representatives in the Union.

(29) Where a verification of beneficial ownership information leads an entity in charge of a central register to conclude that there are inconsistencies or errors in that information, or where that information otherwise fails to fulfil the requirements, it should be possible for the entity to withhold or suspend the proof of registration in the central register, until the failures have been corrected.

(30) Entities in charge of central registers should carry out their functions free of undue influence, including any undue political or industry influence in relation to the verification of information, the imposition of measures or sanctions and the granting of access to persons with a legitimate interest. To that end, entities in charge of central registers should have in place policies to prevent and manage conflicts of interest.

(31) Entities in charge of central registers are well placed to identify, in a rapid and efficient manner, the individuals who ultimately own or control legal entities and arrangements, including individuals designated in relation to targeted financial sanctions. Timely detection of ownership and control structures contributes to improving the understanding of the exposure to risks of non-implementation and evasion of targeted financial sanctions, and to the adoption of mitigating measures to reduce such risks. It is therefore important that entities in charge of central registers be required to screen the beneficial ownership information they hold against designations in relation to targeted financial sanctions, both immediately upon such designation and regularly thereafter, in order to detect whether changes in the ownership or control structure of the legal entity or legal arrangement are conducive to risks of evasion of targeted financial sanctions. An indication in the central registers that legal entities or legal arrangements are associated with persons or entities subject to targeted financial sanctions should contribute to the activities of competent authorities and of the authorities in charge of implementing Union restrictive measures.

(32) The reporting of discrepancies between beneficial ownership information held in the central registers and beneficial ownership information available to obliged entities and, where applicable, competent authorities, is an effective mechanism to verify the accuracy of the information. Any discrepancy identified should be swiftly reported and resolved, in line with data protection requirements.

(33) Where the reporting of discrepancies by FIUs and other competent authorities would jeopardise an analysis of a suspicious transaction or an on-going criminal investigation, the FIUs or other competent authorities should delay the reporting of the discrepancy until the moment at which the reasons for not reporting cease to exist. Furthermore, FIUs and other competent authorities should not report any discrepancy when this would be contrary to any confidentiality provision of national law or would constitute a tipping-off offence.

(34) To ensure a level playing field in the application of the concept of beneficial owner, it is essential that, across the Union, uniform reporting channels and means exist for legal entities and trustees of express trusts or persons holding an equivalent position in similar legal arrangements. To that end, the format for the submission of beneficial ownership information to the relevant central registers should be uniform and offer guarantees of transparency and legal certainty.

(35) In order to ensure a level playing field among the different types of legal forms, trustees should also be required to obtain and hold beneficial ownership information and to communicate that information to a central register or a central database.

(36) It is essential that the information on beneficial ownership remains available through the central registers and through the system of interconnection of central registers for a minimum of 5 years after the legal entity has been dissolved or the legal arrangement has ceased to exist. Member States should be able to provide by law additional grounds for the processing of beneficial ownership information for purposes other than AML/CFT, if such processing meets an objective of public interest and constitutes a necessary and proportionate measure in a democratic society to the legitimate aim pursued.

(37) FIUs, other competent authorities and self-regulatory bodies should have immediate, unfiltered, direct and free access to information on beneficial ownership for the purposes of preventing, detecting, investigating and prosecuting money laundering, its predicate offences or terrorist financing. Obliged entities should also have access to central registers when carrying out customer due diligence. Member States can choose to make access by obliged entities subject to the payment of a fee. However, those fees should be strictly limited to what is necessary to cover the costs of ensuring the quality of the information held in those registers and of making the information available, and should not undermine the effective access to beneficial ownership information.

(38) Direct, timely and unfiltered access to beneficial ownership information by national public authorities is also crucial to ensure the proper implementation of Union restrictive measures, to prevent the risk of non-implementation and evasion of Union restrictive measures, as well as to investigate breaches of those measures. For those reasons, authorities competent for the implementation of such restrictive measures, identified under the relevant Council Regulations adopted on the basis of Article 215 of the Treaty on the Functioning of the European Union (TFEU) should have direct and immediate access to the information held in the interconnected central registers.

(39) It should be possible for Union bodies, offices and agencies that play a role in the Union AML/CFT framework to access beneficial ownership information in the performance of their duties. This is the case for the European Public Prosecutor's Office (EPPO), but also for the European Anti-Fraud Office (OLAF) in the performance of its investigations, as well as for Europol and Eurojust when supporting investigations by national authorities. As a supervisory authority, AMLA is to be granted access to beneficial ownership information when performing supervisory activities. In order to ensure that AMLA can effectively support the activities of FIUs, it should also be able to access beneficial ownership information in the context of joint analyses.

(40) In order to limit interferences with the right to respect for private life and to protection of personal data, access to beneficial ownership information held in central registers by the public should be conditional upon the demonstration of a legitimate interest. Divergent approaches by Member States regarding the verification that such a legitimate interest exists could hamper the harmonised implementation of the AML/CFT framework and the preventive purpose for which such access by members of the public is allowed. It is therefore necessary to devise a framework for the recognition and verification of legitimate interest at Union level, in full respect of the Charter of Fundamental Rights of the European Union (the 'Charter'). Where a legitimate interest exists, the public should be able to access information on beneficial ownership of legal entities and legal arrangements. Legitimate interest should be presumed for certain categories of the public. Access on the basis of a legitimate interest should not be conditional upon the legal status or form of the person requesting access.

(41) Non-governmental organisations, academics and investigative journalists have contributed to the objectives of the Union in the fight against money laundering, its predicate offences and terrorist financing. They should therefore be considered to have a legitimate interest in accessing beneficial ownership information, which is of vital importance for them to undertake their functions and exert public scrutiny, as appropriate. The ability to access the central registers should not be conditional on the medium or platform through which they carry out their activities, or on previous experience in the field. In order to enable such categories to carry out their activities effectively and avoid risks of retaliation, they should be able to access information on legal entities and legal arrangements without demonstrating a link with those entities or arrangements. As provided for under Union data protection rules, any access by beneficial owners to information on the processing made of their personal data should not adversely affect the rights and freedoms of others, including the right to security of the person. Disclosure to the beneficial owner

that persons acting for the purposes of journalism or civil society organisations have consulted their personal data risks undermining the safety of journalists and of members of civil society organisations who carry out investigations into potential criminal activities. Therefore, in order to reconcile the right to the protection of personal data with the freedom of information and expression for journalists in accordance with Article 85 of Regulation (EU) 2016/679 of the European Parliament and of the Council ([15]) and in order to ensure the role of civil society organisations in the prevention, investigation and detection of money laundering, its predicate offences or terrorist financing in accordance with Article 23(1), point (d), of that Regulation, entities in charge of central registers should not share with beneficial owners information on the processing of their data by those categories of the public, but only the fact that persons acting for the purposes of journalism or civil society organisations have consulted their data.

(42) The integrity of business transactions is critical to the proper functioning of the internal market and of the Union's financial system. To that end, it is important that persons who wish to do business with legal entities or legal arrangements in the Union are able to access information on the beneficial owners of those entities or arrangements to verify that their potential business counterparts are not involved in money laundering, its predicate offences or terrorist financing. There is widespread evidence that criminals hide their identity behind corporate structures, and enabling those who could enter into transactions with a legal entity or legal arrangement to become aware of the identity of the beneficial owners contributes to combating the misuse of legal entities or legal arrangements for criminal purposes. A transaction is not limited to trading activities or the provision or buying of products or services, but might also include, situations where a person is likely to invest funds as defined in Article 4, point (25), of Directive (EU) 2015/2366 of the European Parliament and of the Council ([16]) or crypto-assets in the legal entity or legal arrangement, or to acquire the legal entity. Therefore, the requirement of legitimate interest to access beneficial ownership information should not be considered to be met only by persons carrying out economic or commercial activities.

(43) Given the cross-border nature of money laundering, its predicate offence and terrorist financing, it should be recognised that authorities of third countries have a legitimate interest in accessing beneficial ownership information on Union's legal entities and legal arrangements, where such access is needed by those authorities in the context of specific investigations or analyses to perform their tasks with respect to AML/CFT. Similarly, entities that are subject to AML/CFT requirements in third countries should be able to access the beneficial ownership information in the Union central registers when they are required to take customer due diligence measures in compliance with AML/CFT requirements in those countries in relation to legal entities and legal arrangements established in the Union. Any access to information contained in the central registers should be compliant with Union law on the protection of personal data, and in particular with Chapter V of Regulation (EU) 2016/679. To that end, central registers should also consider whether requests from persons established outside the Union can fall within the conditions within which a derogation under Article 49 of that Regulation can be availed of. It is settled case-law of the Court of Justice of the European Union (the 'Court of Justice') that the fight against money laundering, its predicate offences and terrorist financing is an objective of general public interest, and that public security objectives are connected to it. In order to preserve the integrity of investigations and analyses by third-country FIUs and law enforcement and judicial authorities, central registers should refrain from disclosing to the beneficial owners any processing of their personal data by those authorities insofar as such disclosure would adversely affect the investigations and analyses of those authorities. However, in order to preserve the data subject rights, the central registers should only refrain from disclosing that information until such disclosure would no longer jeopardise an investigation or analysis. That deadline should be set to a maximum period of 5 years, and should be extended only upon a justified request by the authority in the third country.

(44) In order to ensure an access regime which is sufficiently flexible and able to adapt to emerging new circumstances, Member States should be able to grant access to beneficial ownership information, on a case-by-case basis, to any person who can demonstrate a legitimate interest linked to the prevention and combating of money laundering, its predicate offences and terrorist financing. Member States should collect information about cases of legitimate interest that go beyond the categories identified in this Directive, and notify them to the Commission.

([15]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([16]) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

(45) Criminals can misuse legal entities at any point. However, certain phases in the lifecycle of legal entities are associated with higher risks, such as at the company formation stage, or when there are changes in the company structure, such as conversion, merger or division, which allow criminals to acquire control of the legal entity. The Union framework provides oversight by public authorities over those phases of a legal entity's existence under Directive (EU) 2017/1132 of the European Parliament and of the Council ([17]). In order to ensure that those public authorities can carry out their activities effectively and contribute to the prevention of the misuse of legal entities for criminal purposes, they should have access to the information contained in the interconnected central registers.

(46) With a view to ensuring the legality and regularity of expenditure included in the accounts submitted to the Commission under Union funding programmes, programme authorities have to collect and store in their management and control systems information on the beneficial owners of the recipients of Union funding. It is therefore necessary to ensure that programme authorities in Member States have access to beneficial ownership information held in the interconnected central registers to fulfil their duties to prevent, detect, correct and report on irregularities, including fraud, pursuant to Regulation (EU) 2021/1060 of the European Parliament and the Council ([18]).

(47) In order to protect Union's financial interests, Member State authorities implementing the Recovery and Resilience Facility under Regulation (EU) 2021/241 of the European Parliament and of the Council ([19]) should have access to the interconnected central registers to collect the beneficial ownership information on the recipient of Union funds or contractor required under that Regulation.

(48) Corruption in public procurement harms the public interest, undermines public trust and has a negative impact on the lives of citizens. Given the vulnerability of public procurement procedures to corruption, fraud and other predicate offences, it should be possible for national authorities with competences in public procurement procedures to consult the central registers to ascertain the identity of the natural persons who ultimately own or control the tenderers, and identify cases where there is a risk that criminals might be involved in the procurement procedure. Timely access to information held in the central register is crucial to ensuring that public authorities carrying out public procurement procedures can fulfil their functions effectively, including by detecting instances of corruption in those procedures. The notion of public authorities in relation to procurement procedures should encompass the concept of contracting authorities in Union legal acts relating to public procurement procedures for goods and services, or concessions as well as any public authority designated by Member States to verify the legality of public procurement procedures, which is not a competent authority for AML/CFT purposes.

(49) Products such as customer screening offered by third-party providers support obliged entities in the performance of customer due diligence. Such products provide them with a holistic view over the customer, which enables them to make informed decisions as to their risk classification, mitigating measures to be applied and possible suspicions regarding the customers' activities. Those products also contribute to the work of competent authorities in the analysis of suspicious transactions and investigations into potential cases of money laundering, its predicate offences and terrorist financing by complementing information on beneficial ownership with other technical solutions that enable competent authorities to have a broader view of complex criminal schemes, including through the localisation of perpetrators. They therefore play a critical role in tracing the increasingly complex and fast movements that characterise money laundering schemes. By virtue of their well-established function in the compliance infrastructure, it is justified to consider that providers offering those products hold a legitimate interest in accessing information held in the central registers, provided that the data obtained from the register are offered only to obliged entities and competent authorities in the Union for the performance of tasks related to preventing and fighting money laundering, its predicate offences and terrorist financing.

(50) In order to avoid divergent approaches towards the implementation of the concept of legitimate interest for the purpose of accessing beneficial ownership information, the procedures for the recognition of such a legitimate interest should be harmonised. This should include common templates for the application and recognition of

([17]) Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (OJ L 169, 30.6.2017, p. 46).

([18]) Regulation (EU) 2021/1060 of the European Parliament and of the Council of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund and the European Maritime, Fisheries and Aquaculture Fund and financial rules for those and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy (OJ L 231, 30.6.2021, p. 159).

([19]) Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility (OJ L 57, 18.2.2021, p. 17).

legitimate interest, which would facilitate mutual recognition by central registers across the Union. To that end, implementing powers should be conferred on the Commission to set out harmonised templates and procedures.

(51) To ensure that the processes for granting access to those with a previously verified legitimate interest are not unduly burdensome, access can be renewed on the basis of simplified procedures through which the entity in charge of the central register ensures that information previously obtained for purposes of verification are correct and relevant, and updated where necessary.

(52) Moreover, with the aim of ensuring a proportionate and balanced approach and to guarantee the rights to private life and personal data protection, Member States should provide for exemptions to the disclosure of the personal information on the beneficial owner through the central registers and to access to such information, in exceptional circumstances, where that information would expose the beneficial owner to a disproportionate risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation. It should also be possible for Member States to require online registration in order to identify any person who requests information from the central register, as well as the payment of a fee for access to the information in the register by persons with legitimate interest. However, those fees should be strictly limited to what is necessary to cover the costs of ensuring the quality of the information held in the central registers and of making the information available, and should not undermine the effective access to beneficial ownership information.

(53) The identification of applicants is necessary to ensure that only persons with a legitimate interest can access beneficial ownership information. However, the identification process should be carried out in such a way that it does not lead to discrimination, including based on the applicants' country of residence or nationality. To that end, Member States should provide sufficient identification mechanisms, including but not limited to electronic identification schemes notified under Regulation (EU) No 910/2014 of the European Parliament and of the Council ([20]), and relevant qualified trust services, to enable persons with a legitimate interest to effectively access beneficial ownership information.

(54) Directive (EU) 2018/843 achieved the interconnection of Member States' central registers holding beneficial ownership information through the European Central Platform established by Directive (EU) 2017/1132. The interconnection has proven to be essential for an effective cross-border access to the beneficial ownership information by competent authorities, obliged entities and persons with a legitimate interest. It will require continued development to implement the evolved regulatory requirements prior to the transposition of this Directive. Therefore, work on interconnection should continue with involvement of Member States in the functioning of the whole system, which should be ensured by means of a regular dialogue between the Commission and the representatives of Member States on the issues concerning the operation of the system and on its future development.

(55) Through the interconnection of the central registers, both national and cross-border access to information on the beneficial ownership of legal arrangements contained in each Member State central register should be granted based on the definition of legitimate interest, by virtue of a decision taken by the entity in charge of the relevant central register. To ensure that decisions on limiting access to beneficial ownership information can be reviewed, appeal mechanisms against such decisions should be established. With a view to ensuring coherent and efficient registration and information exchange, Member States should ensure that the entity in charge of the central register in their Member State cooperates with its counterparts in other Member States, including by sharing information concerning trusts and similar legal arrangements governed by the law of one Member State and administered in another Member State or whose trustee is established or resides in another Member State.

(56) Regulation (EU) 2016/679 applies to the processing of personal data for the purposes of this Directive. Natural persons whose personal data are held in central registers as beneficial owners should be informed about the applicable data protection rules. Furthermore, only personal data that is up to date and corresponds to the actual beneficial owners should be made available and the beneficial owners should be informed about

([20]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

their rights under the Union legal data protection framework and the procedures applicable for exercising those rights.

(57) Delayed access to information by FIUs and other competent authorities on the identity of holders of bank accounts and payment accounts, securities accounts, crypto-asset accounts and safe-deposit boxes hampers the detection of transfers of funds relating to money laundering and terrorist financing. It is therefore essential to establish centralised automated mechanisms, such as a register or data retrieval system, in all Member States as an efficient means to get timely access to information on the identity of holders of bank accounts and payment accounts, securities accounts, crypto-asset accounts and safe-deposit boxes, their proxy holders, and their beneficial owners. Such information should include the historical information on closed customer-account holders, bank accounts and payment accounts, including virtual IBANs, securities accounts, crypto-asset accounts and safe-deposit boxes. When applying the access provisions, it is appropriate for pre-existing mechanisms to be used provided that national FIUs can access the data for which they make inquiries in an immediate and unfiltered manner. Member States should consider feeding such mechanisms with other information deemed necessary and proportionate in order to achieve a more effective mitigation of risks relating to money laundering, its predicate offences and the financing of terrorism. Full confidentiality should be ensured in respect of such inquiries and requests for related information by FIUs, AMLA in the context of joint analyses and supervisory authorities.

(58) Virtual IBANs are virtual numbers issued by credit institutions and financial institutions that allow payments to be redirected to physical bank accounts or payment accounts. While virtual IBANs can be used by businesses for legitimate purposes, for example, to streamline the process of collecting and sending payments across borders, they are also associated with increased risks of money laundering, its predicate offences or terrorist financing as they can be used to obscure the identity of the account holder, making it difficult for FIUs to trace the flow of funds, identify the location of the account and impose the necessary measures, including the suspension or monitoring of the account. In order to mitigate those risks and facilitate the tracing and detection of illicit flows by FIUs, the centralised automated mechanisms should include information on virtual IBANs associated with a bank account or payment account.

(59) In order to respect privacy and protect personal data, the minimum data necessary for the carrying out of AML/CFT investigations should be held in centralised automated mechanisms for bank accounts or payment accounts, securities accounts and crypto-asset accounts. It should be possible for Member States to determine which additional data it is useful and proportionate to gather. When transposing the provisions relating to those mechanisms, Member States should set out retention periods equivalent to the period for retention of the documentation and information obtained within the application of customer due diligence measures. It should be possible for Member States to exceptionally extend the retention period, provided good reasons are given. The additional retention period should not exceed an additional 5 years. That period should be without prejudice to national law setting out other data retention requirements allowing case-by-case decisions to facilitate criminal or administrative proceedings. Access to those mechanisms should be on a need-to-know basis.

(60) Through the interconnection of Member States' centralised automated mechanisms, national FIUs would be able to obtain swiftly cross-border information on the identity of holders of bank accounts and payment accounts, securities accounts, crypto-asset accounts and safe deposit boxes in other Member States, which would reinforce their ability to effectively carry out financial analysis and cooperate with their counterparts from other Member States. Direct cross-border access to information on bank accounts and payment accounts, securities accounts, crypto-asset accounts and safe deposit boxes would enable FIUs to produce financial analysis within a sufficiently short timeframe to trace funds funnelled through various accounts, including by using virtual IBANs, detect potential money laundering and terrorist financing cases and guarantee a swift law enforcement action. AMLA should also be provided with direct access to the interconnected centralised automated mechanisms in order to provide operational support to FIUs in the framework of joint analysis exercises. Member States should ensure that direct access to the interconnected centralised automated mechanisms is extended to supervisory authorities to enable them to effectively perform their tasks.

(61) In order to respect the right to the protection of personal data and the right to privacy, and to limit the impact of cross-border access to the information contained in the national centralised automated mechanisms, the scope of information accessible through the bank account registers interconnection system ('BARIS') would be restricted to

the minimum necessary in accordance with the principle of data minimisation to allow the identification of any natural or legal persons holding or controlling bank accounts or payment accounts, securities accounts, crypto-asset accounts and safe-deposit boxes. FIUs and AMLA, as well as supervisory authorities, should be granted immediate and unfiltered access to BARIS. Member States should ensure that the staff of FIUs maintain high professional standards of confidentiality and data protection, and that they are of high integrity and are appropriately skilled. Moreover, Member States should put in place technical and organisational measures guaranteeing the security of the data to high technological standards.

(62) The interconnection of Member States' centralised automated mechanisms (central registries or central electronic data retrieval systems) containing information on bank accounts and payment accounts, securities accounts, crypto-asset accounts and safe-deposit boxes through BARIS necessitates the coordination of national systems having varying technical characteristics. For that purpose, technical measures and specifications taking into account the differences between the national centralised automated mechanisms should be developed.

(63) Real estate is an attractive commodity for criminals to launder the proceeds of their illicit activities, as it allows the true source of the funds and the identity of the beneficial owner to be obscured. The proper and timely identification of real estate, as well as of natural persons, legal entities and legal arrangements owning real estate by FIUs and other competent authorities is important both for detecting money laundering schemes as well as for freezing and confiscation of assets, as well as for administrative freezing measures implementing targeted financial sanctions. It is therefore important that Member States provide FIUs and other competent authorities with immediate and direct access to information which allows the proper conduct of analyses and investigations into potential criminal cases involving real estate. In order to facilitate effective access, that information should be provided free of charge through a single access point, by digital means and where possible in machine-readable format. The information should include historical information, including the history of real estate ownership, the prices at which the real estate has been acquired in the past and related encumbrances over a defined period in the past in order to enable FIUs and other competent authorities in that Member State to analyse and identify any suspicious activities pertaining to real estate, including land, property transactions which could be indicative of money laundering or other types of criminality. Such historical information concerns types of information already collected when carrying out real estate property transactions. Therefore, there are no new obligations imposed upon affected persons, ensuring that the legitimate expectations of those concerned are duly respected. Given the frequently cross-border nature of criminal schemes involving real estate, it is appropriate to identify a minimum set of information that competent authorities should be able to access and share with their counterparts in other Member States.

(64) Member States have in place or should set up operationally independent and autonomous FIUs to collect and analyse information, with the aim of establishing links between suspicious transactions and activities, and underlying criminal activity in order to prevent and combat money laundering and terrorist financing. The FIU should be the single central national unit responsible for the receipt and analysis of suspicious transaction reports, reports on cross-border physical movements of cash through the Customs Information System, on transactions reported when certain thresholds are exceeded (threshold-based disclosures) as well as other information relevant to money laundering, its predicate offences or terrorist financing submitted by obliged entities. Operational independence and autonomy of the FIU should be ensured by granting the FIU the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions as regards analysis, requests and dissemination of specific information. In all cases, the FIU should have the independent right to forward or disseminate information to relevant competent authorities. The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and enables it to exercise its mandate effectively. The FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence. In order to assess the fulfilment of those requirements and identify weaknesses and best practices, AMLA should be empowered to coordinate the organisation of peer reviews of FIUs.

(65) The staff of FIUs should be of high integrity and appropriately skilled, and should maintain high professional standards. FIUs should have in place procedures to effectively prevent and manage conflicts of interest. Given the nature of their work, FIUs are recipients of, and have access to, large amounts of sensitive personal and financial information. Therefore, the staff of FIUs should have appropriate skills when it comes to the ethical use of big data analytical tools. Moreover, the activities of FIUs might have implications for individuals' fundamental rights, such as

the right to the protection of personal data, right to private life and right to property. FIUs should therefore designate a Fundamental Rights Officer who can be a member of the existing staff of the FIU. The tasks of the Fundamental Rights Officer should include, without impeding or delaying the activities of the FIU, monitoring and promoting the FIU's compliance with fundamental rights, providing advice and guidance to the FIU on fundamental rights implications of its policies and practices, scrutinising the lawfulness and ethics of the FIU's activities and issuing non-binding opinions. The designation of a Fundamental Rights Officer would help to ensure that in carrying out their tasks, FIUs respect and protect fundamental rights of affected individuals.

(66) FIUs should be able to disseminate information to competent authorities tasked with combatting money laundering, its predicate offences, and terrorist financing. Such authorities should be understood to include authorities with an investigative, prosecutorial or judicial role. Across Member States, other authorities have dedicated roles connected to the fight against money laundering, its predicate offences and terrorist financing, and FIUs should also be able to provide them with the results of their operational or strategic analyses, where they consider those results to be relevant to their functions. The results of those analyses provide meaningful intelligence to be used for the development of leads in the course of investigative and prosecutorial work. The source of the suspicious transaction or activity report should not be disclosed in the dissemination. This, however, should not preclude FIUs from disseminating relevant information including, for example, information on IBAN numbers, BIC or SWIFT codes. In addition, FIUs should be able to share other information in their possession including upon request by other competent authorities. In exercising their autonomy and independence, FIUs should consider how a refusal to provide information could impact cooperation and the broader goal of combatting money laundering, its predicate offences and terrorist financing. Refusals should be limited to exceptional circumstances, for example when the information originates from another FIU that has not consented to its further dissemination, or where the FIU has reasons to believe that the information will not be used for the purposes for which it was requested. In such cases the FIU should provide reasons for the refusal. Such reasons could include clarifying that the information is not in the possession of the FIU or that consent for further dissemination has not been granted.

(67) Effective cooperation and information exchange between FIUs and supervisors is of crucial importance for the integrity and stability of the financial system. It ensures a comprehensive and consistent approach to preventing and combating money laundering, its predicate offences and terrorist financing, enhances the effectiveness of the Union AML/CFT regime and safeguards the economy from the threats posed by illicit financial activities. Information in the possession of FIUs pertaining to, for example, the quality and quantity of suspicious transaction reports submitted by obliged entities, the quality and timeliness of obliged entities' responses to requests for information by the FIUs, and information on money laundering, its predicate offences and terrorist financing typologies, trends and methods can help supervisors identify areas where risks are higher or where compliance is weak and thereby provide them with an insight into whether supervision needs to be strengthened in relation to specific obliged entities or sectors. To that end, FIUs should provide supervisors, either spontaneously or upon request, with certain types of information that could be relevant for the purposes of supervision.

(68) FIUs play an important role in identifying the financial operations of terrorist networks, especially cross-border, and in detecting their financial backers. Financial intelligence might be of fundamental importance in uncovering the facilitation of terrorist offences and the networks and schemes of terrorist organisations. FIUs maintain significant differences as regards their functions, competences and powers. The current differences should however not affect an FIU's activity, particularly its capacity to develop preventive analyses in support of all the authorities in charge of intelligence, investigative and judicial activities, and international cooperation. In the exercise of their tasks, it has become essential to identify the minimum set of data FIUs should have swift access to and be able to exchange without impediments with their counterparts from other Member States. In all cases of suspected money laundering, its predicate offences and terrorist financing, information should flow directly and quickly between FIUs without undue delay. It is therefore essential to further enhance the effectiveness and efficiency of FIUs, by clarifying the powers of and cooperation between FIUs.

(69) The powers of FIUs include the right to access, directly or indirectly, the 'financial', 'administrative' and 'law enforcement' information that they require in order to combat money laundering, its predicate offences and terrorist financing. The lack of definition of what types of information those general categories include has resulted in FIUs having been granted with access to considerably diversified sets of information which has an impact on FIUs' analytical functions as well as on their capacity to cooperate effectively with their counterparts from other Member States, including in the framework of joint analysis exercises. It is therefore necessary to define the minimum sets of 'financial', 'administrative' and 'law enforcement' information that should be made directly or indirectly available to every FIU across the Union. FIUs also receive and store in their databases, or have access to, information related to transactions that are reported when specified thresholds are exceeded (threshold-based reports). Those reports are an important source of information and are widely used by FIUs in the context of domestic and joint analyses. Therefore, threshold-based reports are among the types of information exchanged through FIU.net. Direct access is an important prerequisite for the operational effectiveness and responsiveness of FIUs. To that end, it should be possible for Member States to provide FIUs with direct access to a broader set of information than those required by this Directive. At the same time, this Directive does not require Member States to set up new databases or registers in the cases where certain types of information, for example, information on procurement, is spread across various repositories or archives. Where a database or register has not been set up, Member States should take other necessary measures to ensure that FIUs can obtain that information in an expeditious manner. Moreover, FIUs should be able to obtain swiftly from any obliged entity all necessary information relating to their functions. An FIU should also be able to obtain such information upon request made by another FIU and to exchange that information with the requesting FIU.

(70) Access should be considered direct and immediate when the information is contained in a database, register or an electronic data retrieval system enabling the FIU to obtain it directly, through an automated mechanism, without the involvement of an intermediary. Where the information is held by another entity or authority, direct access entails that those authorities or entities transmit it to the FIU in an expeditious manner without interfering with the content of the requested data or the information to be provided. The information should not undergo any filtering. In some situations, however, the confidentiality requirements attached to the information might not allow the provision of the information in an unfiltered manner. This is the case, for example, where tax information can only be provided to FIUs upon agreement of a tax authority in a third country, where direct access to law enforcement information could jeopardise an ongoing investigation, as well as in relation to passenger name record data collected pursuant to Directive (EU) 2016/681 of the European Parliament and of the Council ([21]). In such cases, Member States should make every effort to ensure effective access to the information by FIUs, including by allowing FIUs to have access under similar conditions to those offered to other authorities at national level to facilitate their analytical activities.

(71) The vast majority of FIUs have been granted the power to take urgent action and suspend or withhold consent to a transaction in order to perform the analyses, confirm the suspicion and disseminate the results of the analytical activities to the competent authorities. However, there are certain variations in relation to the duration of the suspension powers across Member States, with an impact not only on the postponement of activities that have a cross-border nature through FIU-to-FIU cooperation, but also on individuals' fundamental rights. Furthermore, in order to ensure that FIUs have the capacity to promptly restrain criminal funds or assets and prevent their dissipation, also for seizure purposes, FIUs should be granted the power to suspend the use of a bank account or payment account, crypto-asset account or a business relationship in order to analyse the transactions performed through the account or business relationship, confirm the suspicion and disseminate the results of the analysis to the relevant competent authorities. Given that such suspension would have an impact on the right to property, FIUs should be able to suspend transactions, accounts or business relationships for a limited period in order to preserve the funds, carry out the necessary analyses and disseminate the results of the analyses to the competent authorities for the possible adoption of appropriate measures. Given the more significant impact on an affected person's fundamental rights, the suspension of an account or business relationship should be imposed for a more limited period, which should be set at 5 working days. Member States can define a longer period of suspension where, pursuant to national law, the FIU exercises competences in the area of asset recovery and carries out functions of tracing, seizing, freezing or confiscating criminal assets. In such cases, the preservation of affected persons' fundamental rights should be guaranteed and FIUs should exercise their functions in accordance with the appropriate national safeguards. FIUs should lift the suspension of the transaction, account or business relationship

([21]) Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016, p. 132).

as soon as such suspension is no longer necessary. Where a longer suspension period is defined, affected persons whose transactions, accounts or business relationships have been suspended should have the possibility to challenge the suspension order before a court.

(72) In specific circumstances, FIUs should be able to request, on their own behalf or on behalf of another FIU, an obliged entity to monitor, for a defined period, transactions or activities carried out through a bank account or payment account or crypto-asset account or another type of business relationship in relation to persons presenting a significant risk of money laundering, its predicate offences or terrorist financing. Closer monitoring of an account or a business relationship can provide the FIU with additional insights into the account holder's transaction patterns and lead to the timely detection of unusual or suspicious transactions or activities that might warrant further action by the FIU, including the suspension of the account or the business relationship, the analysis of the intelligence gathered and its dissemination to investigative and prosecutorial authorities. FIUs should also be able to alert obliged entities of information relevant to the performance of customer due diligence. Such alerts can help obliged entities to inform their customer due diligence procedures and ensure their consistency with risks, update their risk assessment and risk management systems accordingly and provide them with additional information that might trigger the need for enhanced due diligence on certain customers or transactions that present higher risks.

(73) For the purposes of greater transparency and accountability and to increase awareness with regard to their activities, FIUs should issue activity reports on an annual basis. Those reports should at least provide statistical data in relation to the suspicious transaction reports received and the follow-up given, the number of disseminations made to national competent authorities and the follow-up provided to those disseminations, the number of requests submitted to and received by other FIUs as well as information on trends and typologies identified. Those reports should be made public except for the parts thereof which contain sensitive and classified information.

(74) At least once per year, the FIU should provide obliged entities with feedback on the quality of suspicious transaction reports, their timeliness, the description of suspicion and any additional documents provided. Such feedback can be provided to individual obliged entities or groups of obliged entities and should aim to further improve the obliged entities' ability to detect and identify suspicious transactions and activities, improve the quality of suspicious transaction reports, enhance the overall reporting mechanisms and provide obliged entities with important insights into trends, typologies and risks associated with money laundering, its predicate offences and terrorist financing. When determining the type and frequency of the feedback, FIUs should, insofar as possible, take into account areas where improvements in reporting activities might be needed. In order to support a consistent approach across FIUs and adequate feedback to obliged entities, AMLA should issue recommendations to FIUs on best practices and approaches towards providing feedback. Where this would not jeopardise analytical or investigative work, FIUs could consider providing feedback on the use made or outcome of suspicious transaction reports, whether on individual reports or in an aggregated manner. FIUs should also provide customs authorities with feedback, at least once per year, on the effectiveness and follow-up to reports on cross-border physical movements of cash.

(75) The purpose of the FIU is to collect and analyse information with the aim of establishing links between suspicious transactions or activities, and underlying criminal activity in order to prevent and combat money laundering and terrorist financing, and to disseminate the results of its analysis as well as additional information to the competent authorities where there are grounds to suspect money laundering, its predicate offences or terrorist financing. An FIU should not refrain from or refuse the exchange of information to another FIU, spontaneously or upon request, for reasons such as a lack of identification of a predicate offence, features of criminal national laws and differences between the definitions of predicate offences or the absence of a reference to particular predicate offences. FIUs have reported difficulties in exchanging information based on differences in national definitions of certain predicate offences, such as tax crimes, which are not harmonised by Union law. Such differences should not hamper the mutual exchange, the dissemination to other competent authorities and the use of that information. FIUs should rapidly, constructively and effectively ensure the widest range of international cooperation with third countries' FIUs in relation to money laundering, its predicate offences and terrorist financing in accordance with the applicable data protection rules for data transfers, FATF Recommendations and Egmont Principles for Information Exchange between Financial Intelligence Units. To that end, FIUs should be encouraged to conclude bilateral agreements and memoranda of understanding with counterparts from third countries, while taking account of any fundamental rights obligations and of the need to protect the rule of law.

(76) An FIU can impose certain restrictions and limitations with regard to the further use of information it provides to another FIU. The recipient FIU should use the information only for the purposes for which it was sought or provided. An FIU should grant its prior consent to another FIU to forward the information to other competent authorities regardless of the type of possible predicate offence and regardless of whether the predicate offence has been identified at the time of the exchange, in order to allow the dissemination function to be carried out effectively. Such prior consent to further dissemination should be granted promptly and should not be refused unless it would fall beyond the scope of application of the AML/CFT provisions or would not be in accordance with fundamental principles of national law. FIUs should provide an explanation regarding any refusal to grant consent.

(77) FIUs should use secure facilities, including protected channels of communication, to cooperate and exchange information amongst each other. In this respect, a system for the exchange of information between FIUs of Member States (FIU.net) should be set up. The system should be managed and hosted by AMLA and should provide for the highest level of security and the full encryption of the information exchanged. FIU.net should be used by FIUs to cooperate and exchange information amongst each other and could also be used, where appropriate and subject to a decision by AMLA, to exchange information with FIUs of third countries and with other authorities and Union bodies, offices and agencies. The functionalities of the FIU.net should be used by FIUs to their full potential. Those functionalities should allow FIUs to match their data with data of other FIUs in a pseudonymous manner, with the aim of detecting subjects of the FIU's interests in other Member States and identifying their proceeds and funds, whilst ensuring full protection of personal data. In order to identify links between financial information and criminal intelligence, FIUs should also be able to use the functionalities of FIU.net to pseudonymously cross-match their data with information held by Union bodies, offices and agencies insofar as such cross-matching falls within the latter's respective legal mandates and in full respect of the applicable data protection rules.

(78) It is important that FIUs cooperate and exchange information effectively with one another. In that regard, AMLA should provide the necessary assistance, not only by means of coordinating joint analyses of cross-border suspicious transaction reports, but also by developing draft implementing and regulatory technical standards concerning the format to be used for the exchange of information between FIUs, the template for the submission of suspicious transaction reports and the relevance and selection criteria to be taken into account when determining whether a suspicious transaction report concerns another Member State as well as guidelines on the nature, features and objectives of operational and of strategic analysis and on the procedures to be put in place when forwarding and receiving a suspicious transaction report which concerns another Member State and the follow-up to be given. AMLA should also set up a peer review process in order to strengthen consistency and effectiveness of FIUs' activities and to facilitate the exchange of best practices between FIUs.

(79) FIUs are responsible for receiving suspicious transaction or activity reports from obliged entities established in the territory of their Member States. Certain suspicious transactions or activities reported to FIUs might however pertain to activities carried out by obliged entities in other Member States, where they operate without an establishment. In those cases, it is important that FIUs disseminate those reports to their counterpart in the Member State concerned by the transaction or activity, without attaching conditions to the use of those reports. The FIU.net system enables the dissemination of such cross-border reports. In order to enhance that functionality, the system is undergoing upgrades to enable the fast dissemination of such reports and to support significant exchanges of information between FIUs, and thereby the effective implementation of this Directive.

(80) Time limits for exchanges of information between FIUs are necessary in order to ensure quick, effective and consistent cooperation. Time limits should be set out in order to ensure effective sharing of information within a reasonable time or to meet procedural constraints. Shorter time limits should be provided in exceptional, justified and urgent cases where the requested FIU is able to access directly the databases where the requested information is held. In cases where the requested FIU is not able to provide the information within the time limit, it should inform the requesting FIU thereof.

(81) The movement of illicit money traverses borders and can affect different Member States. The cross-border cases, involving multiple jurisdictions, are becoming increasingly frequent and significant, also due to the activities carried out by obliged entities on a cross-border basis. In order to deal effectively with cases that concern several Member States, FIUs should be able to go beyond the simple exchange of information for the detection and analysis

of suspicious transactions and activities and carry out jointly the analytical activity itself. FIUs have reported certain important issues which limit or condition the capacity of FIUs to engage in joint analysis. Carrying out joint analysis of suspicious transactions and activities will enable FIUs to exploit potential synergies, to use information from different sources, to obtain a full picture of the anomalous activities and to enrich the analysis. FIUs should be able to conduct joint analyses of suspicious transactions and activities and to set up and participate in joint analysis teams for specific purposes and limited period with the assistance of AMLA. AMLA should use the FIU.net system in order to be able to send, receive and cross-match information and provide operational support to FIUs in the context of the joint analysis of cross-border cases.

(82) The participation of third parties, including Union bodies, offices and agencies, might be instrumental to the successful outcome of FIUs' analyses, including joint analyses. Therefore, FIUs can invite third parties to take part in the joint analysis where such participation would fall within the respective mandates of those third parties. Participation by third parties in the analytical process could help identify links between financial intelligence and criminal information and intelligence, enrich the analysis, and determine if there are indications that a criminal offence has been committed.

(83) Effective supervision of all obliged entities is essential to protect the integrity of the Union financial system and of the internal market. To that end, Member States should deploy effective and impartial AML/CFT supervision and set out the conditions for effective, timely and sustained cooperation between supervisors.

(84) Member States should ensure effective, impartial and risk-based supervision of all obliged entities, preferably by public authorities via a separate and independent national supervisor. National supervisors should be able to perform a comprehensive range of tasks in order to exercise effective supervision of all obliged entities.

(85) The Union has witnessed on occasions a lax approach to the supervision of the obliged entities' duties in terms of anti-money laundering and counter-terrorist financing duties. Therefore, it is necessary that national supervisors, as part of the integrated supervisory mechanism put in place by this Directive and Regulation (EU) 2024/1620, obtain clarity as to their respective rights and obligations.

(86) In order to assess and monitor more effectively and regularly the risks obliged entities are exposed to and the internal policies, procedures and controls they put in place to manage and mitigate those risks, and to implement targeted financial sanctions, it is necessary to clarify that national supervisors are both entitled and bound to conduct all the necessary off-site, on-site and thematic checks and any other inquiries and assessments as they see necessary. They should also be able to react without undue delay to any suspicion of non-compliance with applicable requirements and take appropriate supervisory measures to address allegations of non-compliance. This will not only help supervisors decide on those cases where the specific risks inherent in a sector are clear and understood, but also provide them with the tools required to further disseminate relevant information to obliged entities in order to inform their understanding of money laundering and terrorist financing risks.

(87) Outreach activities, including the dissemination of information by the supervisors to the obliged entities under their supervision, is essential to guarantee that the private sector has an adequate understanding of the nature and level of money laundering and terrorist financing risks they face. This includes disseminations of designations under targeted financial sanctions and UN financial sanctions, which should take place immediately once such designations are made in order to enable the sector to comply with their obligations. As the implementation of AML/CFT requirements by obliged entities involves the processing of personal data, it is important that supervisors are cognisant of guidance and other publications issued by the data protection authorities, either at national level or at Union level through the European Data Protection Board, and that they include that information, as appropriate, in their disseminations to the entities under their supervision.

(88) Supervisors should adopt a risk-based approach to their work, which would enable them to focus their resources where the risks are the highest, whilst ensuring that no sector or entity is left exposed to criminal attempts to launder money or finance terrorism. To that end, supervisors should plan their activities on an annual basis. In doing so, they should not only ensure risk-based coverage of the sectors under their supervision, but also that they are able to react promptly in the event of objective and significant indications of breaches within an obliged entity, including in particular following public revelations or information submitted by whistleblowers. Supervisors should also ensure transparency with respect to the supervisory activities they have carried out, such as supervisory colleges they organised and attended, on-site and off-site supervisory actions taken, pecuniary sanctions imposed or

administrative measures applied. AMLA should play a leading role in fostering a common understanding of risks, and should therefore be entrusted with developing the benchmarks and a methodology for assessing and classifying the inherent and residual risk profile of obliged entities, as well as the frequency at which such risk profile should be reviewed.

(89) The disclosure to FIUs of facts that could be related to money laundering or to terrorist financing by supervisors is one of the cornerstones of efficient and effective supervision of money laundering and terrorist financing risks, and it allows supervisors to address shortcomings in the reporting process of obliged entities. To that effect, supervisors should be able to report to the FIU instances of suspicions that the obliged entity failed to report or to complement reports submitted by the obliged entity with additional information, which they detect in the course of their supervisory activities. Supervisors should also be able to report suspicions of money laundering, its predicate offences or terrorist financing by the employees of obliged entities, or persons in an equivalent position, by its management or its beneficial owners. It is therefore necessary for Member States to put in place a system that ensures that FIUs are properly and promptly informed. The reporting of suspicions to the FIU should not be understood as replacing the obligation for public authorities to report to the relevant competent authorities any criminal activity they uncover or become aware of in the course of performing their tasks. Information covered by the legal privilege should not be collected or consulted in the context of supervisory tasks, unless the exemptions set out in Regulation (EU) 2024/1624 apply. If supervisors come across or into possession of such information, they should not take it into account for the purposes of their supervisory activities or report it to the FIU.

(90) Cooperation between national supervisors is essential to ensure a common supervisory approach across the Union. To be effective, that cooperation has to be used to the greatest extent possible and regardless of the respective nature or status of the supervisors. In addition to traditional cooperation — such as the ability to conduct investigations on behalf of a requesting supervisory authority — it is appropriate to mandate the set-up of AML/CFT supervisory colleges in the financial sector with respect to obliged entities that operate in several Member States through establishments and with respect to obliged entities which are part of a cross-border group. Third-country financial supervisors can be invited to those colleges under certain conditions, including confidentiality requirements equivalent to those incumbent on Union financial supervisors and compliance with Union law regarding the processing and transmission of personal data. The activities of AML/CFT supervisory colleges should be proportionate to the level of risk to which the credit institution or financial institution is exposed, and the scale of cross-border activity.

(91) Directive (EU) 2015/849 included a general requirement for supervisors of home and host Member States to cooperate. That requirement was subsequently strengthened to avoid the exchange of information and cooperation between supervisors being prohibited or unreasonably restricted. However, in the absence of a clear legal framework, the set-up of AML/CFT supervisory colleges has been based on non-binding guidelines. It is therefore necessary to establish clear rules for the organisation of AML/CFT colleges and to provide for a coordinated, legally sound approach, recognising the need for structured interaction between supervisors across the Union. In line with its coordinating and oversight role, AMLA should be entrusted with developing the draft regulatory technical standards defining the general conditions that enable the proper functioning of AML/CFT supervisory colleges.

(92) Obliged entities operating in the non-financial sector might also carry out activities across borders or be part of groups that carry out cross-border activities. It is therefore appropriate to lay down rules that define the functioning of AML/CFT supervisory colleges for groups carrying out both financial and non-financial activities, and that enable the setting-up of supervisory colleges in the non-financial sector, taking into account the need to apply additional safeguards in relation to groups or cross-border entities providing legal services. In order to ensure effective cross-border supervision in the non-financial sector, AMLA should provide support to the functioning of such colleges and regularly provide its opinion on the functioning of those colleges as implementation of the enabling framework provided by this Directive progresses.

(93) Where an obliged entity operates establishments in another Member State, including through a network of agents, the supervisor of the home Member State should be responsible for supervising the obliged entity's application of group-wide AML/CFT policies and procedures. This could involve on-site visits in establishments based in another Member State. The supervisor of the home Member State should cooperate closely with the supervisor of the host

Member State and should inform it of any issues that could affect their assessment of the establishment's compliance with the AML/CFT rules of the host Member State.

(94) Where an obliged entity operates establishments in another Member State, including through a network of agents, the supervisor of the host Member State should retain responsibility for enforcing the establishment's compliance with AML/CFT rules, including, where appropriate, by carrying out on-site inspections and off-site monitoring and by taking appropriate and proportionate measures to address breaches of those requirements. The same should apply to other types of infrastructure of obliged entities that operate under the freedom to provide services, where that infrastructure is sufficient to require supervision by the supervisor of the host Member State. The supervisor of the host Member State should cooperate closely with the supervisor of the home Member State and should inform it of any issues that could affect its assessment of the obliged entity's application of AML/CFT policies and procedures, and allow the supervisor of the home Member State to take measures to address any breach identified. However, where serious, repeated or systematic breaches of AML/CFT rules that require immediate remedies are detected, the supervisor of the host Member State should be able to apply appropriate and proportionate temporary remedial measures, applicable under similar circumstances to obliged entities under their competence, to address such serious, repeated or systematic breaches, where appropriate, with the assistance of, or in cooperation with, the supervisor of the home Member State.

(95) In areas that are not harmonised at Union level, Member States can adopt national measures, even when those measures constitute restrictions to the freedoms of the internal market. This is the case, for example, of measures taken to regulate the provision of gambling services, particularly when those activities are carried out online, without any infrastructure in the Member State. However, to be compatible with Union law, such measures need to attain a general interest, be non-discriminatory and suitable for achieving that objective, and must not go beyond what is strictly necessary to achieve it. Where Member States subject the provision of services that are regulated under the Union AML/CFT framework to specific authorisation requirements, such as the obtention of a licence, they should also be responsible for the supervision of those services. The requirement to supervise those services does not prejudge the conclusions that the Court of Justice might draw on the compatibility of national measures with Union law.

(96) In light of anti-money laundering vulnerabilities related to electronic money issuers, payment service providers and crypto-assets service providers, it should be possible for Member States to require that those providers established on their territory in forms other than a branch or through other types of infrastructure and the head office of which is located in another Member State appoint a central contact point. Such a central contact point, acting on behalf of the appointing institution, should ensure the establishments' compliance with AML/CFT rules.

(97) To ensure better coordination of efforts and contribute effectively to the needs of the integrated supervisory mechanism, the respective duties of supervisors in relation to obliged entities operating in other Member States through establishments or forms of infrastructure justifying supervision by the host Member State should be clarified, and specific, proportionate cooperation mechanisms should be provided for.

(98) Cross-border groups need to have in place far-reaching group-wide policies and procedures. To ensure that cross-border operations are matched by adequate supervision, it is necessary to set out detailed supervisory rules, enabling supervisors of the home Member State and those of the host Member State to cooperate with each other to the greatest extent possible, regardless of their respective nature or status, and with AMLA to assess risks and monitor developments that could affect the various entities that form part of the group, coordinate supervisory action and settle disputes. Given its coordinating role, AMLA should be entrusted with the duty to develop the draft regulatory technical standards defining the detailed respective duties of the home and host supervisors of groups, and the arrangements for cooperation between them. The supervision of the effective implementation of group policy on AML/CFT should be done in accordance with the principles and methods of consolidated supervision as laid down in the relevant Union sectoral legal acts.

(99) Exchange of information and cooperation between supervisors is essential in the context of increasingly integrated global financial systems. On the one hand, Union supervisors, including AMLA, should inform each other of instances in which the law of a third country does not permit the implementation of the policies and procedures required under Regulation (EU) 2024/1624. On the other hand, it should be possible for Member States to authorise supervisors to conclude cooperation agreements providing for cooperation and exchanges of confidential

information with their counterparts in third countries, in compliance with applicable rules for personal data transfers. Given its oversight role, AMLA should provide assistance as might be necessary to assess the equivalence of professional secrecy requirements applicable to the third-country counterpart.

(100) Directive (EU) 2015/849 allows Member States to entrust the supervision of some obliged entities to self-regulatory bodies. However, the quality and intensity of supervision performed by such self-regulatory bodies has been insufficient, and under no, or close to no, public scrutiny. Where a Member State decides to entrust supervision to a self-regulatory body, it should also designate a public authority to oversee the activities of the self-regulatory body to ensure that the performance of those activities is in line with this Directive. That public authority should be a public administration entity and should perform its functions free of undue influence. The functions to be exercised by the public authority overseeing self-regulatory bodies do not imply that the authority should exercise supervisory functions vis-à-vis obliged entities, or take decisions in individual cases handled by the self-regulatory body. However, this does not prevent Member States from allocating additional tasks to that authority if they deem it necessary to achieve the objectives of this Directive. When doing so, Member States should ensure that additional tasks are in line with fundamental rights, and in particular that those tasks do not interfere with the exercise of the right of defence and the confidentiality of lawyer-client communication.

(101) The importance of combating money laundering and terrorist financing should result in Member States laying down effective, proportionate and dissuasive pecuniary sanctions and administrative measures in national law for failure to comply with Regulation (EU) 2024/1624. National supervisors should be empowered by Member States to apply such administrative measures to obliged entities to remedy the situation in the case of breaches and, where the breach so justifies, impose pecuniary sanctions. Depending on the organisational systems in place in Member States, such measures and sanctions could also be applied in cooperation between supervisors and other authorities, by delegation from the supervisors to other authorities or by application by the supervisors to judicial authorities. The pecuniary sanctions and administrative measures should be sufficiently broad to allow Member States and supervisors to take account of the differences between obliged entities, in particular between credit institutions and financial institutions and other obliged entities, as regards their size, characteristics and the nature of the business.

(102) Member States currently have a diverse range of pecuniary sanctions and administrative measures for breaches of the key preventative provisions in place and an inconsistent approach to investigating and sanctioning violations of anti-money laundering requirements. Moreover, there is no common understanding among supervisors as to what should constitute a 'serious' violation and thus they cannot readily discern when a pecuniary sanction should be imposed. That diversity is detrimental to the efforts made in combating money laundering and terrorist financing and the Union's response is fragmented. Therefore, common criteria for determining the most appropriate supervisory response to breaches should be laid down and a range of administrative measures that the supervisors could apply to remedy breaches, whether in combination with pecuniary sanctions or, when the breaches are not sufficiently serious to be punished with a pecuniary sanction, on their own, should be provided. In order to incentivise obliged entities to comply with the provisions of Regulation (EU) 2024/1624, it is necessary to strengthen the dissuasive nature of pecuniary sanctions. Accordingly, the minimum amount of the maximum penalty that can be imposed in the case of serious breaches of Regulation (EU) 2024/1624 should be raised. In transposing this Directive, Member States should ensure that the imposition of pecuniary sanctions and application of administrative measures, and the imposition of criminal sanctions in accordance with national law, does not breach the principle of ne bis in idem.

(103) In the case of obliged entities that are legal persons, breaches of AML/CFT requirements occur following action by, or under the responsibility of the natural persons who have the power to direct its activities, including through agents, distributors or other persons acting on behalf of the obliged entity. In order to ensure that supervisory action in response to such breaches is effective, the obliged entity should also be held liable for actions taken by those natural persons, whether carried out intentionally or negligently. Without prejudice to the liability of legal persons in criminal proceedings, any intent to derive a benefit for the obliged entity from breaches points to wider failures in the internal policies, procedures and controls of the obliged entity to prevent money laundering, its predicate offences and terrorist financing. Such failures undermine the obliged entity's role as gatekeeper of the Union's financial system. Any intent to derive benefit from a breach of AML/CFT requirement should therefore be taken as an aggravating circumstance.

(104) Member States have different systems in place for the imposition of pecuniary sanctions, application of administrative measures and imposition of periodic penalty payments. In addition, certain administrative measures that supervisors are empowered to apply, such as the withdrawal or suspension of a licence, are dependent on the execution of those measures by other authorities. In order to cater for such a diverse range of situations, it is appropriate to allow flexibility as regards the means that supervisors have to impose pecuniary sanctions, apply administrative measures and impose periodic penalty payments. Regardless of the means chosen, it is incumbent on Member States and the authorities involved to ensure that the mechanisms implemented achieve the intended result of restoring compliance and impose effective, dissuasive and proportionate pecuniary sanctions.

(105) With a view to ensuring that obliged entities comply with AML/CFT requirements and effectively mitigate the risks of money laundering, its predicate offences and terrorist financing to which they are exposed, supervisors should be able to apply administrative measures not only to remedy identified breaches, but also where they identify that weaknesses in the internal policies, procedures and controls are likely to result in breaches of AML/CFT requirements, or where those policies, procedures and controls are inadequate to mitigate risks. The scope of administrative measures applied, and the timing granted to obliged entities to implement the requested actions, depend on the specific breaches or weaknesses identified. Where multiple breaches or weaknesses are identified, different deadlines might apply for the implementation of each individual administrative measure. Consistent with the punitive and educational goal of publications, only decisions to apply administrative measures in relation to breaches of AML/CFT requirements should be published, but not administrative measures applied to prevent such breach.

(106) Timely compliance by obliged entities with administrative measures applied to them is essential to ensure an adequate and consistent level of protection against money laundering, its predicate offences and terrorist financing across the internal market. Where obliged entities fail to comply with administrative measures within the deadline set, it is necessary that supervisors are able to apply enhanced pressure on the obliged entity to restore compliance without delay. To that end, it should be possible for supervisors to impose periodic penalty payments as of the deadline set for restoring compliance, including with retroactive effect when the decision imposing the periodic penalty payment is taken at a later stage. In calculating the amounts of periodic penalty payments, supervisors should take into account the overall turnover of the obliged entity and the type and gravity of the breach or weakness targeted by the supervisory measure to ensure its effectiveness and proportionality. Given their goal of pressuring an obliged entity into complying with an administrative measure, periodic penalty payments should be limited in time and apply for no longer than 6 months. While it should be possible for supervisors to renew the imposition of periodic penalty payments for another 6 months maximum, alternative measures to address an extended situation of non-compliance should be considered, consistent with the wide range of administrative measures that supervisors can apply.

(107) Where the legal system of the Member State does not allow the imposition of pecuniary sanctions provided for in this Directive by administrative means, the rules on pecuniary sanctions can be applied in such a manner that the penalty is initiated by the supervisor and imposed by judicial authorities. Therefore, it is necessary that those Member States ensure that the application of the rules and pecuniary sanctions has an effect equivalent to the pecuniary sanctions imposed by the supervisors. When imposing such pecuniary sanctions, judicial authorities should take into account the recommendation by the supervisor initiating the penalty. The pecuniary sanctions imposed should be effective, proportionate and dissuasive.

(108) Obliged entities can benefit from the freedom to provide services and to establish across the internal market to offer their products and services across the Union. An effective supervisory system requires that supervisors are aware of the weaknesses in obliged entities' compliance with AML/CFT rules. It is therefore important that supervisors are able to inform one another of pecuniary sanctions imposed on, and administrative measures applied to obliged entities, when such information would be relevant for other supervisors.

(109) Publication of a pecuniary sanction or administrative measure for breach of Regulation (EU) 2024/1624 can have a strong dissuasive effect against repetition of such a breach. It also informs other entities of the money laundering and terrorist financing risks associated with the sanctioned obliged entity before entering into a business relationship and assists supervisors in other Member States in relation to the risks associated with an obliged entity when it operates in their Member State on a cross-border basis. For those reasons, the requirement to publish decisions on pecuniary sanctions against which there is no appeal should be confirmed, and should be extended to the publication of certain administrative measures that are applied to remedy breaches of AML/CFT requirements and to periodic penalty payments. However, any such publication should be proportionate and, in the taking of a decision whether to publish a pecuniary sanction or administrative measure, supervisors should take into account the gravity

of the breach and the dissuasive effect that the publication is likely to achieve. To that end, Member States might decide to delay the publication of administrative measures against which there is an appeal when those measures are applied to remedy a breach that is not serious, repeated or systematic.

(110) Directive (EU) 2019/1937 of the European Parliament and of the Council ([22]) applies to the reporting of breaches of Directive (EU) 2015/849 relating to money laundering and terrorist financing and to the protection of persons reporting such breaches, as referred to in Part II of the Annex to Directive (EU) 2019/1937. Since this Directive repeals Directive (EU) 2015/849, the reference to Directive (EU) 2015/849 in Annex II to Directive (EU) 2019/1937 should be understood as a reference to this Directive. At the same time, it is necessary to maintain tailored rules on the reporting of breaches of AML/CFT requirements that complement Directive (EU) 2019/1937, in particular, as regards the requirements for obliged entities to establish internal reporting channels and the identification of authorities competent to receive and follow-up on reports relating to breaches of rules relating to the prevention and fight against money laundering and terrorist financing.

(111) It is essential to have a new fully-integrated and coherent AML/CFT policy at Union level, with designated roles for both Union and national competent authorities and with a view to ensure their smooth and constant cooperation. In that regard, cooperation between all national and Union AML/CFT authorities is of the utmost importance and should be clarified and enhanced. It remains the duty of Member States to provide for the necessary rules to ensure that at national level policy makers, the FIUs, supervisors, including AMLA, and other competent authorities involved in AML/CFT, as well as tax authorities and law enforcement authorities when acting within the scope of this Directive, have effective mechanisms to enable them to cooperate and coordinate, including through a restrictive approach to the refusal by competent authorities to cooperate and exchange information at the request of another competent authority. Irrespective of the mechanisms put in place, such national cooperation should result in an effective system to prevent and combat money laundering, its predicate offences and terrorist financing, and to prevent the non-implementation and evasion of targeted financial sanctions.

(112) In order to facilitate and promote effective cooperation, and in particular the exchange of information, Member States should be required to communicate to the Commission and AMLA the list of their competent authorities and relevant contact details.

(113) The risk of money laundering and terrorist financing can be detected by all supervisors in charge of credit institutions. Information of a prudential nature relating to credit institutions and financial institutions, such as information relating to the fitness and properness of directors and shareholders, to the internal control mechanisms, to governance or to compliance and risk management, is often indispensable for the adequate AML/CFT supervision of such institutions. Similarly, AML/CFT information is also important for the prudential supervision of such institutions. Therefore, cooperation and exchange of information with AML/CFT supervisors and FIU should be extended to all competent authorities in charge of the supervision of those obliged entities in accordance with other Union legal instruments, such as Directives 2013/36/EU ([23]), 2014/49/EU ([24]), 2014/59/EU ([25]) and 2014/92/EU ([26]) of the European Parliament and of the Council and Directive (EU) 2015/2366. To ensure the effective implementation of that cooperation, Member States should inform AMLA annually of the exchanges carried out.

([22]) Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, p. 17).

([23]) Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

([24]) Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes (OJ L 173, 12.6.2014, p. 149).

([25]) Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190).

([26]) Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (OJ L 257, 28.8.2014, p. 214).

(114) Cooperation with other authorities competent for supervising credit institutions under Directives 2014/92/EU and (EU) 2015/2366 has the potential to reduce unintended consequences of AML/CFT requirements. Credit institutions might choose to terminate or restrict business relationships with customers or categories of customers in order to avoid, rather than manage, risk. Such de-risking practices could weaken the AML/CFT framework and the detection of suspicious transactions, as they push affected customers to resort to less secure or unregulated payment channels to meet their financial needs. At the same time, widespread de-risking practices in the banking sector could lead to financial exclusion for certain categories of payment entities or consumers. Financial supervisors are best placed to identify situations where a credit institution has refused to enter into a business relationship despite possibly being obliged to do so on the basis of the national law implementing Directive 2014/92/EU or Directive (EU) 2015/2366, and without a justification based on the documented customer due diligence. Financial supervisors should alert the authorities responsible for ensuring compliance by financial institution with Directive 2014/92/EU or Directive (EU) 2015/2366 when such cases arise or where business relationships are terminated as a result of de-risking practices.

(115) Cooperation between financial supervisors and the authorities responsible for crisis management of credit institutions and investment firms, in particular the Deposit Guarantee Scheme's designated authorities and resolution authorities, is necessary to reconcile the objectives of preventing money laundering under this Directive and of protecting financial stability and depositors under Directives 2014/49/EU and 2014/59/EU. Financial supervisors should inform the designated authorities and resolution authorities under those Directives of any instance where they identify an increased likelihood of failure or the unavailability of deposits on AML/CFT grounds. Financial supervisors should also inform those authorities of any transaction, account or business relationship that has been suspended by the FIU to allow the performance of the tasks of the designated authorities and resolution authorities in cases of increased risk of failure or unavailability of deposits, irrespective of the reason for that increased risk.

(116) To facilitate such cooperation in relation to credit institutions and financial institutions, AMLA, in consultation with the European Banking Authority, should issue guidelines specifying the main elements of such cooperation including how information should be exchanged.

(117) Cooperation mechanisms should also extend to the authorities in charge of the supervision and oversight of auditors, as such cooperation can enhance the effectiveness of the Union anti-money laundering framework.

(118) The exchange of information and the provision of assistance between competent authorities of Member States is essential for the purposes of this Directive. Consequently, Member States should not prohibit or place unreasonable or unduly restrictive conditions on such exchange of information or provision of assistance.

(119) Supervisors should be able to cooperate and exchange confidential information, regardless of their respective nature or status. To that end, they should have an adequate legal basis for exchange of confidential information and for cooperation. Exchange of information and cooperation with other authorities competent for supervising or overseeing obliged entities under other Union legal acts should not be hampered unintentionally by legal uncertainty which could stem from a lack of explicit provisions in this field. Clarification of the legal framework is even more important since prudential supervision has, in a number of cases, been entrusted to non-AML/CFT supervisors, such as the European Central Bank (ECB).

(120) Information in possession of supervisors might be crucial for the performance of activities of other competent authorities. To ensure the effectiveness of the Union AML/CFT framework, Member States should authorise the exchange of information between supervisors and other competent authorities. Strict rules should apply in relation to the use of confidential information exchanged.

(121) The effectiveness of the Union AML/CFT framework relies on cooperation between a wide array of competent authorities. To facilitate such cooperation, AMLA should be entrusted to develop guidelines in coordination with the ECB, the European Supervisory Authorities, Europol, Eurojust, and EPPO on cooperation between all competent authorities. Such guidelines should also describe how authorities competent for the supervision or oversight of obliged entities under other Union legal acts should take into account money laundering and terrorist financing concerns in the performance of their duties.

(122) Regulation (EU) 2016/679 applies to the processing of personal data for the purposes of this Directive. Regulation (EU) 2018/1725 of the European Parliament and of the Council ([27]) applies to the processing of personal data by the Union institutions, bodies, offices and agencies for the purposes of this Directive. The fight against money laundering and terrorist financing is recognised as an important public interest ground by Member States. However, competent authorities responsible for investigating or prosecuting money laundering, its predicate offences or terrorist financing, or those which have the function of tracing, seizing or freezing and confiscating criminal assets should respect the rules pertaining to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, including Directive (EU) 2016/680 of the European Parliament and of the Council ([28]).

(123) It is essential that the alignment of this Directive with the revised FATF Recommendations is carried out in full compliance with Union law, in particular as regards Union data protection law, including rules on data transfers, as well as the protection of fundamental rights as enshrined in the Charter. Certain aspects of the implementation of this Directive involve the collection, analysis, storage and sharing of data within the Union and with third countries. Such processing of personal data should be permitted, while fully respecting fundamental rights, only for the purposes laid down in this Directive, and for the activities required under this Directive, such as the exchange of information among competent authorities.

(124) The rights of access to data by the data subject are applicable to the personal data processed for the purpose of this Directive. However, access by the data subject to any information related to a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. Exceptions to and restrictions of that right in accordance with Article 23 of Regulation (EU) 2016/679 and, where relevant, Article 25 of Regulation (EU) 2018/1725, might therefore be justified. The data subject has the right to request that a supervisory authority as referred to in Article 51 of Regulation (EU) 2016/679 or, where applicable, the European Data Protection Supervisor, check the lawfulness of the processing and has the right to seek a judicial remedy as referred to in Article 79 of that Regulation. The supervisory authority referred to in Article 51 of Regulation (EU) 2016/679 can also act on an ex officio basis. Without prejudice to the restrictions on the right to access, the supervisory authority should be able to inform the data subject that it has carried out all necessary verifications, and of the result as regards the lawfulness of the processing in question.

(125) In order to ensure continued exchange of information between FIUs during the period of set-up of AMLA, the Commission should continue to host the FIU.net on a temporary basis. To ensure full involvement of FIUs in the operation of the system, the Commission should regularly exchange with the EU Financial Intelligence Units' Platform (the 'EU FIUs' Platform'), an informal group composed of representatives from FIUs and active since 2006, and used to facilitate cooperation among FIUs and exchange views on cooperation-related issues.

(126) Regulatory technical standards should ensure consistent harmonisation across the Union. As the body with highly specialised expertise in the field of AML/CFT, it is appropriate to entrust AMLA with the elaboration, for submission to the Commission, of draft regulatory technical standards which do not involve policy choices.

(127) In order to ensure consistent approaches among FIUs and among supervisors, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of defining indicators to classify the level of gravity of failures to report adequate, accurate and up-to-date information to the central registers. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([29]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

([27]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

([28]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

([29]) OJ L 123, 12.5.2016, p. 1.

(128) The Commission should be empowered to adopt regulatory technical standards developed by AMLA specifying the relevance and selection criteria when determining whether a suspicious transaction report concerns another Member State; setting out benchmarks and methodology for assessing and classifying the inherent and residual risk profile of obliged entities and the frequency of risk profile reviews; setting out the criteria for determining the circumstances of appointment of a central contact point of certain services providers and the functions of the central contact points; specifying duties of the home and host supervisors, and the modalities of cooperation between them; specifying the general conditions for the functioning of the AML/CFT supervisory colleges in the financial sector, the template for the written agreement to be signed by financial supervisors, any additional measure to be implemented by the colleges when groups include obliged entities in the non-financial sector and conditions for the participation of financial supervisors in third countries; specifying he general conditions for the functioning of the AML/CFT supervisory colleges in the non-financial sector, the template for the written agreement to be signed by non-financial supervisors, conditions for the participation of non-financial supervisors in third countries and any additional measure to be implemented by the colleges when groups include credit institutions or financial institutions; setting out indicators to classify the level of gravity of breaches of this Directive, criteria to be taken into account when setting the level of pecuniary sanctions or applying administrative measures and a methodology for the imposition of periodic penalty payments. The Commission should adopt those regulatory technical standards by means of delegated acts pursuant to Article 290 TFEU and in accordance with Article 49 of Regulation (EU) 2024/1620.

(129) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission in order to lay down a methodology for the collection of statistics; establish the format for the submission of beneficial ownership information to the central register; define technical specifications and procedures necessary for the implementation of access to beneficial ownership information on the basis of a legitimate interest by the central registers; establish the format for the submission of the information to the centralised automated mechanisms; set out the technical specifications and procedures for the connection of Member States' centralised automated mechanisms to BARIS; set out technical specifications and procedures necessary to provide for the interconnection of Member States' central registers; and set out technical specifications and procedures necessary to provide for the interconnection of Member States' centralised automated mechanisms. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([30]).

(130) The Commission should be empowered to adopt implementing technical standards developed by AMLA specifying the format to be used for the exchange of the information among FIUs of Member States as well as specifying the template to be used for the conclusion of cooperation agreements between Union supervisors and third-country counterparts. The Commission should adopt those implementing technical standards by means of implementing acts pursuant to Article 291 TFEU and in accordance with Article 53 of Regulation (EU) 2024/1620.

(131) This Directive respects the fundamental rights and observes the principles recognised by the Charter, in particular the right to respect for private and family life, the right to the protection of personal data and the freedom to conduct a business.

(132) Equality between women and men, and diversity are fundamental values of the Union, which it sets out to promote across the whole range of Union actions. While progress has been made in those areas, more is needed to achieve balanced representation in decision-making, whether at Union or at national level. Without prejudice to the primary application of merit-based criteria, when appointing the heads of their national supervisory authorities and FIUs, Member States should seek to ensure gender balance, diversity and inclusion, and take into account, to the extent possible, intersections between them. Member States should strive to ensure balanced and inclusive representation also when selecting their representatives to the General Boards of AMLA.

(133) When drawing up a report evaluating the implementation of this Directive, the Commission should give due consideration to the respect of the fundamental rights and principles recognised by the Charter.

([30]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(134) The judgement of the Court of Justice in Joined Cases C-37/20 and C-601/20, WM and Sovim SA v Luxembourg Business Registers ([31]), annulled the amendment made by Directive (EU) 2018/843 to Article 30(5) of Directive (EU) 2015/849 insofar as it required Member States to ensure that information on the beneficial ownership of companies and of other legal entities incorporated within their territory is accessible in all cases to any member of the general public. In order to ensure legal clarity, it is important to adapt that provision by clarifying that only persons or organisations with legitimate interest should be able to access that information. The same condition should apply to the access to information on beneficial ownership of trusts or similar legal arrangements. Directive (EU) 2015/849 should therefore be amended. The implications of that judgement extend beyond Article 30(5) of Directive (EU) 2015/849 and are similar for the provisions regulating access to beneficial ownership information of legal arrangements. In order to ensure that the Union framework strikes the right balance between the protection of fundamental rights and the pursuit of a legitimate objective of general interest such as the protection of the Union's financial system against money laundering and terrorist financing, it is therefore appropriate to introduce amendments to Article 31(4) of Directive (EU) 2015/849. Member States should be granted one year from the date of entry into force of this Directive to bring into force the necessary laws, regulations and administrative measures to transpose those amendments. Given the importance of ensuring a proportionate Union AML/CFT framework, Member States should make every effort to transpose those amendments as soon as possible before that deadline.

(135) Given the need to urgently implement a harmonised approach to the access to central registers on the basis of the demonstration of a legitimate interest, the relevant provisions should be transposed by Member States by 10 July 2026. However, since the initial period of the new regime for access on the basis of the demonstration of a legitimate interest will likely see a peak in demands to be processed by the entities in charge of the central registers, the deadlines for the granting of access should not apply for the first 4 months of application of the new regime. Member States should set up single access points for information on real estate registers by 10 July 2029. Centralised automated mechanisms allowing the identification of holders of bank accounts or payment accounts, securities accounts, crypto-asset accounts and accounts and safe-deposit boxes should also be interconnected by that date.

(136) Since the objectives of this Directive, namely the establishment of a coordinated and coherent mechanism to prevent money laundering and terrorist financing, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(137) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents ([32]), Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(138) The European Data Protection Supervisor has been consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 22 September 2021 ([33]).

(139) Directive (EU) 2015/849 should therefore be repealed,

HAVE ADOPTED THIS DIRECTIVE:

([31]) Judgment of the Court of Justice of 22 November 2022, WM and Sovim SA v Luxembourg Business Registers, Joined Cases C-37/20 and C-601/20, ECLI:EU:C:2022:912.
([32]) OJ C 369, 17.12.2011, p. 14.
([33]) OJ C 524, 29.12.2021, p. 10.

CHAPTER I

**GENERAL PROVISIONS**

*SECTION 1*

***Subject matter, scope and definitions***

*Article 1*

**Subject matter**

This Directive lays down rules concerning:

(a) the measures applicable to sectors exposed to money laundering and terrorist financing, at national level;

(b) the requirements in relation to registration of, identification of, and checks on, senior management and beneficial owners of obliged entities;

(c) the identification of money laundering and terrorist financing risks at Union and Member State level;

(d) the set-up of and access to beneficial ownership and bank account registers and access to real estate information;

(e) the responsibilities and tasks of Financial Intelligence Units (FIUs);

(f) the responsibilities and tasks of bodies involved in the supervision of obliged entities;

(g) cooperation between competent authorities and cooperation with authorities covered by other Union legal acts.

*Article 2*

**Definitions**

For the purposes of this Directive, the definitions set out in Article 2(1) of Regulation (EU) 2024/1624 apply.

The following definitions also apply:

(1) 'financial supervisor' means a supervisor in charge of credit institutions and financial institutions;

(2) 'non-financial supervisor' means a supervisor in charge of the non-financial sector;

(3) 'non-financial sector' means the obliged entities listed in Article 3, point (3), of Regulation (EU) 2024/1624;

(4) 'obliged entity' means a natural or legal person listed in Article 3 of Regulation (EU) 2024/1624 that is not exempted in accordance with Article 4, 5, 6 or 7 of that Regulation;

(5) 'home Member State' means the Member State where the registered office of the obliged entity is located or, if the obliged entity has no registered office, the Member State in which its head office is located;

(6) 'host Member State' means a Member State, other than the home Member State, in which the obliged entity operates an establishment, such as a subsidiary or a branch, or where the obliged entity operates under the freedom to provide services through an infrastructure;

(7) 'customs authorities' means the customs authorities as defined in Article 5, point (1), of Regulation (EU) No 952/2013 of the European Parliament and of the Council ([34]) and the competent authorities as defined in Article 2(1), point (g), of Regulation (EU) 2018/1672 of the European Parliament and of the Council ([35]);

(8) 'AML/CFT supervisory college' means a permanent structure for cooperation and information sharing for the purposes of supervising a group or an entity that operates in a host Member State or third country;

(9) 'draft national measure' means the text of an act, whichever its form, which, once enacted, will have legal effect, the text being at a stage of preparation at which substantial amendments can still be made;

(10) 'securities account' means a securities account as defined in Article 2(1), point (28), of Regulation (EU) No 909/2014 of the European Parliament and of the Council ([36]);

(11) 'securities' means financial instruments as defined in Article 4(1), point (15), of Directive 2014/65/EU of the European Parliament and of the Council ([37]).

*SECTION 2*

***National measures in sectors exposed to money laundering and terrorist financing***

*Article 3*

**Identification of exposed sectors at national level**

1. Where a Member State identifies that, in addition to obliged entities, entities in other sectors are exposed to money laundering and terrorist financing risks, it may decide to apply all or part of Regulation (EU) 2024/1624 to those additional entities.

2. For the purposes of paragraph 1, Member States shall notify the Commission of their intention to apply all or part of Regulation (EU) 2024/1624 to entities in other sectors. Such notification shall be accompanied by:

(a) a justification of the money laundering and terrorist financing risks underpinning such intention;

(b) an assessment of the impact that such application will have on the provision of services within the internal market;

(c) the requirements of Regulation (EU) 2024/1624 that the Member State intends to apply to those entities;

(d) the text of the draft national measures, as well as any update thereof where the Member State has significantly altered the scope, content or implementation of those notified measures.

3. Member States shall postpone the adoption of national measures for 6 months from the date of the notification referred to in paragraph 2.

The postponement referred to in the first subparagraph of this paragraph shall not apply in cases where the national measure aims at addressing a serious and present threat of money laundering or terrorist financing. In that case, the notification referred to in paragraph 2 shall be accompanied by a justification as to why the Member State will not postpone its adoption.

4. Before the end of the period referred to in paragraph 3, the Commission, having consulted the Authority for Anti-Money Laundering and Countering the Financing of Terrorism established by Regulation (EU) 2024/1620 (AMLA), shall issue a detailed opinion regarding whether the measure envisaged:

([34]) Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (OJ L 269, 10.10.2013, p. 1).
([35]) Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 (OJ L 284, 12.11.2018, p. 6).
([36]) Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257, 28.8.2014, p. 1).
([37]) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

(a) is adequate to address the risks identified, in particular as regards whether the risks identified by the Member State concern the internal market;

(b) may create obstacles to the free movement of services or capital or to the freedom of establishment of service providers within the internal market which are not proportionate to the money laundering and terrorist financing risks the measure aims to mitigate.

The detailed opinion referred to in the first subparagraph shall also indicate whether the Commission intends to propose action at Union level.

5. Where the Commission does not consider it appropriate to propose action at Union level, the Member State concerned shall, within 2 months of receiving the detailed opinion referred to in paragraph 4, report to the Commission on the action it proposes in relation thereto. The Commission shall comment on the action proposed by the Member State.

6. Where the Commission indicates its intention to propose action at Union level in accordance with paragraph 4, second subparagraph, the Member State concerned shall abstain from adopting the national measures referred to in paragraph 2, point (d), unless those national measures aim at addressing a serious and present threat of money laundering or terrorist financing.

7. Where, on 9 July 2024, Member States have already applied national provisions transposing Directive (EU) 2015/849 to other sectors than obliged entities, they may apply all or part of Regulation (EU) 2024/1624 to those sectors.

By 10 January 2028, Member States shall notify the Commission of the sectors identified at national level pursuant to the first subparagraph of this paragraph to which the requirements of Regulation (EU) 2024/1624 apply, accompanied by a justification of the exposure of those sectors to money laundering and terrorist financing risks. Within 6 months of such notification, the Commission having consulted AMLA, shall issue a detailed opinion pursuant to paragraph 4. Where the Commission does not consider it appropriate to propose action at Union level, paragraph 5 shall apply.

8. By 10 July 2028 and every year thereafter, the Commission shall publish a consolidated list of the sectors to which Member States have decided to apply all or part of Regulation (EU) 2024/1624 in the Official Journal of the European Union.

*Article 4*

**Requirements relating to certain service providers**

1. Member States shall ensure that currency exchange and cheque cashing offices, and trust or company service providers, are either licensed or registered.

2. Member States shall ensure that all providers of gambling services are regulated.

3. Member States shall ensure that obliged entities other than those referred to in paragraphs 1 and 2 are subject to minimum registration requirements which enable supervisors to identify them.

The first subparagraph shall not apply where the obliged entities other than those referred to in paragraphs 1 and 2 are subject to licensing or registration requirements under other Union legal acts, or to national rules regulating access to the profession or subjecting it to licensing or registration requirements which enable supervisors to identify them.

*Article 5*

**Requirements relating to the granting of residence rights in exchange for investment**

1. Member States whose national law enables the granting of residence rights in exchange for any kind of investment, such as capital transfers, purchase or renting of property, investment in government bonds, investment in corporate entities, donation or endowment of an activity contributing to the public good and contributions to the state budget, shall put in place at least the following measures to mitigate the associated risks of money laundering, its predicate offences or terrorist financing:

(a) a risk management process, including the identification, classification and mitigation of risks under the coordination of a designated authority;

(b) measures providing for the mitigation of risks of money laundering, its predicate offences or terrorist financing associated with applicants for the granting of residence rights in exchange for investment including:

(i) checks on the profile of the applicant by the designated authority, including obtaining information on the source of funds and source of wealth of the applicant;

(ii) verification of information on applicants against information held by competent authorities as referred to in Article 2(1), point (44)(a) and (c), of Regulation (EU) 2024/1624 subject to the respect of the applicable national criminal procedural law and against lists of individuals and entities subject to Union restrictive measures;

(iii) periodic reviews of medium and high-risk applicants.

2. Member States shall ensure monitoring of implementation of the risk management process as referred to in paragraph 1, point (a), including by assessing it on an annual basis.

3. Member States shall adopt and implement the measures referred to in paragraph 1 of this Article in a manner consistent with the risks identified under the risk assessment carried out pursuant to Article 8.

4. Member States shall publish an annual report on the risks of money laundering, its predicate offences or terrorist financing associated with the granting of residence rights in exchange for investment. Those reports shall be made public and shall include the information on:

(a) the number of received applications and of countries of origin of the applicants;

(b) the number of residence permits granted or rejected, and the reasons for such rejections;

(c) any evolution detected in the risks of money laundering, its predicate offences and terrorist financing associated with the granting of residence rights in exchange for investment.

5. By 10 July 2028, Member States shall notify the Commission of the measures adopted under paragraph 1 of this Article. That notification shall include an explanation of those measures based on the relevant risk assessment carried out by Member States pursuant to Article 8.

6. The Commission shall publish in the Official Journal of the European Union the measures notified by Member States pursuant to paragraph 5.

7. By 10 July 2030, the Commission shall publish a report assessing the measures notified pursuant to paragraph 5 in mitigating the risks of money laundering, its predicate offences and terrorist financing and, where necessary, issue recommendations.

*Article 6*

**Checks on the senior management and beneficial owners of certain obliged entities**

1. Member States shall require supervisors to verify that the members of the senior management in the obliged entities referred to in Article 4(1) and (2) as well as financial mixed activity holding companies, and the beneficial owners of such entities are of good repute, and act with honesty and integrity. Senior management of such entities shall also possess the knowledge and expertise necessary to carry out their functions.

2. With respect to the obliged entities referred to in Article 3, points (3)(a), (b), (d), (e), (f) and (h) to (o), of Regulation (EU) 2024/1624, Member States shall ensure that supervisors take the necessary measures to prevent persons convicted of money laundering, its relevant predicate offences or terrorist financing or their associates from being professionally accredited, from holding a senior management function in or from being the beneficial owners of those obliged entities.

3. Member States shall ensure that supervisors verify, on a risk-sensitive basis, whether the requirements of paragraphs 1 and 2 continue to be met. In particular, they shall verify whether the senior management of obliged entities referred to in paragraph 1 is of good repute, acts with honesty and integrity and possesses knowledge and expertise necessary to carry out its functions in cases where there are reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted, or there is increased risk thereof in an obliged entity.

4. Member States shall ensure that supervisors have the power to request the removal of any person convicted of money laundering, its relevant predicate offences or terrorist financing, from the senior management of obliged entities as referred to in paragraphs 1 and 2. Member States shall ensure that supervisors have the power to remove or impose a temporary ban on members of the senior management of the obliged entities referred to in paragraph 1 that are not deemed to be of good repute, act with honesty and integrity or possess the knowledge and expertise necessary to carry out their functions.

5. Member States shall ensure that supervisors have the power to disassociate persons convicted of money laundering, its relevant predicate offences or terrorist financing, who are beneficial owners of obliged entities as referred to in paragraphs 1 and 2, from obliged entities, including by granting supervisors the power to request the divestment of the holding by those beneficial owners in obliged entities.

6. For the purposes of this Article, Member States shall ensure that, in accordance with national law, supervisors or any other authority competent at national level for assessing the requirements applicable to persons referred to in paragraphs 1 and 2 of this Article, check the central AML/CFT database under Article 11 of Regulation (EU) 2024/1620 and whether a relevant conviction exists in the criminal record of the person concerned. Any exchange of information for those purposes shall be carried out in accordance with Framework Decision 2009/315/JHA and Decision 2009/316/JHA as implemented in national law.

7. Member States shall ensure that decisions taken by supervisors pursuant to this Article are subject to effective remedial procedures, including judicial remedy.

8. By 10 July 2029, AMLA shall issue guidelines on:

(a) the criteria to assess good repute, honesty and integrity as referred to in paragraph 1;

(b) the criteria to assess knowledge and expertise as referred to in paragraph 1;

(c) the consistent application by supervisors of the power entrusted to them under this Article.

When drawing up the guidelines referred to in the first subparagraph, AMLA shall take into account the specificities of each sector in which the obliged entities operate.

9. Member States shall apply this Article in relation to the obliged entities referred to in Article 3, points 3(n) and (o) of Regulation (EU) 2024/1624 from 10 July 2029.

*SECTION 3*

***Risk assessments***

*Article 7*

**Risk assessment at Union level**

1. The Commission shall conduct an assessment of the risks of money laundering and terrorist financing and of non-implementation and evasion of targeted financial sanctions affecting the internal market and relating to cross-border activities.

2. By 10 July 2028, the Commission shall draw up a report identifying, analysing and evaluating those risks at Union level. The Commission shall update that report every 4 years thereafter. The Commission may update parts of the report more frequently, if appropriate.

Where, while updating its report, the Commission identifies new risks, it may recommend to Member States to consider updating their national risk assessments, or to carry out sectoral risk assessments, pursuant to Article 8 in order to assess those risks.

The report referred to in the first subparagraph shall be made public, except for those parts which contain classified information.

3. The report referred to in paragraph 1 shall cover at least the following:

(a) the areas and sectors of the internal market that are exposed to money laundering and terrorist financing risks;

(b) the nature and level of the risks associated with each area and sector;

(c) the most widespread means used to launder illicit proceeds, including, where available, those particularly used in transactions between Member States and third countries, independently of the identification of a third country pursuant to Section 2 of Chapter III of Regulation (EU) 2024/1624;

(d) an assessment of the risks of money laundering and terrorist financing associated with legal persons and legal arrangements, including the exposure to risks deriving from foreign legal persons and foreign legal arrangements;

(e) the risks of non-implementation and evasion of targeted financial sanctions.

4. The Commission shall make recommendations to Member States on the measures suitable for addressing the identified risks. In the event that Member States decide not to apply any of the recommendations in their national AML/CFT regimes, they shall notify the Commission thereof and provide a detailed justification stating their reasons for such a decision.

5. By 10 July 2030 and every 2 years thereafter, AMLA, in accordance with Article 55 of Regulation (EU) 2024/1620, shall issue an opinion addressed to the Commission on the risks of money laundering and terrorist financing affecting the Union. AMLA may issue opinions or updates of its previous opinions more frequently, where it deems it appropriate to do so. The opinions issued by AMLA shall be made public, except for those parts which contain classified information.

6. In conducting the assessment referred to in paragraph 1, the Commission shall organise the work at Union level, shall take into account the opinions referred to in paragraph 5 and shall involve Member States' experts in the area of AML/CFT, representatives from national supervisory authorities and FIUs, AMLA and other Union level bodies, and, where appropriate, other relevant stakeholders.

7. Within 2 years of the adoption of the report referred to in paragraph 2, and every 4 years thereafter, the Commission shall submit a report to the European Parliament and to the Council on the actions taken based on the findings of that report.

*Article 8*

**National risk assessment**

1. Each Member State shall carry out a national risk assessment to identify, assess, understand and mitigate the risks of money laundering and terrorist financing, and the risks of non-implementation and evasion of targeted financial sanctions affecting it. It shall keep that risk assessment up to date and review it at least every 4 years.

Where Member States consider that the risk situation so requires, they may review the national risk assessment more frequently or conduct ad hoc sectoral risk assessments.

2. Each Member State shall designate an authority or establish a mechanism to coordinate the national response to the risks referred to in paragraph 1. The identity of that authority or the description of the mechanism shall be notified to the Commission. The Commission shall publish the list of the designated authorities or established mechanisms in the Official Journal of the European Union.

3. In carrying out the national risk assessments referred to in paragraph 1 of this Article, Member States shall take into account the report referred to in Article 7(2), including sectors and products covered and the findings of that report.

4. Member States shall use the national risk assessment to:

(a) improve their AML/CFT regimes, in particular by identifying any areas where obliged entities are to apply enhanced measures in line with a risk-based approach and, where appropriate, specifying the measures to be taken;

(b) identify, where appropriate, sectors or areas of lower or greater risk of money laundering and terrorist financing;

(c) assess the risks of money laundering and terrorist financing associated with each type of legal person established in their territory and each type of legal arrangement which is governed under national law, or which is administered in their territory or whose trustees or persons holding equivalent positions in similar legal arrangements reside in their

territory; and have an understanding of the exposure to risks deriving from foreign legal persons and foreign legal arrangements;

(d) decide on the allocation and prioritisation of resources to combat money laundering and terrorist financing as well as non-implementation and evasion of targeted financial sanctions;

(e) ensure that appropriate rules are drawn up for each sector or area, in accordance with the risks of money laundering and terrorist financing;

(f) make appropriate information available promptly to competent authorities and to obliged entities to facilitate the carrying out of their own money laundering and terrorist financing risk assessments as well as the assessment of risks of non-implementation and evasion of targeted financial sanctions referred to in Article 10 of Regulation (EU) 2024/1624.

In the national risk assessment, Member States shall describe the institutional structure and broad procedures of their AML/CFT regime, including the FIU, tax authorities and prosecutors, the mechanisms for cooperation with counterparts within the Union or in third countries, as well as the allocated human and financial resources to the extent that this information is available.

5. Member States shall ensure appropriate participation of competent authorities and relevant stakeholders when carrying out their national risk assessment.

6. Member States shall make the results of their national risk assessments, including updates and reviews, available to the Commission, to AMLA and to the other Member States. A Member State may provide relevant additional information, where appropriate, to the Member State carrying out the national risk assessment. A summary of the findings of the assessment shall be made public. That summary shall not contain classified information. Any document disseminated or made public pursuant to this paragraph shall not contain any information permitting the identification of any natural person or name any legal person.

*Article 9*

**Statistics**

1. Member States shall maintain comprehensive statistics on matters relevant to the effectiveness of their AML/CFT frameworks in order to review the effectiveness of those frameworks.

2. The statistics referred to in paragraph 1 of this Article shall include:

(a) data measuring the size and importance of the different sectors which fall within the scope of this Directive, including the number of natural and legal persons and the economic importance of each sector;

(b) data measuring the reporting, investigation and judicial phases of the national AML/CFT regime, including the number of suspicious transaction reports made to the FIU, the follow-up given to those reports, the information on cross-border physical transfers of cash transmitted to the FIU in accordance with Article 9 of Regulation (EU) 2018/1672 together with the follow-up given to the information submitted and, on an annual basis, the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences, the types of predicate offences identified in accordance with Article 2 of Directive (EU) 2018/1673 of the European Parliament and of the Council ([38]) where such information is available, and the value in euro of property that has been frozen, seized or confiscated;

(c) the number and percentage of suspicious transaction reports resulting in dissemination to other competent authorities and, if available, the number and percentage of reports resulting in further investigation, together with the annual report drawn up by FIUs pursuant to Article 27;

([38]) Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law (OJ L 284, 12.11.2018, p. 22).

(d) data regarding the number of cross-border requests for information that were made, received, refused and partially or fully answered by the FIU, broken down by counterpart country;

(e) the number of mutual legal assistance or other international requests for information relating to beneficial ownership and bank account information as referred to in Chapter IV of Regulation (EU) 2024/1624 and Sections 1 and 2 of Chapter II of this Directive received from or made to counterparts outside the Union, broken down by competent authority and counterpart country;

(f) human resources allocated to supervisors as well as human resources allocated to the FIU to fulfil the tasks specified in Article 19;

(g) the number of on-site and off-site supervisory actions, the number of breaches identified on the basis of supervisory actions and pecuniary sanctions and periodic penalty payments imposed or administrative measures applied by supervisory authorities and self-regulatory bodies pursuant to Section 4 of Chapter IV;

(h) the number and type of breaches identified in relation to the obligations of Chapter IV of Regulation (EU) 2024/1624 and pecuniary sanctions imposed or administrative measures applied in relation to those breaches, the number of discrepancies reported to the central register referred to in Article 10 of this Directive, as well as the number of checks carried out by the entity in charge of the central register or on its behalf pursuant to Article 10(11) of this Directive;

(i) the following information regarding the implementation of Article 12:

  (i) the number of requests to access beneficial ownership information in central registers on the basis of the categories laid down in Article 12(2);

  (ii) the percentage of requests for access to information which is refused under each category laid down in Article 12 (2);

  (iii) a summary of the categories of persons granted access to beneficial ownership information under Article 12(2), second subparagraph;

(j) the number of searches of bank account registers or data retrieval mechanisms made by competent authorities, broken down by category of competent authority, and the number of searches of the interconnection of bank account registers made by FIUs and supervisory authorities;

(k) the following data regarding implementation of targeted financial sanctions:

  (i) the value of funds or other assets frozen, broken down by type;

  (ii) human resources allocated to authorities competent for implementation and enforcement of targeted financial sanctions.

3. Member States shall ensure that the statistics referred to in paragraph 2 are collected and transmitted to the Commission on an annual basis. The statistics referred to in paragraph 2, points (a), (c), (d) and (f), shall also be transmitted to AMLA.

AMLA shall store those statistics in its database in accordance with Article 11 of Regulation (EU) 2024/1620.

4. By 10 July 2029, AMLA shall adopt an opinion addressed to the Commission on the methodology for the collection of the statistics referred to in paragraph 2, points (a), (c), (d), (f) and (g).

5. The Commission may lay down, by means of implementing acts, the methodology for the collection of the statistics referred to in paragraph 2 of this Article and the arrangements for their transmission to the Commission and to AMLA. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

6. By 10 July 2030 and every 2 years thereafter, the Commission shall publish a report summarising and explaining the statistics referred to in paragraph 2, and make it available on its website.

CHAPTER II

**REGISTERS**

*SECTION 1*

***Central beneficial ownership registers***

*Article 10*

**Central beneficial ownership registers**

1. Member States shall ensure that beneficial ownership information as referred to in Article62 of Regulation (EU) 2024/1624, the statement pursuant to Article 63(4) of that Regulation and information on nominee arrangements as referred to in Article 66 of that Regulation are held in a central register in the Member State where the legal entity is created or where the trustee of an express trust or person holding an equivalent position in a similar legal arrangement is established or resides, or from where the legal arrangement is administered. Such requirement shall not apply to legal entities or legal arrangements as referred to in Article 65 of Regulation (EU) 2024/1624.

The information contained in the central beneficial ownership register referred to in the first subparagraph ('central register') shall be available in machine-readable format and be collected in accordance with the implementing acts referred to in paragraph 6.

2. By way of derogation from the first subparagraph of paragraph 1, Member States shall ensure that beneficial ownership information, as referred to in Article 62 of Regulation (EU) 2024/1624, of foreign legal entities and foreign legal arrangements, as referred to in Article 67 of that Regulation, is held in a central register in the Member State in accordance with the conditions laid down in Article 67 of that Regulation. Member States shall also ensure that the central register contains an indication of which situation listed in Article 67(1) of Regulation (EU) 2024/1624 triggers the registration of the foreign legal entity or foreign legal arrangement.

3. Where the trustees of an express trust or persons holding equivalent positions in a similar legal arrangement are established or reside in different Member States, a certificate of proof of registration, or an excerpt of the beneficial ownership information held in a central register by one Member State, shall be sufficient to consider the registration obligation fulfilled.

4. Member States shall ensure that the entities in charge of the central registers are empowered to request from legal entities, trustees of any express trust and persons holding an equivalent position in a similar legal arrangement, and their legal and beneficial owners, any information necessary to identify and verify their beneficial owners, including resolutions of the board of directors and minutes of their meetings, partnership agreements, trust deeds, power of attorney or other contractual agreements and documentation.

5. Where no person is identified as the beneficial owner pursuant to Article 63(3) and Article 64(6) of Regulation (EU) 2024/1624, the central register shall include:

(a) a statement that there is no beneficial owner or that the beneficial owners could not be determined, accompanied by a corresponding justification pursuant to Article 63(4), point (a), and Article 64(7), point (a), of Regulation (EU) 2024/1624;

(b) the details of all natural persons who hold the position of senior managing officials in the legal entity equivalent to the information required under Article 62(1), second subparagraph, point (a), of Regulation (EU) 2024/1624.

Member States shall ensure that the information referred to in the first subparagraph, point (a), is available to competent authorities, as well as to AMLA for the purposes of joint analyses pursuant to Article 32 of this Directive and Article 40 of Regulation (EU) 2024/1620, to self-regulatory bodies and to obliged entities. However, obliged entities shall only have access to the statement submitted by the legal entity or legal arrangement if they report a discrepancy pursuant to Article 24 of Regulation (EU) 2024/1624 or provide proof of the steps they have taken to determine the beneficial owners of the legal entity or legal arrangement, in which case they shall be able to access the justification as well.

6. By 10 July 2025, the Commission shall establish, by means of implementing acts, the format for the submission of beneficial ownership information as referred to in Article 62 of Regulation (EU) 2024/1624 to the central register, including a checklist of minimum requirements for the information to be examined by the entity in charge of the central register. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72 (2) of this Directive.

7. Member States shall ensure that the beneficial ownership information held in the central registers is adequate, accurate and up-to-date, and shall put in place mechanisms to that effect. For that purpose, Member States shall apply at least the following requirements:

(a) entities in charge of the central registers shall verify, within a reasonable time upon submission of the beneficial ownership information, and on a regular basis thereafter, that such information is adequate, accurate and up to date;

(b) competent authorities, if appropriate and to the extent that such requirement does not interfere unnecessarily with their functions, shall report to the entities in charge of the central registers any discrepancies they find between information available in the central registers and the information available to them.

The extent and frequency of the verification referred to in point (a) of the first subparagraph of this paragraph shall be commensurate with the risks associated with the categories of legal entities and legal arrangements identified pursuant to Article 7(3), point (d), and Article 8(4), point (c).

By 10 July 2028, the Commission shall issue recommendations on the methods and procedures to be used by entities in charge of central registers to verify beneficial ownership information and by obliged entities and competent authorities to identify and report discrepancies regarding beneficial ownership information.

8. Member States shall ensure that the information contained in the central registers includes any change to the beneficial ownership of legal entities and legal arrangements and to nominee arrangements, following their first recording in the central register.

9. Member States shall ensure that the entities in charge of the central registers verify whether beneficial ownership information held in those registers concerns persons or entities designated in relation to targeted financial sanctions. Such verification shall take place immediately upon a designation in relation to targeted financial sanctions and at regular intervals.

Member States shall ensure that the information contained in the central registers includes an indication that the legal entity is associated with persons or entities subject to targeted financial sanctions in any of the following situations:

(a) a legal entity or legal arrangement is subject to targeted financial sanctions;

(b) a legal entity or legal arrangement is controlled by a person or entity subject to targeted financial sanctions;

(c) a beneficial owner of a legal entity or legal arrangement is subject to targeted financial sanctions.

The indication referred to in the second subparagraph of this paragraph shall be visible to any person or entity granted access to the information contained in the central registers pursuant to Articles 11 and 12, and shall remain in place until the targeted financial sanctions are lifted.

10. Member States shall ensure that the entities in charge of the central registers take, within 30 working days of the reporting of a discrepancy by a competent authority or by an obliged entity, appropriate actions to resolve the reported discrepancy pursuant to Article 24 of Regulation (EU) 2024/1624, including by amending the information contained in the central registers where the entity is able to verify the beneficial ownership information. A specific mention of the fact that there are discrepancies reported shall be included in the central registers until the discrepancy is resolved and be visible to any person or entity granted access under Articles 11 and 12 of this Directive.

Where the discrepancy is of a complex nature and the entities in charge of the central registers cannot resolve it within 30 working days, they shall record the instance as well as the steps that have been taken, and take any measure necessary to resolve the discrepancy as soon as possible.

11. Member States shall ensure that the entity in charge of the central register is empowered, whether directly or by application to another authority, including judicial authorities, to carry out checks, including on-site inspections at the business premises or registered office of legal entities, in order to establish the current beneficial ownership of the entity and to verify that the information submitted to the central register is accurate, adequate and up-to-date. The right of the entity in charge of the central register to verify beneficial ownership information shall not be restricted, obstructed or precluded.

Where the trustee or person holding an equivalent position is an obliged entity as referred to in in Article 3, point (3)(a), (b) or (c), of Regulation (EU) 2024/1624, Member States shall ensure that the entity in charge of the central register is also empowered to carry out checks, including on-site inspections at the business premises or registered office of the trustee or person in an equivalent position. Those checks shall adhere at least to the following safeguards:

(a) with respect to natural persons, where the business premises or registered office are the same as the natural person's private residence, the on-site inspection shall be subject to prior judicial authorisation;

(b) any procedural safeguard in place in the Member State to protect the legal privilege shall be respected and no information protected by legal privilege shall be accessed.

Member States shall ensure that entities in charge of central registers are empowered to request information from other registers, including in third countries, to the extent that that such information is necessary for the performance of such entities' functions.

12. Member States shall ensure that entities in charge of central registers have at their disposal the automated mechanisms necessary to carry out verifications as referred to in paragraph 7, points (a), and paragraph 9, including by comparing information contained in those registers with information held by other sources.

13. Member States shall ensure that where a verification as referred to in paragraph 7, point (a), is carried out at the time of submission of beneficial ownership information, and such verification leads an entity in charge of a central register to conclude that there are inconsistencies or errors in the beneficial ownership information, the entity in charge of a central register is able to withhold or refuse to issue a valid certificate of proof of registration.

14. Member States shall ensure that where a verification as referred to in paragraph 7, point (a), is carried out after the submission of beneficial ownership information, and such verification leads an entity in charge of a central register to conclude that the information is no longer adequate, accurate, and up-to-date, the entity in charge of the central register is able to suspend the validity of the certification of proof of registration until it considers the beneficial ownership information provided to be in order, except where the inconsistencies are limited to typographical errors, different ways of transliteration, or minor inaccuracies that do not affect the identification of the beneficial owners or their beneficial interest.

15. Member States shall ensure that the entity in charge of the central register is empowered to, whether directly or by application to another authority, including judicial authorities, apply effective, proportionate and dissuasive measures or impose such pecuniary sanctions for failures, including of a repeated nature, to provide the central register with accurate, adequate and up-to-date information about their beneficial ownership.

16. The Commission is empowered to adopt delegated acts in accordance with Article 71 to supplement this Directive by defining indicators to classify the level of gravity of failures to report adequate, accurate and up-to-date information to the central registers, including in cases of repeated failures.

17. Member States shall ensure that if, in the course of the checks carried out pursuant to this Article, or in any other way, the entities in charge of the central registers discover facts that could be related to money laundering or to terrorist financing, they shall promptly inform the FIU thereof.

18. Member States shall ensure that, in the performance of their tasks, the entities in charge of central registers carry out their functions free of undue influence and that those entities implement standards for their employees as regards conflicts of interest and strict confidentiality.

19. The central registers shall be interconnected via the European Central Platform established by Article 22(1) of Directive (EU) 2017/1132.

20. The information referred to in paragraph 1 shall be available through the central registers and through the system of interconnection of central registers for 5 years after the legal entity has been dissolved or the legal arrangement has ceased to exist.

Without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings, Member States may, in specific cases, permit such information to be retained, or require that such information be retained, for an additional maximum period of 5 years where Member States have established that such retention is necessary and proportionate for the purpose of preventing, detecting, investigating or prosecuting suspected money laundering or terrorist financing.

Upon expiry of the retention period referred to in the first subparagraph, Member States shall ensure that the personal data is deleted from the central registers.

21. By 10 July 2031, the Commission shall, publish a report including the following:

(a) an assessment of the effectiveness of the measures taken by the entities in charge of the central registers to ensure that they have adequate, up-to-date and accurate information;

(b) a description of the main types of discrepancies identified by obliged entities and competent authorities in relation to the beneficial ownership information held in the central registers;

(c) best practices and, where appropriate, recommendations with regard to the measures taken by the entities in charge of the central registers to ensure that those registers hold adequate, accurate and up-to-date information;

(d) overview of the features of each central register put in place by Member States, including information on mechanisms to ensure that beneficial ownership information held in those registers is kept accurate, adequate and up to date;

(e) an assessment of the proportionality of the fees imposed for accessing information held in the central registers.

*Article 11*

**General rules regarding access to beneficial ownership registers by competent authorities, self-regulatory bodies and obliged entities**

1. Member States shall ensure that competent authorities have immediate, unfiltered, direct and free access to the information held in the interconnected central registers referred to in Article 10, without alerting the legal entity or legal arrangement concerned.

2. Access as referred to in paragraph 1 shall be granted to:

(a) competent authorities;

(b) self-regulatory bodies in the performance of supervisory functions pursuant to Article 37;

(c) tax authorities;

(d) national authorities with designated responsibilities for the implementation of Union restrictive measures identified under the relevant Council Regulations adopted on the basis of Article 215 TFEU;

(e) AMLA for the purposes of joint analyses pursuant to Article 32 of this Directive and Article 40 of Regulation (EU) 2024/1620;

(f) EPPO;

(g) OLAF;

(h) Europol and Eurojust when providing operational support to the competent authorities of Member States.

3. Member States shall ensure that, when taking customer due diligence measures in accordance with Chapter III of Regulation (EU) 2024/1624, obliged entities have timely access to the information held in the interconnected central registers referred to in Article 10 of this Directive.

4. Member States may choose to make beneficial ownership information held in their central registers available to obliged entities upon payment of a fee, which shall be limited to what is strictly necessary to cover the costs of ensuring the quality of the information held in the central registers and of making the information available. Those fees shall be established in such a way as not to undermine effective access to the information held in the central registers.

5. By 10 October 2026, Member States shall notify to the Commission the list of competent authorities and self-regulatory bodies and the categories of obliged entities that were granted access to the central registers and the type of information available to obliged entities. Member States shall update that notification when there are any changes to the list of competent authorities or categories of obliged entities or to the extent of access granted to obliged entities. The Commission shall make the information on the access by competent authorities and obliged entities, including any change to it, available to the other Member States.

*Article 12*

**Specific access rules to beneficial ownership registers for persons with legitimate interest**

1. Member States shall ensure that any natural or legal person that can demonstrate a legitimate interest in the prevention and combating of money laundering, its predicate offences and terrorist financing has access to the following information on beneficial owners of legal entities and legal arrangements held in the interconnected central registers referred to in Article 10, without alerting the legal entity or legal arrangement concerned:

(a) the name of the beneficial owner;

(b) the month and year of birth of the beneficial owner;

(c) the country of residence and nationality or nationalities of the beneficial owner;

(d) for beneficial owners of legal entities, the nature and extent of the beneficial interest held;

(e) for beneficial owners of express trusts or similar legal arrangements, the nature of the beneficial interest.

In addition to the information referred to in the first subparagraph of this paragraph, Member States shall ensure that any natural or legal persons referred to in paragraph 2, points (a), (b) and (e), also has access to historical information on the beneficial ownership of the legal entity or the legal arrangement, including of legal entities or legal arrangements that have been dissolved or ceased to exist in the preceding 5 years, as well as a description of the control or ownership structure.

Access pursuant to this paragraph shall be granted through electronic means. However, Member States shall ensure that natural and legal persons who can demonstrate a legitimate interest are also able to access the information in other formats if they are unable to use electronic means.

2. The following natural or legal persons shall be deemed to have a legitimate interest to access the information listed in paragraph 1:

(a) persons acting for the purpose of journalism, reporting or any other form of expression in the media, that are connected with the prevention or combating of money laundering, its predicate offences or terrorist financing;

(b) civil society organisations, including non-governmental organisations and academia, that are connected with the prevention or combating of money laundering, its predicate offences or terrorist financing;

(c) natural or legal persons likely to enter into a transaction with a legal entity or legal arrangement and who wish to prevent any link between such a transaction and money laundering, its predicate offences or terrorist financing;

(d) entities subject to AML/CFT requirements in third countries, provided they can demonstrate the need to access the information referred to in paragraph 1 in relation to a legal entity or legal arrangement to perform customer due diligence in respect of a customer or prospective customer pursuant to AML/CFT requirements in those third countries;

(e) third-country counterparts of Union AML/CFT competent authorities provided they can demonstrate the need to access the information referred to in paragraph 1 in relation to a legal entity or legal arrangement to perform their tasks under the AML/CFT frameworks of those third countries in the context of a specific case;

(f) Member State authorities in charge of implementing Title I, Chapters II and III of Directive (EU) 2017/1132, in particular the authorities in charge of the registration of companies in the register referred to in Article 16 of that Directive, and Member State authorities responsible for scrutinising the legality of conversions, mergers and divisions of limited liability companies pursuant to Title II of that Directive;

(g) programme authorities identified by Member States pursuant to Article 71 of Regulation (EU) 2021/1060, in respect of beneficiaries of Union funds;

(h) public authorities implementing the Recovery and Resilience Facility under Regulation (EU) 2021/241, in respect of beneficiaries under the Facility;

(i) Member States' public authorities in the context of public procurement procedures, in respect of the tenderers and operators being awarded the contract under the public procurement procedure;

(j) providers of AML/CFT products, to the strict extent that products developed on the basis of the information referred to in paragraph 1 or containing that information are provided only to customers that are obliged entities or competent authorities provided that those providers can demonstrate the need to access the information referred to in paragraph 1 in the context of a contract with an obliged entity or a competent authority.

In addition to the categories identified under the first subparagraph, Member States shall also ensure that other persons who are able to demonstrate a legitimate interest with respect to the purpose of preventing and combating money laundering, its predicate offences and terrorist financing, are granted access to beneficial ownership information on a case-by-case basis.

3. By 10 July 2026, Member States shall notify to the Commission:

(a) the list of public authorities that are entitled to consult beneficial ownership information pursuant to paragraph 2, points (f), (g) and (h), and the public authorities or categories of public authorities that are entitled to consult beneficial ownership information pursuant to paragraph 2, point (i);

(b) any additional category of persons who have been found to have a legitimate interest to access beneficial ownership information identified in accordance with paragraph 2, second subparagraph.

Member States shall notify the Commission of any change or addition to the categories referred to in the first subparagraph without delay, and in any case within 1 month of its occurrence.

The Commission shall make the information received pursuant to this paragraph available to the other Member States.

4. Member States shall ensure that the central registers keep records of the persons accessing the information pursuant to this Article and are able to disclose them to the beneficial owners when they file a request pursuant to Article 15(1), point (c), of Regulation (EU) 2016/679.

However, Member States shall ensure that the information provided by central registers does not lead to the identification of any person consulting the register where such persons are:

(a) persons acting for the purpose of journalism, reporting or any other form of expression in the media, that are connected with the prevention or combating of money laundering, its predicate offences or terrorist financing;

(b) civil society organisations that are connected with the prevention or combating of money laundering, its predicate offences or terrorist financing.

In addition, Member States shall ensure that entities in charge of the central registers refrain from disclosing the identity of any third-country counterpart of Union AML/CFT competent authorities referred to in Article 2(1), point 44(a) and (c), of Regulation (EU) 2024/1624, for as long as necessary to protect the analyses or investigations of that authority.

In relation to the persons referred to in points (a) and (b) of the second subparagraph of this paragraph, Member States shall ensure that where beneficial owners file a request pursuant to Article 15(1), point (c), of Regulation (EU) 2016/679, they are provided with information on the function or occupation of the persons having consulted their beneficial ownership information.

For the purposes of the third subparagraph, when requesting access to beneficial ownership information pursuant to this Article, the authorities shall indicate the period for which they request the central registers to refrain from disclosure, which shall not exceed 5 years, and the reasons for that restriction, including how the provision of the information would jeopardise the purpose of their analyses and investigations. Member States shall ensure that, where central registers do not disclose the identity of the entity having consulted the beneficial ownership information, any extension of that period shall only be granted on the basis of a justified request by the authority in the third country, for a maximum period of 1 year, after which a new justified request for extension shall be submitted by that authority.

*Article 13*

**Procedure for the verification and mutual recognition of a legitimate interest to access beneficial ownership information**

1. Member States shall ensure that entities in charge of the central registers as referred to in Article 10 take measures to verify the existence of the legitimate interest referred to in Article 12 on the basis of documents, information and data obtained from the natural or legal person seeking access to the central register ('applicant') and, where necessary, information available to them pursuant to Article 12(3).

2. The existence of a legitimate interest to access beneficial ownership information shall be determined by taking into consideration:

(a) the function or occupation of the applicant; and

(b) with the exception of persons referred to in Article 12(2), first subparagraph, points (a) and (b), the connection with the specific legal entities or legal arrangements whose information is being sought.

3. Member States shall ensure that where access to information is requested by a person whose legitimate interest in accessing beneficial ownership information under one of the categories set out in Article 12(2), first subparagraph, has already been verified by the central register of another Member State, the verification of the condition laid down in paragraph 2, point (a), of this Article is satisfied by collecting proof of the legitimate interest issued by the central register of that other Member State.

Member States may apply the procedure set out in the first subparagraph of this paragraph to the additional categories identified by other Member States pursuant to Article 12(2), second subparagraph.

4. Member States shall ensure that entities in charge of central registers verify the identity of applicants whenever they access the registers. To that end, Member States shall ensure that sufficient processes are available for the verification of the identity of the applicant, including by allowing the use of electronic identification means and relevant qualified trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council ([39]).

5. For the purposes of paragraph 2, point (a), Member States shall ensure that central registers have mechanisms in place to allow repeated access to persons with a legitimate interest to access beneficial ownership information without the need to assess their function or occupation whenever accessing the information.

6. From 10 November 2026, Member States shall ensure that the entities in charge of central registers conduct the verification referred to in paragraph 1 and provide a response to the applicant within 12 working days.

By way of derogation from the first subparagraph, in the case of a sudden high number of requests for accessing beneficial ownership information pursuant to this Article, the deadline for providing a response to the applicant may be extended by 12 working days. If, after the extension has lapsed, the number of incoming requests continues to be high, that deadline may be extended by additional 12 working days.

Member States shall notify the Commission of any extension as referred to in the second subparagraph in a timely manner.

([39]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

Where entities in charge of central registers decide to grant access to beneficial ownership information, they shall issue a certificate granting access for 3 years. Entities in charge of central registers shall respond to any subsequent request to access beneficial ownership information by the same person within 7 working days.

7. Member States shall ensure that entities in charge of central registers shall only refuse a request to access beneficial ownership information on one of the following grounds:

(a) the applicant has not provided the necessary information or documents pursuant to paragraph 1;

(b) a legitimate interest to access beneficial ownership information has not been demonstrated;

(c) where on the basis of information in its possession, the entity in charge of the central register has a reasonable concern that the information will not be used for the purposes for which it was requested or that the information will be used for purposes that are not connected to the prevention of money laundering, its predicate offences or terrorist financing;

(d) one or more of the situations referred to in Article 15 applies;

(e) in the cases referred to in paragraph 3, the legitimate interest to access beneficial ownership information granted by the central register of another Member State does not extend to the purposes for which the information is sought;

(f) where the applicant is in a third country and responding to the request to access information would not comply with the provisions of Chapter V of Regulation (EU) 2016/679.

Member States shall ensure that entities in charge of central registers consider requesting additional information or documents from the applicant prior to refusing a request for access on the grounds listed in points (a), (b), (c) and (e) of the first subparagraph. Where entities in charge of central registers request additional information, the deadline for providing a response shall be extended by 7 working days.

8. Where entities in charge of central registers refuse to provide access to information pursuant to paragraph 7, Member States shall require that they inform the applicant of the reasons for refusal and of their right of redress. The entity in charge of the central register shall document the steps taken to assess the request and to obtain additional information pursuant to paragraph 7, second subparagraph.

Member States shall ensure that entities in charge of central registers are able to revoke access where any of the grounds listed in paragraph 7 arise or become known to the entity in charge of the central register after such access has been granted, including, where relevant, on the basis of revocation by a central register in another Member State.

9. Member States shall ensure that they have in place judicial or administrative remedies for challenging the refusal or revocation of access pursuant to paragraph 7.

10. Member States shall ensure that entities in charge of central registers are able to repeat the verification of the function or occupation identified under paragraph 2, point (a), from time-to-time and in any case not earlier than 12 months after granting access, unless the entity in charge of the central register has reasonable grounds to believe that the legitimate interest no longer exists.

11. Member States shall require persons who have been granted access pursuant to this Article to notify the entity in charge of the central register of changes that may trigger the cessation of a valid legitimate interest, including changes concerning their function or occupation.

12. Member States may choose to make beneficial ownership information held in their central registers available to the applicants upon payment of a fee, which shall be limited to what is strictly necessary to cover the costs of ensuring the quality of the information held in those registers and of making the information available. Those fees shall be established in such a way so as not to undermine the effective access to the information held in the central registers.

*Article 14*

**Templates and procedures**

1. The Commission shall define, by means of implementing acts, technical specifications and procedures necessary for the implementation of access on the basis of a legitimate interest by the central registers referred to in Article 10, including:

(a) standardised templates for requesting access to the central register and for requesting access to beneficial ownership information on legal entities and legal arrangements;

(b) standardised templates to be used by central registers to confirm or refuse a request to access the register or to access beneficial ownership information;

(c) procedures to facilitate the mutual recognition of legitimate interest to access beneficial ownership information by the central registers in Member States other than the one where the request for access was first made and accepted, including procedures to ensure the secure transfer of information on an applicant;

(d) procedures for central registers to notify each other of revocations of access to beneficial ownership information pursuant to Article 13(8).

2. The implementing acts referred to in paragraph 1 of this Article shall be adopted in accordance with the examination procedure referred to in Article 72(2).

*Article 15*

**Exceptions to the access rules to beneficial ownership registers**

In exceptional circumstances to be laid down in national law, where the access referred to in Articles 11(3) and 12(1) would expose the beneficial owner to disproportionate risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation, or where the beneficial owner is a minor or otherwise legally incapable, Member States shall provide for an exemption from such access to all or part of the personal information on the beneficial owner. Member States shall ensure that such exemptions are granted on a case-by-case basis upon a detailed evaluation of the exceptional nature of the circumstances and confirmation that those disproportionate risks exist. The right to an administrative review of the decision granting an exemption and the right to an effective judicial remedy shall be guaranteed. A Member State that has granted exemptions shall publish annual statistical data on the number of exemptions granted and the reasons given and report the data to the Commission.

Exemptions granted pursuant to this Article shall not apply to obliged entities as referred to in Article 3, point (3)(b), of Regulation (EU) 2024/1624 that are public officials.

*SECTION 2*

***Bank account information***

*Article 16*

**Bank account registers and electronic data retrieval systems**

1. Member States shall put in place centralised automated mechanisms, such as central registers or central electronic data retrieval systems, which allow the identification, in a timely manner, of any natural or legal persons holding or controlling payment accounts, or bank accounts identified by IBAN, including virtual IBANs, securities accounts, crypto-asset accounts and safe-deposit boxes held by a credit institution or financial institution within their territory.

Member States shall notify the Commission of the characteristics of those national mechanisms as well as the criteria pursuant to which information is included in those national mechanisms.

2. Member States shall ensure that the information held in the centralised automated mechanisms is directly accessible in an immediate and unfiltered manner to FIUs, as well as to AMLA for the purposes of joint analyses pursuant to Article 32 of this Directive and Article 40 of Regulation (EU) 2024/1620. The information shall also be accessible in a timely manner to supervisory authorities to fulfil their obligations under this Directive.

3. The following information shall be accessible and searchable through the centralised automated mechanisms:

(a) for customer-account holders and any person purporting to act on behalf of a customer account holder: the name, complemented by either the other identification data required under Article 22(1) of Regulation (EU) 2024/1624 or a unique identification number as well as, where applicable, the dates on which the person purporting to act on behalf of the customer started and ceased to have the power to act on behalf of the customer;

(b) for beneficial owners of customer-account holders: the name, complemented by either the other identification data required under Article 22(1) of Regulation (EU) 2024/1624 or a unique identification number as well as the dates on which the natural person became and, where applicable, ceased to be the beneficial owner of the customer account holder;

(c) for bank accounts or payment accounts: the IBAN number, or where the payment account is not identified by an IBAN number, the unique account identifier, and the date of account opening and, where applicable, the date of account closing;

(d) for virtual IBANs issued by a credit institution or a financial institution: the virtual IBAN number, the unique account identifier of the account to which payments addressed to the virtual IBAN are automatically redirected, and the dates of account opening and closing;

(e) for securities accounts: the unique identifier of the account, and the dates of account opening and closing;

(f) for crypto-asset accounts: the unique identifier of the account, and the dates of account opening and closing;

(g) for safe-deposit boxes: the name of the lessee complemented by either the other identification data required under Article 22(1) of Regulation (EU) 2024/1624, or a unique identification number and the date on which the lease started and, where applicable, the date on which it ended.

In the case of a virtual IBAN, the customer account holder as referred to in point (a) of the first subparagraph shall be the holder of the account to which payments addressed to the virtual IBAN are automatically redirected.

For the purposes of points (a) and (b) of the first subparagraph, the name shall comprise for natural persons, all names and surnames and for legal entities, legal arrangements or other organisations with legal capacity, the name under which they are registered.

4. The Commission may establish, by means of implementing acts, the format for the submission of the information to the centralised automated mechanisms. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

5. Member States may require other information deemed essential for FIUs, for AMLA for the purposes of joint analyses pursuant to Article 32 of this Directive and Article 40 of Regulation (EU) 2024/1620 and for supervisory authorities to fulfil their obligations under this Directive to be accessible and searchable through the centralised automated mechanisms.

6. The centralised automated mechanisms shall be interconnected via the bank account registers interconnection system ('BARIS'), to be developed and operated by the Commission. The Commission shall ensure such interconnection in cooperation with Member States by 10 July 2029.

The Commission may set out, by means of implementing acts, the technical specifications and procedures for the connection of Member States' centralised automated mechanisms to BARIS. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

7. Member States shall ensure that the information referred to in paragraph 3 is available through BARIS. Member States shall take adequate measures to ensure that only the information referred to in paragraph 3 that is up to date and corresponds to the actual bank account and payment account, including virtual IBANs, securities account, crypto-asset account and safe-deposit box is made available through their national centralised automated mechanisms and through BARIS. Access to that information shall be granted in accordance with data protection rules.

The other information that Member States consider essential for FIUs and other competent authorities pursuant to paragraph 4 shall not be accessible and searchable through BARIS.

8. Member States shall ensure that information on holders of bank accounts or payment accounts, including virtual IBANs, securities accounts, crypto-asset accounts and safe-deposit boxes is made available through their national centralised automated mechanisms and through BARIS during a period of 5 years after the closure of the account.

Without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings, Member States may, in specific cases, permit such information to be retained, or require that such information be retained, for an additional maximum period of 5 years where Member States have established that such retention is necessary and proportionate for the purpose of preventing, detecting, investigating or prosecuting suspected money laundering or terrorist financing.

9. FIUs and, for the purposes of joint analyses pursuant to Article 32 of this Directive and Article 40 of Regulation (EU) 2024/1620, AMLA shall be granted immediate and unfiltered access to the information on payment accounts and bank accounts identified by IBAN, including virtual IBAN, securities accounts, crypto-asset accounts and safe-deposit boxes in other Member States available through BARIS. Supervisory authorities shall be granted access in a timely manner to the information available through BARIS. Member States shall cooperate among themselves and with the Commission in order to implement this paragraph.

Member States shall ensure that the staff of the national FIUs and supervisory authorities that have access to BARIS maintain high professional standards of confidentiality and data protection, are of high integrity and are appropriately skilled.

The requirements laid down in the second subparagraph shall also apply to AMLA in the context of joint analyses and when acting as a supervisor.

10. Member States shall ensure that technical and organisational measures are put in place to ensure the security of the data to high technological standards for the purposes of the exercise by FIUs and supervisory authorities of the power to access and search the information available through BARIS in accordance with paragraphs 5 and 6.

The requirements laid down in the first subparagraph shall also apply to AMLA in the context of joint analyses and when acting as a supervisor.

*Article 17*

**Implementing acts for the interconnection of registers**

1. The Commission may set out, by means of implementing acts, technical specifications and procedures necessary to provide for the interconnection of Member States' central registers in accordance with Article 10(19) with regard to:

(a) the technical specifications defining the set of the technical data necessary for the platform to perform its functions as well as the method of storage, use and protection of such data;

(b) the common criteria according to which beneficial ownership information is available through the system of interconnection of central registers, depending on the level of access granted by Member States;

(c) the technical details on how the information on beneficial owners is to be made available;

(d) the technical conditions of availability of services provided by the system of interconnection of central registers;

(e) the technical arrangements to implement the different types of access to information on beneficial ownership in accordance with Articles 11 and 12 of this Directive, including the authentication of users through the use of electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014;

(f) the payment arrangements where access to beneficial ownership information is subject to the payment of a fee according to Articles 11(4) and 13(12) taking into account available payment facilities such as remote payment transactions.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

2. The Commission may set out, by means of implementing acts, technical specifications and procedures necessary to provide for the interconnection of Member States' centralised automated mechanisms as referred to in Article 16(6), with regard to:

(a) the technical specification defining the methods of communication by electronic means for the purposes of BARIS;

(b) the technical specification of the communication protocols;

(c) the technical specifications defining the data security, data protection safeguards, use and protection of the information which is searchable and accessible by means of BARIS;

(d) the common criteria according to which bank account information is searchable through BARIS;

(e) the technical details on how the information is made available by means of BARIS, including the authentication of users through the use of electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014;

(f) the technical conditions of availability of services provided by BARIS.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

3. When adopting the implementing acts referred to in paragraphs 1 and 2, the Commission shall take into account proven technology and existing practices. The Commission shall ensure that BARIS to be developed and operated does not incur costs beyond what is absolutely necessary in order to implement this Directive.

*SECTION 3*

***Single access point to real estate information***

*Article 18*

**Single access point to real estate information**

1. Member States shall ensure that competent authorities have immediate and direct access free of charge to information which allows for the identification in a timely manner of any real estate property and of the natural persons or legal entities or legal arrangements owning that property, as well as to information allowing for the identification and analysis of transactions involving real estate. That access shall be provided via a single access point to be established in each Member State which allows competent authorities to access, via electronic means, information in digital format, which shall be, where possible machine-readable.

Access to the single access points referred to in the first subparagraph shall also be granted to AMLA for the purposes of joint analyses pursuant to Article 32 of this Directive and Article 40 of Regulation (EU) 2024/1620.

2. Member States shall ensure that at least the following information is made available through the single access point referred to in paragraph 1:

(a) information on the property:

(i) cadastral parcel and cadastral reference;

(ii) geographical location, including address of the property;

(iii) area/size of the property;

(iv) type of property, including whether built or non-built property and destination of use;

(b) information on ownership:

(i) the name of the owner and any person purporting to act on behalf of the owner;

(ii) where the owner is a legal entity, the name and legal form of the legal entity, as well as the company unique identification number and the tax identification number;

(iii) where the owner is a legal arrangement, the name of the legal arrangement and the tax identification number;

(iv) price at which the property has been acquired;

(v) where applicable, any entitlements or restrictions;

(c) information on encumbrances regarding:

(i) mortgages;

(ii) judicial restrictions;

(iii) property rights;

(iv) other guarantees, if any;

(d) history of property ownership, price and related encumbrances;

(e) relevant documents.

Member States shall ensure that, where a cadastral parcel includes multiple properties, the information referred to in the first subparagraph is provided in relation to each property in that cadastral parcel.

Member States shall ensure that historical information pursuant to the first subparagraph, point (d), covers at least the period from 8 July 2019.

3. Member States shall put in place mechanisms to ensure that the information provided through the single access point referred to in paragraph 1 is up to date and accurate.

4. Member States shall have measures in place to ensure that information held electronically is provided immediately to the requesting competent authority. Where that information is not held electronically, Member States shall ensure that it is provided in a timely manner and in such a way as not to undermine the activities of the requesting competent authority.

5. By 10 October 2029, Member States shall notify to the Commission:

(a) the characteristics of the single access point referred to in paragraph 1 established at national level, including the website at which it can be accessed;

(b) the list of competent authorities granted access to the single access point referred to in paragraph 1;

(c) any data made available to competent authorities in addition to those listed in paragraph 2.

Member States shall update such notification when changes to the list of competent authorities or to the extent of access to information granted occurs. The Commission shall make that information, including any change to it, available to the other Member States.

6. By 10 July 2032, the Commission shall submit a report to the European Parliament and to the Council assessing the conditions and the technical specifications and procedures for ensuring secure and efficient interconnection of the single access points referred to in paragraph 1. Where appropriate, that report shall be accompanied by a legislative proposal.

CHAPTER III

**FIUS**

*Article 19*

**Establishment of the FIU**

1. Each Member State shall establish an FIU in order to prevent, detect and effectively combat money laundering and terrorist financing.

2. The FIU shall be the single central national unit responsible for receiving and analysing reports submitted by obliged entities in accordance with Article 69 of Regulation (EU) 2024/1624, reports submitted by obliged entities in accordance with Article 74 and Article 80(4), second subparagraph, of that Regulation, and any other information relevant to money laundering, its predicate offences or terrorist financing, including information transmitted by customs authorities pursuant to Article 9 of Regulation (EU) 2018/1672, as well as information submitted by supervisory authorities or by other authorities.

3. The FIU shall be responsible for disseminating the results of its analyses and any additional information to relevant competent authorities where there are grounds to suspect money laundering, its predicate offences or terrorist financing. It shall be able to obtain additional information from obliged entities.

The FIU's financial analysis function shall consist of the following:

(a) an operational analysis which focuses on individual cases and specific targets or on appropriate selected information, prioritised on the basis of risk, the type and volume of the disclosures received and the expected use of the information after dissemination;

(b) a strategic analysis addressing money laundering and terrorist financing trends and patterns and evolutions thereof.

4. Each FIU shall be operationally independent and autonomous, which means that it shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and, in accordance with paragraph 3, disseminate specific information. It shall be free from any undue political, government or industry influence or interference.

When an FIU is located within the existing structure of another authority, the FIU's core functions shall be independent and operationally separated from the other functions of the host authority.

5. Member States shall provide their FIUs with adequate financial, human and technical resources in order to fulfil their tasks. FIUs shall be able to obtain and deploy the resources needed to carry out their functions.

6. Member States shall ensure that the staff of their FIUs are bound by professional secrecy requirements equivalent to those laid down in Article 67, and that they maintain high professional standards, including high standards of data protection, and are of high integrity and appropriately skilled in relation to the ethical handling of big data sets. Member States shall ensure that FIUs have in place procedures to prevent and manage conflicts of interest.

7. Member States shall ensure that FIUs have rules in place governing the security and confidentiality of information.

8. Member States shall ensure that FIUs have in place secure and protected channels for communicating and exchanging information by electronic means with competent authorities and obliged entities.

9. Member States shall ensure that FIUs are able to make arrangements with other domestic competent authorities pursuant to Article 46 on the exchange of information.

10. By 10 July 2028, AMLA shall issue guidelines addressed to FIUs on:

(a) the measures to be put in place to preserve the operational autonomy and independence of the FIU, including measures to prevent that conflicts of interest affect its operational autonomy and independence;

(b) the nature, features and objectives of operational and of strategic analysis;

(c) tools and methods for use and cross-check of financial, administrative and law enforcement information to which FIUs have access; and

(d) practices and procedures for the exercise of the suspension or the withholding of consent to a transaction and suspension or monitoring of an account or business relationship pursuant to Articles 24 and 25.

*Article 20*

**Fundamental Rights Officer**

1. Member States shall ensure that FIUs designate a Fundamental Rights Officer. The Fundamental Rights Officer may be a member of the existing staff of the FIU.

2. The Fundamental Rights Officer shall perform the following tasks:

(a) advise the staff of the FIU on any activity carried out by the FIU where the Fundamental Rights Officer deems it necessary, or where requested by the staff, without impeding or delaying those activities;

(b) promote and monitor the FIU's compliance with fundamental rights;

(c) provide non-binding opinions on the compliance of FIU's activities with fundamental rights;

(d) inform the head of the FIU about possible violations of fundamental rights in the course of the FIU's activities.

3. The FIU shall ensure that the Fundamental Rights Officer does not receive any instructions regarding the exercise of the Fundamental Rights Officer's tasks.

*Article 21*

**Access to information**

1. Member States shall ensure that FIUs, regardless of their organisational status, have access to the information that they require to fulfil their tasks, including financial, administrative and law enforcement information. Member States shall ensure that FIUs have at least:

(a) immediate and direct access to the following financial information:

(i) information contained in the national centralised automated mechanisms in accordance with Article 16;

(ii) information from obliged entities, including information on transfers of funds as defined in Article 3, point (9), of Regulation (EU) 2023/1113 and transfers of crypto-assets as defined in Article 3, point (10), of that Regulation;

(iii) information on mortgages and loans;

(iv) information contained in the national currency and currency exchange databases;

(v) information on securities;

(b) immediate and direct access to the following administrative information:

(i) fiscal data, including data held by tax and revenue authorities as well as data obtained pursuant to Article 8(3a) of Council Directive 2011/16/EU ([40]);

(ii) information on public procurement procedures for goods or services, or concessions;

([40]) Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC (OJ L 64, 11.3.2011, p. 1).

(iii) information from BARIS as referred to in Article 16, as well as from national real estate registers or electronic data retrieval systems and land and cadastral registers;

(iv) information contained in national citizenship and population registers of natural persons;

(v) information contained in national passports and visas registers;

(vi) information contained in cross-border travel databases;

(vii) information contained in commercial databases, including business and company registers and databases of politically exposed persons;

(viii) information contained in national motor vehicles, aircraft and watercraft registers;

(ix) information contained in national social security registers;

(x) customs data, including cross-border physical transfers of cash;

(xi) information contained in national weapons and arms registers;

(xii) information contained in national beneficial ownership registers;

(xiii) data available through the interconnection of central registers in accordance with Article 10(19);

(xiv) information contained in registers of non-profit organisations;

(xv) information held by national financial supervisors and regulators, in accordance with Article 61 and Article 67 (2);

(xvi) databases storing data on CO2 emission trading established pursuant to Commission Regulation (EU) No 389/2013 ([41]);

(xvii) information on annual financial statements by companies;

(xviii) national migration and immigration registers;

(xix) information held by commercial courts;

(xx) information held in insolvency databases and by insolvency practitioners;

(xxi) information on funds and other assets frozen or immobilised pursuant to targeted financial sanctions;

(c) direct or indirect access to the following law enforcement information:

(i) any type of information or data which is already held by competent authorities in the context of preventing, detecting, investigating or prosecuting criminal offences;

(ii) any type of information or data which is held by public authorities or by private entities in the context of preventing, detecting, investigating or prosecuting criminal offences and which is available to competent authorities without the taking of coercive measures under national law.

The information referred to in point (c) of the first subparagraph shall include criminal records, information on investigations, information on the freezing or seizure of assets, or on other investigative or provisional measures and information on convictions and on confiscations.

Member States may allow the restriction of access to the law enforcement information referred to in point (c) of the first subparagraph on a case-by-case basis, where the provision of such information is likely to jeopardise an ongoing investigation.

([41]) Commission Regulation (EU) No 389/2013 of 2 May 2013 establishing a Union Registry pursuant to Directive 2003/87/EC of the European Parliament and of the Council, Decisions No 280/2004/EC and No 406/2009/EC of the European Parliament and of the Council and repealing Commission Regulations (EU) No 920/2010 and (EU) No 1193/2011 (OJ L 122, 3.5.2013, p. 1).

2. Access to the information listed in paragraph 1 shall be considered direct and immediate where the information is contained in an IT database, register or data retrieval system from which the FIU can retrieve the information without any intermediate steps, or where the following conditions are met:

(a) the entities or authorities holding the information provide it expeditiously to FIUs; and

(b) no entity, authority or third party is able to interfere with the requested data or the information to be provided.

3. Member States shall ensure that, whenever possible, the FIU is granted direct access to the information listed in paragraph 1, first subparagraph, point (c). In cases where FIU is provided with indirect access to information, the entity or authority holding the requested information shall provide it in a timely manner.

4. In the context of its functions, each FIU shall be able to request, obtain and use information from any obliged entity to perform its functions pursuant to Article 19(3) of this Directive, even if no prior report is filed pursuant to Article 69(1), the first subparagraph, point (a), or Article 70(1), of Regulation (EU) 2024/1624. Obliged entities shall not be obliged to comply with requests for information made pursuant to this paragraph when they concern information obtained in the situations referred to in Article 70(2) of that Regulation.

*Article 22*

**Responses to requests for information**

1. Member States shall ensure that FIUs are able to respond in a timely manner to reasoned requests for information justified by concerns relating to money laundering, its predicate offences or terrorist financing by the competent authorities referred to in Article 2(1), points (44)(c) and (d), of Regulation (EU) 2024/1624 in their respective Member State where that information is already held by the FIU and is necessary on a case-by-case basis. The decision on conducting the dissemination of information shall remain with the FIU.

Where there are objective grounds for assuming that the provision of such information would have a negative impact on ongoing investigations or analyses, or, in exceptional circumstances, where disclosure of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested, the FIU shall not be obliged to comply with the request for information.

In such cases, the FIU shall provide the reasons in writing to the requesting authority.

2. Competent authorities shall provide feedback to the FIU about the use made of, and the usefulness of, the information provided in accordance with this Article and Article 19(3), and about the outcome of actions taken and of investigations performed on the basis of that information. Such feedback shall be provided as soon as possible and in any case, in an aggregated form, at least on an annual basis, in such a way as to allow the FIU to improve its operational analysis function.

*Article 23*

**Provision of information to supervisors**

1. Member States shall ensure that FIUs provide supervisors, spontaneously or upon request, information that may be relevant for the purposes of supervision pursuant to Chapter IV, including at least information on:

(a) the quality and quantity of suspicious transaction reports submitted by obliged entities;

(b) the quality and timeliness of responses provided by obliged entities to FIU requests pursuant to Article 69(1), the first subparagraph, point (b), of Regulation (EU) 2024/1624;

(c) relevant results of strategic analyses carried out pursuant to Article 19(3), point (b), of this Directive, as well as any relevant information on money laundering, its predicate offences and terrorist financing trends and methods, including geographical, cross-border and emerging risks.

2. Member States shall ensure that FIUs notify supervisors whenever information in their possession indicates potential breaches by obliged entities of Regulations (EU) 2024/1624 and (EU) 2023/1113.

3. Except where strictly necessary for the purposes of paragraph 2, Member States shall ensure that information provided by FIUs pursuant to this Article does not contain any information on specific natural or legal persons nor cases including natural or legal persons subject to an ongoing analysis or investigation or which may lead to the identification of natural or legal persons.

*Article 24*

**Suspension or withholding of consent**

1. Member States shall ensure that FIUs are empowered to take urgent action, directly or indirectly, where there is a suspicion that a transaction is related to money laundering or terrorist financing, to suspend or withhold consent to that transaction.

Member States shall ensure that, where the need to suspend or withhold consent to a transaction is established on the basis of a suspicion reported pursuant to Article 69 of Regulation (EU) 2024/1624, the suspension or withholding of consent is imposed on the obliged entity within the period referred to in Article 71 of that Regulation. Where the need to suspend a transaction is based on the analytical work of the FIU, regardless of whether a prior report has been filed by the obliged entity, the suspension shall be imposed as soon as possible by the FIU.

The suspension or withholding of consent to a transaction shall be imposed by the FIU in order to preserve the funds, to perform its analyses, including the analysis of the transaction, to assess whether the suspicion is confirmed and if so, to disseminate the results of the analyses to the relevant competent authorities to allow for the adoption of appropriate measures.

Member States shall lay down the period of suspension or withholding of consent applicable for the FIUs analytical work which shall not exceed 10 working days. Member States may lay down a longer period where, pursuant to national law, FIUs perform the function of tracing, seizing, freezing or confiscating criminal assets. Where a longer period of suspension or withholding of consent is laid down, Member States shall ensure that FIUs exercise their function subject to appropriate national safeguards, such as the possibility for the person whose transaction has been suspended to challenge that suspension before a court.

Member States shall ensure that FIUs are empowered to lift the suspension or withholding of consent at any time where they conclude that the suspension or withholding of consent is no longer necessary to fulfil objectives set out in the third subparagraph.

Member States shall ensure that FIUs are empowered to suspend or withhold consent as referred to in this paragraph at the request of an FIU from another Member State.

2. Where there is a suspicion that a bank account or payment account, a crypto-asset account or a business relationship is related to money laundering or terrorist financing, Member States shall ensure that the FIU is empowered to take urgent action, directly or indirectly, to suspend the use of that account or to suspend the business relationship in order to preserve the funds, to perform its analyses, to assess whether the suspicion is confirmed and if so, to disseminate the results of the analyses to the relevant competent authorities to allow for the adoption of appropriate measures.

Member States shall lay down the period of suspension applicable for the FIUs analytical work which shall not exceed 5 working days. Member States may lay down a longer period where, pursuant to national law, FIUs perform the function of tracing, seizing, freezing or confiscating criminal assets. Where a longer period of suspension is laid down, Member States shall ensure that FIUs exercise their function subject to appropriate national safeguards, such as the possibility for the person whose bank account or payment account, crypto-asset account or business relationship is suspended to challenge that suspension before a court.

Member States shall ensure that FIUs are empowered to lift the suspension at any time where they conclude that the suspension is no longer necessary to fulfil objectives set out in the first subparagraph.

Member States shall ensure that FIUs are empowered to suspend the use of an account or suspend a business relationship as referred to in this paragraph at the request of an FIU from another Member State.

3. The imposition of a suspension or the withholding of consent in accordance with this Article shall not attach liability of any kind to the FIU or its directors or employees.

*Article 25*

**Instructions to monitor transactions or activities**

Member States shall ensure that FIUs are empowered to instruct obliged entities to monitor, for a period to be specified by the FIU, the transactions or activities that are being carried out through one or more bank accounts or payment accounts or crypto-asset accounts or other business relationships managed by the obliged entity for persons who present a significant risk of money laundering, its predicate offences or terrorist financing. Member States shall also ensure that FIUs are empowered to instruct the obliged entity to report on the results of the monitoring.

Member States shall ensure that FIUs are empowered to impose monitoring measures as referred to in this Article at the request of an FIU from another Member State.

*Article 26*

**Alerts to obliged entities**

1. Member States shall ensure that FIUs are able to alert obliged entities of information relevant for the performance of customer due diligence pursuant to Chapter III of Regulation (EU) 2024/1624. That information shall include:

(a) types of transactions or activities that present a significant risk of money laundering, its predicate offences and terrorist financing;

(b) specific persons that present a significant risk of money laundering, its predicate offences and terrorist financing;

(c) specific geographic areas that present a significant risk of money laundering, its predicate offences and terrorist financing.

2. The requirement referred in paragraph 1 shall apply for a period laid down in national law, which shall not exceed 6 months.

3. FIUs shall provide obliged entities with strategic information about typologies, risk indicators and trends in money laundering and terrorist financing on an annual basis.

*Article 27*

**FIU annual report**

Each Member State shall ensure that its FIU publishes an annual report on its activities. The report shall contain statistics on:

(a) the follow up given by the FIU to suspicious transaction and activity reports it has received;

(b) suspicious transaction reports submitted by obliged entities;

(c) disclosures by supervisors and central registers;

(d) disseminations to competent authorities and follow-up given to those disseminations;

(e) requests submitted to and received from other FIUs;

(f) requests submitted to and received from competent authorities referred to in Article 2(1), point (44)(c), of Regulation (EU) 2024/1624;

(g) human resources allocated;

(h) data on cross-border physical transfers of cash transmitted by customs authorities pursuant to Article 9 of Regulation (EU) 2018/1672.

The report referred to in the first paragraph shall also contain information on the trends and typologies identified in the files disseminated to other competent authorities. The information contained in the report shall not permit the identification of any natural or legal person.

*Article 28*

**Feedback by FIU**

1. Member States shall ensure that FIUs provide obliged entities with feedback on the reporting of suspicions pursuant to Article 69 of Regulation (EU) 2024/1624. Such feedback shall cover at least the quality of the information provided, the timeliness of reporting, the description of the suspicion and the documentation provided at submission stage.

Feedback pursuant to this Article shall not be understood as encompassing each report submitted by obliged entities.

The FIU shall provide feedback at least once per year, whether provided to the individual obliged entity or to groups or categories of obliged entities, taking into consideration the overall number of suspicious transactions reported by the obliged entities.

Feedback shall also be made available to supervisors to allow them to perform risk-based supervision in accordance with Article 40.

FIUs shall report on an annual basis to AMLA on the provision of feedback to obliged entities pursuant to this Article, and shall provide statistics on the number of suspicious transaction reports submitted by the categories of obliged entities.

By 10 July 2028, AMLA shall issue recommendations to FIUs on best practices and approaches towards the provision of feedback, including on the type and frequency of feedback.

The obligation to provide feedback shall not jeopardise any ongoing analytical work carried out by the FIU or any investigation or administrative action subsequent to the dissemination by the FIU, and shall not affect the applicability of data protection and confidentiality requirements.

2. Member States shall ensure that FIUs provide customs authorities with feedback, at least on an annual basis, on the effectiveness of and follow-up to the information transmitted pursuant to Article 9 of Regulation (EU) 2018/1672.

*Article 29*

**Cooperation between FIUs**

Member States shall ensure that FIUs cooperate with each other to the greatest extent possible, regardless of their organisational status.

*Article 30*

**Protected channels of communication**

1. A system for the exchange of information between FIUs of Member States (FIU.net) shall be set up. FIU.net shall ensure the secure communication and exchange of information and shall be capable of producing a written record of all processing activities. FIU.net may also be used for communications with FIUs' counterparts in third countries and with other authorities and with Union bodies, offices and agencies. FIU.net shall be managed by AMLA.

FIU.net shall be used for the exchange of information between FIUs and AMLA for the purposes of joint analyses pursuant to Article 32 of this Directive and Article 40 of Regulation (EU) 2024/1620.

2. Member States shall ensure that FIUs exchange information pursuant to Article 31 and 32 using FIU.net. In the event of a technical failure of FIU.net, the information shall be transmitted by any other appropriate means ensuring a high level of data security and data protection.

Exchanges of information between FIUs and their counterparts in third countries that are not connected to FIU.net shall take place through protected channels of communication.

3. Member States shall ensure that, in order to fulfil their tasks as laid down in this Directive, FIUs cooperate to the greatest extent possible in the application of state-of-the-art technologies in accordance with their national law.

Member States shall also ensure that FIUs cooperate to the greatest extent possible in the application of solutions developed and managed by AMLA in accordance with Article 5(5), point (i), Article 45(1), point (d), and Article 47 of Regulation (EU) 2024/1620.

4. Member States shall ensure that FIUs are able to use the functionalities of the FIU.net to cross-match, on a hit/no-hit basis, the data they make available on FIU.net, with the data made available on that system by other FIUs and Union bodies, offices and agencies insofar as such cross-matching falls within the respective mandates of those Union bodies, offices and agencies.

5. AMLA may suspend the access of an FIU or counterpart in a third country or Union body, office or agency to FIU.net where it has grounds to believe that such access would jeopardise the implementation of this Chapter and the security and confidentiality of the information held by FIUs and exchanged through FIU.net, including where there are concerns in relation to an FIU's independence and autonomy.

*Article 31*

**Exchange of information between FIUs**

1. Member States shall ensure that FIUs exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering, its predicate offences, or terrorist financing, and the natural or legal person involved, regardless of the type of predicate offences that may be involved, and even if the type of predicate offences that may be involved is not identified at the time of the exchange.

A request shall contain the relevant facts, background information, reasons for the request, links with the country of the requested FIU and how the information sought will be used.

When an FIU receives a report pursuant to Article 69(1), the first subparagraph, point (a), of Regulation (EU) 2024/1624 which concerns another Member State, it shall promptly forward the report, or all the relevant information obtained from it, to the FIU of that other Member State.

2. By 10 July 2026, AMLA shall develop draft implementing technical standards and submit them to the Commission for adoption. Those draft implementing technical standards shall specify the format to be used for the exchange of the information referred to in paragraph 1.

Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph in accordance with Article 53 of Regulation (EU) 2024/1620.

3. By 10 July 2026, AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall specify the relevance and selection criteria when determining whether a report submitted pursuant to Article 69(1), first subparagraph, point (a), of Regulation (EU) 2024/1624 concerns another Member State as referred to in paragraph 1, third subparagraph, of this Article.

Power is delegated to the Commission to supplement this Directive by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 49 to 52 of Regulation (EU) 2024/1620.

4. By 10 July 2028, AMLA shall issue guidelines addressed to FIUs on the procedures to be put in place when forwarding and receiving a report pursuant to Article 69(1), the first subparagraph, point (a), of Regulation (EU) 2024/1624 which concerns another Member State, and the follow-up to be given to that report.

5. Member States shall ensure that the FIU to whom the request is made is required to use the whole range of its available powers which it would normally use domestically for receiving and analysing information when it replies to a request for information referred to in paragraph 1 from another FIU.

When an FIU seeks to obtain additional information from an obliged entity established in another Member State which operates on the territory of its Member State, the request shall be addressed to the FIU of the Member State in whose territory the obliged entity is established. That FIU shall obtain information in accordance with Article 69(1) of Regulation (EU) 2024/1624 and transfer the answers promptly.

6. Member States shall ensure that where an FIU is requested to provide information pursuant to paragraph 1, it shall respond to the request as soon as possible and in any case no later than 5 working days after the receipt of the request if the FIU is either in possession of the requested information or the requested information is held in a database or register which is directly accessible by the requested FIU. In exceptional, duly justified cases, this deadline may be extended to a maximum of 10 working days. Where the requested FIU is unable to obtain the requested information, it shall inform the requesting FIU thereof.

7. Member States shall ensure that in exceptional, justified and urgent cases and, by way of derogation from paragraph 6, where pursuant to paragraph 1 an FIU is requested to provide information which is either held in a database or registry directly accessible by the requested FIU or which is already in its possession, the requested FIU shall provide that information no later than 1 working day after the receipt of the request.

If the requested FIU is unable to respond within 1 working day or cannot access the information directly, it shall provide a justification. Where the provision of the information requested within 1 working day would put a disproportionate burden on the requested FIU, it may postpone the provision of the information. In that case, the requested FIU shall immediately inform the requesting FIU of such postponement. The requested FIU may extend to a maximum of 3 working days the deadline to reply to a request for information.

8. An FIU may refuse to exchange information only in exceptional circumstances where the exchange could be contrary to fundamental principles of its national law. Those exceptional circumstances shall be specified in a way which prevents misuse of, and undue limitations on, the free exchange of information for analytical purposes.

By 10 July 2028, Member States shall notify to the Commission the exceptional circumstances referred to in the first subparagraph. Member States shall update such notifications where changes to the exceptional circumstances identified at national level occur.

The Commission shall publish the consolidated list of notifications referred to in the second subparagraph.

9. By 10 July 2029, the Commission shall submit a report to the European Parliament and to the Council assessing whether the exceptional circumstances notified pursuant to paragraph 8 are justified.

*Article 32*

**Joint analyses**

1. Member States shall ensure that their FIUs are able to carry out joint analyses of suspicious transactions and activities.

2. For the purpose of paragraph 1 of this Article, the relevant FIUs, assisted by AMLA in accordance with Article 40 of Regulation (EU) 2024/1620, shall set up a joint analysis team for a specific purpose and limited period, which may be extended by mutual consent, to carry out operational analyses of suspicious transactions or activities involving one or more of the FIUs setting up the team.

3. A joint analysis team may be set up where:

(a) an FIU's operational analyses require difficult and demanding analyses with links to other Member States;

(b) a number of FIUs are conducting operational analyses in which the circumstances of the case justify concerted action in the Member States involved.

A request for the setting up of a joint analysis team may be made by any of the FIUs concerned or AMLA pursuant to Article 44 of Regulation (EU) 2024/1620.

4. Member States shall ensure that the staff member of their FIU allocated to the joint analysis team is able, in accordance with the applicable national law and within the limits of the staff member's competence, to provide the team with information available to its FIU for the purpose of the analysis conducted by the team.

5. Where the joint analysis team needs assistance from a FIU other than those which are part of the team, it might request that other FIU to:

(a) join the joint analysis team;

(b) submit financial intelligence and financial information to the joint analysis team.

6. Member States shall ensure that FIUs are able to invite third parties, including Union bodies, offices and agencies, to take part in the joint analyses where relevant for the purposes of the joint analyses and where such participation falls within the respective mandates of those third parties.

Member States shall ensure that the FIUs participating in the joint analyses determine the conditions that apply in relation to the participation of third parties and put in place measures guaranteeing the confidentiality and security of the information exchanged. Member States shall ensure that the information exchanged is used solely for the purposes for which that joint analysis was set up.

*Article 33*

**Use by FIUs of information exchanged between them**

Information and documents received pursuant to Articles 29, 31 and 32 shall be used for the accomplishment of the FIU's tasks as laid down in this Directive. When exchanging information and documents pursuant to Articles 29 and 31, the transmitting FIU may impose restrictions and conditions for the use of that information, except where the transmission consists of a report submitted by an obliged entity pursuant to Article 69(1) of Regulation (EU) 2024/1624, or information derived therefrom, which concerns another Member State where the obliged entity operates through the freedom to provide services and which includes no link to the Member State of the transmitting FIU. The receiving FIU shall comply with those restrictions and conditions.

Member States shall ensure that FIUs designate at least one contact person or point to be responsible for receiving requests for information from FIUs in other Member States.

*Article 34*

**Consent to further dissemination of information exchanged between FIUs**

1. Member States shall ensure that the information exchanged pursuant to Articles 29, 31 and 32 is used only for the purpose for which it was sought or provided and that any dissemination of that information by the receiving FIU to any other authority, agency or department, or any use of this information for purposes other than those originally approved, is made subject to the prior consent by the FIU providing the information.

The requirements of the first subparagraph of this paragraph shall not apply where the information provided by the FIU consists of a report submitted by an obliged entity pursuant to Article 69(1) of Regulation (EU) 2024/1624 which concerns another Member State where the obliged entity operates through the freedom to provide services and which has no link to the Member State of the FIU providing the information.

2. Member States shall ensure that the requested FIU's prior consent to disseminate the information to competent authorities is granted promptly and to the largest extent possible, regardless of the type of predicate offences and whether or not the predicate offence has been identified. The requested FIU shall not refuse its consent to such dissemination unless this would fall beyond the scope of application of its AML/CFT provisions or could lead to impairment of an investigation, or would otherwise not be in accordance with fundamental principles of national law of that Member State. Any such refusal to grant consent shall be appropriately explained. The cases where FIUs may refuse to grant consent shall be specified in a way which prevents misuse of, and undue limitations to, the dissemination of information to competent authorities.

3. By 10 July 2028, Member States shall notify to the Commission the exceptional circumstances in which dissemination would not be in accordance with fundamental principles of national law referred to in paragraph 2. Member States shall update such notifications where changes to the exceptional circumstances identified at national level occur.

The Commission shall publish the consolidated list of notifications referred to in the first subparagraph.

4. By 10 July 2029, the Commission shall submit a report to the European Parliament and to the Council assessing whether the exceptional circumstances notified pursuant to paragraph 3 are justified.

*Article 35*

**Effect of criminal law provisions**

Differences between national law definitions of predicate offences shall not impede the ability of FIUs to provide assistance to another FIU and shall not limit the exchange, dissemination and use of information pursuant to Articles 31, 32, 33 and 34.

*Article 36*

**Confidentiality of reporting**

1. Member States shall ensure that FIUs have in place mechanisms to protect the identity of the obliged entities and their employees, or persons in an equivalent position, including agents and distributors, who report suspicions pursuant to Article 69(1), first subparagraph, point (a), of Regulation (EU) 2024/1624.

2. Member States shall ensure that FIUs do not disclose the source of the report referred to in paragraph 1 of this Article, when responding to requests for information by competent authorities pursuant to Article 22 or when disseminating the results of their analyses pursuant to Article 19. This paragraph is without prejudice to the applicable national criminal procedural law.

CHAPTER IV

**ANTI-MONEY LAUNDERING SUPERVISION**

*SECTION 1*

***General provisions***

*Article 37*

**Powers and resources of national supervisors**

1. Each Member State shall ensure that all obliged entities established in its territory, except for the circumstances covered in Article 38, are subject to adequate and effective supervision. To that end, each Member State shall appoint one or more supervisors to monitor effectively, and to take the measures necessary to ensure compliance by the obliged entities with Regulations (EU) 2024/1624 and (EU) 2023/1113.

Where, for reasons of overriding general interest, Member States have introduced specific authorisations requirements for obliged entities to operate in their territory under the freedom to provide services, they shall ensure that the activities carried out by the obliged entities under those specific authorisations are subject to supervision by their national supervisors, regardless of whether the authorised activities are carried out through an infrastructure in their territory or remotely. Member States shall also ensure that supervision under this subparagraph is notified to the supervisors of the Member State where the head office of the obliged entity is located.

This paragraph shall not apply when AMLA acts as a supervisor.

2. Member States shall ensure that supervisors have adequate financial, human and technical resources to perform their tasks as listed in paragraph 5. Member States shall ensure that staff of those authorities are of high integrity and appropriately skilled, and maintain high professional standards, including standards of confidentiality, data protection and standards addressing conflicts of interest.

3. In the case of the obliged entities referred to in Article 3, points (3)(a) and (b), of Regulation (EU) 2024/1624, Member States may allow the function referred to in paragraph 1 of this Article to be performed by self-regulatory bodies, provided that those self-regulatory bodies have the powers referred to in paragraph 6 of this Article and have adequate financial, human and technical resources to perform their functions. Member States shall ensure that staff of those bodies are of high integrity and appropriately skilled, and that they maintain high professional standards, including standards of confidentiality, data protection and standards addressing conflicts of interest.

4. Where a Member State has entrusted the supervision of a category of obliged entities to more than one supervisor, it shall ensure that those supervisors supervise obliged entities in a consistent and efficient manner across the sector. To that end, the Member State shall appoint a leading supervisor or establish a coordination mechanism among those supervisors.

Where a Member State has entrusted the supervision of all obliged entities to more than one supervisor, it shall establish a coordination mechanism among those supervisors to ensure that obliged entities are effectively supervised to the highest standards. Such a coordination mechanism shall include all supervisors, except where:

(a) supervision is entrusted to a self-regulatory body, in which case the public authority referred to in Article 52 shall participate in the coordination mechanism;

(b) supervision of a category of obliged entities is entrusted to several supervisors, in which case the lead supervisor shall participate in the coordination mechanism; where no lead supervisor has been appointed, supervisors shall designate a representative among them.

5. For the purposes of paragraph 1, Member States shall ensure that the national supervisors perform the following tasks:

(a) to disseminate relevant information to obliged entities pursuant to Article 39;

(b) to decide on those cases where the specific risks inherent in a sector are clear and understood and individual documented risk assessments pursuant to Article 10 of Regulation (EU) 2024/1624 are not required;

(c) to verify the adequacy and implementation of the internal policies, procedures and controls of obliged entities pursuant to Chapter II of Regulation (EU) 2024/1624 and of the human resources allocated to the performance of the tasks required under that Regulation, as well as, for supervisors of collective investment undertakings, to decide on those cases where the collective investment undertaking may outsource the reporting of suspicious activities pursuant to Article 18(7) of Regulation (EU) 2024/1624 to a service provider;

(d) to regularly assess and monitor the money laundering and terrorist financing risks as well as the risks of non-implementation and evasion of targeted financial sanctions the obliged entities are exposed to;

(e) to monitor compliance by obliged entities with regard to their obligations in relation to targeted financial sanctions;

(f) to conduct all the necessary off-site investigations, on-site inspections and thematic checks and any other inquiries, assessments and analyses necessary to verify that obliged entities comply with Regulation (EU) 2024/1624, and with any administrative measures taken pursuant to Article 56 of this Directive;

(g) to take appropriate supervisory measures to address any breaches of applicable requirements by the obliged entities identified in the process of supervisory assessments and follow up on the implementation of such measures.

6. Member States shall ensure that supervisors have adequate powers to perform their tasks as provided for in paragraph 5, including the power to:

(a) compel the production of any information from obliged entities which is relevant for monitoring and verifying compliance with Regulation (EU) 2024/1624 or Regulation (EU) 2023/1113 and to perform checks, including from service providers to whom the obliged entity has outsourced part of its tasks to meet the requirements of those Regulations;

(b) apply appropriate and proportionate administrative measures to remedy the situation in the case of breaches, including through the imposition of pecuniary sanctions in accordance with Section 4 of this Chapter.

7. Member States shall ensure that financial supervisors and supervisors in charge of gambling service providers have powers additional to those referred to in paragraph 6, including the power to inspect the business premises of the obliged entity without prior announcement where the proper conduct and efficiency of an inspection so require, and that they have all the necessary means to carry out such inspection.

For the purposes of the first subparagraph, the supervisors shall at least be able to:

(a) examine the books and records of the obliged entity and take copies or extracts from such books and records;

(b) obtain access to any software, databases, IT tools or other electronic means of recording information used by the obliged entity;

(c) obtain written or oral information from any person responsible for AML/CFT internal policies, procedures and controls or their representatives or staff, as well as any representative or staff of entities to which the obliged entity has outsourced tasks pursuant to Article 18 of Regulation (EU) 2024/1624, and interview any other person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation.

*Article 38*

**Supervision of forms of infrastructure of certain intermediaries operating under the freedom to provide services**

1. Where the activities of the following obliged entities are carried out in their territory under the freedom to provide services through agents or distributors, or through other types of infrastructure, including when those activities are carried out under an authorisation obtained under Directive 2013/36/EU, Member States shall ensure that such activities are subject to supervision by their national supervisors:

(a) electronic money issuers as defined in Article 2, point (3), of Directive 2009/110/EC of the European Parliament and of the Council ([42]);

(b) payment service providers as defined in Article 4, point (11), of Directive (EU) 2015/2366; and

(c) crypto-asset service providers.

For the purposes of the first subparagraph, the supervisors of the Member State where the activities are carried out shall monitor effectively and ensure compliance with the Regulations (EU) 2024/1624 and (EU) 2023/1113.

2. By way of derogation from paragraph 1, supervision of agents, distributors, or other types of infrastructure, referred to in that paragraph shall be carried out by the supervisor of the Member State where the head office of the obliged entity is located where:

(a) the criteria set out in the regulatory technical standard referred to in Article 41(2) are not met; and

(b) the supervisor of the Member State where those agents, distributors, or other types of infrastructure, are located notifies the supervisor of the Member State where the head office of the obliged entity is located that, considering the limited infrastructure of the entity in its territory, supervision of the activities referred to in paragraph 1 is to be carried out by the supervisor of the Member State where the head office of the obliged entity is located.

3. For the purposes of this Article, the supervisor of the Member State where the head office of the obliged entity is located and the supervisor of the Member State where the obliged entity operates under the freedom to provide services through agents or distributors, or through other types of infrastructure, shall provide each other any information necessary to assess whether the criteria referred to in paragraph 2, point (a), are met, including on any change in the circumstances of the obliged entity that may have an impact on the satisfaction of those criteria.

([42]) Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

4. Member States shall ensure that the supervisor of the Member State where the head office of the obliged entity is located informs the obliged entity within 2 weeks of receiving the notification under paragraph 2, point (b), that it will supervise the activities of the agents, distributors, or other types of infrastructure, through which the obliged entities operates under the freedom to provide services in another Member State, and of any subsequent change to their supervision.

5. This Article shall not apply when AMLA acts as a supervisor.

*Article 39*

**Provision of information to obliged entities**

1. Member States shall ensure that supervisors make information on money laundering and terrorist financing available to the obliged entities under their supervision.

2. The information referred to in paragraph 1 shall include the following:

(a) the risk assessment at Union level conducted by the Commission pursuant to Article 7 and any relevant recommendation by the Commission on the basis of that Article;

(b) national or sectoral risk assessments carried out pursuant to Article 8;

(c) relevant guidelines, recommendations and opinions issued by AMLA in accordance with Articles 54 and 55 of Regulation (EU) 2024/1620;

(d) information on third countries identified pursuant to Chapter III, Section 2, of Regulation (EU) 2024/1624;

(e) any guidance and report produced by AMLA, other supervisors and, where relevant, the public authority overseeing self-regulatory bodies, the FIU or any other competent authority or international organisations and standard setters regarding money laundering and terrorist financing methods which might apply to a sector and indications which may facilitate the identification of transactions or activities at risk of being linked to money laundering and terrorist financing in that sector, as well as guidance on obliged entities' obligations in relation to targeted financial sanctions.

3. Member States shall ensure that supervisors carry out outreach activities, as appropriate, to inform the obliged entities under their supervision of their obligations.

4. Member States shall ensure that supervisors make information on persons or entities designated in relation to targeted financial sanctions and UN financial sanctions available to the obliged entities under their supervision immediately.

*Article 40*

**Risk-based supervision**

1. Member States shall ensure that supervisors apply a risk-based approach to supervision. To that end, Member States shall ensure that they:

(a) have a clear understanding of the risks of money laundering and terrorist financing present in their Member State;

(b) assess all relevant information on the specific domestic and international risks associated with customers, products and services of the obliged entities;

(c) base the frequency and intensity of on-site, off-site and thematic supervision on the risk profile of obliged entities, and on the risks of money laundering and terrorist financing in that Member State.

For the purposes of point (c) of the first subparagraph of this paragraph, supervisors shall draw up annual supervisory programmes, which shall take into account the timing and resources needed to react promptly in the event of objective and significant indications of breaches of Regulations (EU) 2024/1624 and (EU) 2023/1113.

2. By 10 July 2026, AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall set out the benchmarks and a methodology for assessing and classifying the inherent and residual risk profile of obliged entities, as well as the frequency at which such risk profile shall be reviewed. Such frequency shall take into account any major events or developments in the management and operations of the obliged entity, as well as the nature and size of the business.

Power is delegated to the Commission to supplement this Directive by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 49 to 52 of Regulation (EU) 2024/1620.

3. By 10 July 2028, AMLA shall issue guidelines addressed to supervisors on:

(a) the characteristics of a risk-based approach to supervision;

(b) the measures to be put in place within supervisors to ensure adequate and effective supervision, including to train their staff;

(c) the steps to be taken when conducting supervision on a risk-sensitive basis.

Where relevant, the guidelines referred to in the first subparagraph shall take into account the outcomes of the assessments carried out pursuant to Articles 30 and 35 of Regulation (EU) 2024/1620.

4. Member States shall ensure that supervisors take into account the degree of discretion allowed to the obliged entity, and appropriately review the risk assessments underlying this discretion, and the adequacy of its internal policies, procedures and controls.

5. Member States shall ensure that supervisors prepare a detailed annual activity report and that a summary of that report is made public. That summary shall not contain confidential information and shall include:

(a) the categories of obliged entities under the supervision and the number of obliged entities per category;

(b) a description of the powers with which the supervisors are entrusted and the tasks assigned to them and, where relevant, of mechanisms referred to in Article 37(4) in which they participate and, for the lead supervisor, a summary of the coordination activities carried out;

(c) an overview of the supervisory activities carried out.

*Article 41*

**Central contact points**

1. For the purposes of Article 37(1) and Article 38(1), Member States may require electronic money issuers, payment service providers and crypto-asset service providers operating establishments in their territory other than a subsidiary or a branch, or operating in their territory through agents or distributors, or through other types of infrastructure, under the freedom to provide services, to appoint a central contact point in their territory. That central contact point shall ensure, on behalf of the obliged entity, compliance with AML/CFT rules and shall facilitate supervision by supervisors, including by providing supervisors with documents and information on request.

2. By 10 July 2026, AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall set out the criteria for determining the circumstances in which the appointment of a central contact point pursuant to paragraph 1 is appropriate, and the functions of the central contact points.

Power is delegated to the Commission to supplement this Directive by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 49 to 52 of Regulation (EU) 2024/1620.

*Article 42*

**Disclosure to FIUs**

1. Member States shall ensure that if, in the course of the checks carried out on the obliged entities, or in any other way, supervisors discover facts that could be related to money laundering, its predicate offences or terrorist financing, they shall promptly inform the FIU.

2. Member States shall ensure that supervisors empowered to oversee the stock, foreign exchange and financial derivatives markets, inform the FIU if they discover information that could be related to money laundering or terrorist financing.

3. Member States shall ensure that compliance with the requirements of this Article does not replace any obligation for supervisory authorities to report to the relevant competent authorities any criminal activity they uncover or become aware of in the context of their supervisory activities.

*Article 43*

**Provision of information to FIUs**

Member States shall ensure that supervisors communicate to the FIU at least the following information:

(a) the list of establishments operating in the respective Member State and the list of infrastructure under their supervision pursuant to Article 38(1), and of any changes to those lists;

(b) any relevant findings indicating serious weaknesses of the reporting systems of obliged entities;

(c) the results of the risk assessments performed pursuant to Article 40, in aggregated form.

*Article 44*

**General principles regarding supervisory cooperation**

Member States shall ensure that supervisors cooperate with each other to the greatest extent possible, regardless of their respective nature or status. Such cooperation may include conducting, within the powers of the requested supervisor, inquiries on behalf of a requesting supervisor, and the subsequent exchange of the information obtained through such inquiries, or facilitating the conduct of such inquiries by the requesting supervisor.

*Article 45*

**Provision of information on cross-border activities**

1. Member States shall ensure that the supervisors of the home Member State inform the supervisors of the host Member State as soon as possible, and in any case within 3 months of receiving a notification pursuant to Article 8(1) of Regulation (EU) 2024/1624 of the activities that the obliged entity intends to carry out in the host Member State.

Any subsequent change notified to the supervisors of the home Member State pursuant to Article 8(2) of Regulation (EU) 2024/1624 shall be notified to the supervisors of the host Member State as soon as possible and in any case within 1 month of receiving it.

2. Member States shall ensure that the supervisors of the home Member State share with the supervisors of the host Member State information on the activities effectively carried out by the obliged entity in the territory of the host Member State that they receive in the context of their supervisory activities, including information submitted by the obliged entities in response to supervisory questionnaires, and any relevant information connected to the activities carried out in the host Member State.

The information referred to in the first subparagraph shall be exchanged at least annually. Where that information is provided in an aggregated form, Member States shall ensure that the supervisors of the home Member State respond promptly to any request for additional information by the supervisors of the host Member State.

By way of derogation from the second subparagraph of this paragraph, Member States shall ensure that supervisors of the home Member State inform the supervisors of the host Member State immediately upon receiving notification by obliged entities pursuant to Article 8(1) of Regulation (EU) 2024/1624 that activities in the host Member State have commenced.

*Article 46*

**Provisions related to cooperation in the context of group supervision**

1. In the case of credit institutions and financial institutions that are part of a group, Member States shall ensure that, for the purposes laid down in Article 37(1), financial supervisors of the home Member State and those of the host Member State cooperate with each other to the greatest extent possible, regardless of their respective nature or status. They shall also cooperate with AMLA when acting as a supervisor.

2. Except when AMLA acts as a supervisor, Member States shall ensure that the financial supervisors of the home Member State supervise the effective implementation of the group-wide policies, procedures and controls referred to in Chapter II, Section 2, of Regulation (EU) 2024/1624. Member States shall also ensure that financial supervisors of the host Member State supervise the compliance of the establishments located in the territory of their Member State with Regulations (EU) 2024/1624 and (EU) 2023/1113.

3. For the purposes of this Article, and except in cases where AML/CFT supervisory colleges are set up in accordance with Article 49, Member States shall ensure that financial supervisors provide one another with any information they require for the exercise of their supervisory tasks, whether on request or on their own initiative. In particular, financial supervisors shall exchange any information that could significantly influence the assessment of the inherent or residual risk exposure of a credit institution or financial institution in another Member State, including:

(a) identification of the group's legal, governance and organisational structure, covering all subsidiaries and branches;

(b) relevant information on the beneficial owners and senior management, including outcomes of fit and proper checks, whether carried out under this Directive or under other Union legal acts;

(c) policies, procedures and controls in place within the group;

(d) customer due diligence information, including customer files and records of transactions;

(e) adverse developments in relation to the parent undertaking, subsidiaries or branches, which could seriously affect other parts of the group;

(f) pecuniary sanctions that financial supervisors intend to impose and administrative measures that financial supervisors intend to apply in accordance with Section 4 of this Chapter.

Member States shall also ensure that financial supervisors are able to conduct, within their powers, inquiries on behalf of a requesting supervisor, and to share the information obtained through such inquiries, or to facilitate the conduct of such inquiries by the requesting supervisor.

4. By 10 July 2026, AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall detail the respective duties of the home and host supervisors, and the modalities of cooperation between them.

Power is delegated to the Commission to supplement this Directive by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 49 to 52 of Regulation (EU) 2024/1620.

5. Financial supervisors may refer to AMLA any of the following situations:

(a) where a financial supervisor has not communicated the information referred to in paragraph 3;

(b) where a request for cooperation has been rejected or has not been acted upon within a reasonable time;

(c) where there is a disagreement on the basis of objective reasons on breaches identified and on the pecuniary sanctions to be imposed or administrative measures to be applied on the entity or group to remedy those breaches.

AMLA may act in accordance with the powers conferred on it under Article 33 of Regulation (EU) 2024/1620. When doing so, AMLA shall provide its opinion on the subject-matter of the request within 1 month.

6. Member States shall ensure that this Article also applies to the supervision of:

(a) groups of obliged entities in the non-financial sector;

(b) obliged entities operating under the freedom to provide services without any infrastructure in another Member States than the Member State where they are established, where the supervision of activities in that other Member State is carried out by the supervisors of that other Member State pursuant to Article 37(1), second subparagraph.

Where the situations referred to in paragraph 5 arise in relation to non-financial supervisors, AMLA may act in accordance with the powers conferred on it under Article 38 of Regulation (EU) 2024/1620.

Member States shall also ensure that in cases where obliged entities in the non-financial sector are part of structures which share common ownership, management or compliance control, including networks or partnerships, non-financial supervisors cooperate and exchange information.

*Article 47*

**Supervisory cooperation regarding obliged entities carrying out cross-border activities**

1. Where obliged entities that are not part of a group carry out cross-border activities as referred to in Article 54(1) and supervision is shared between the supervisors of the home and host Member States pursuant to Articles 37(1) and 38(1), Member States shall ensure that those supervisors cooperate with each other to the greatest extent possible and assist each other in the performance of supervision pursuant to Articles 37(1) and 38(1).

For the purposes of the first subparagraph, and except in cases where AML/CFT supervisory colleges are set up in accordance with Article 49, Member States shall ensure that supervisors:

(a) provide one another with any information they require for the exercise of their supervisory tasks, whether on request or on their own initiative, including the information referred to in Article 46(3), first subparagraph, points (a), (b) and (d), where that information is necessary for the performance of supervisory tasks;

(b) inform one another of any adverse development in relation to the obliged entity, its establishments or types of infrastructure, which could seriously affect the entity's compliance with applicable requirements, and pecuniary sanctions they intend to impose, or administrative measures they intend to apply in accordance with Section 4 of this Chapter;

(c) are able to conduct, within their powers, inquiries on behalf of a requesting supervisor, and to share the information obtained through such inquiries, or to facilitate the conduct of such inquiries by the requesting supervisor.

This paragraph shall also apply in the case of obliged entities that are established in a single Member State and operate under the freedom to provide services in another Member State without any infrastructure, where the supervision of activities in that other Member State is carried out by the supervisors of that Member State pursuant to Article 37(1), second subparagraph.

2. Where supervision of the obliged entity and any of its types of infrastructure in other Member States is entrusted to the supervisors of the home Member State pursuant to Article 38(2), Member States shall ensure that the supervisors of the home Member State inform regularly the supervisors of the host Member State of the measures in place within the obliged entity, and compliance of that entity with applicable requirements, including those in place in the host Member State. Where serious, repeated or systematic breaches are identified, the supervisors of the home Member State shall promptly inform the supervisors of the host Member State of those breaches and of any pecuniary sanctions they intend to impose and administrative measures they intend to apply to remedy them.

Member States shall ensure that supervisors of the host Member State provide assistance to the supervisors of the home Member State to ensure the verification of compliance by the obliged entity with legal requirements. In particular, Member States shall ensure that supervisors of the host Member State inform the supervisors of the home Member State of any serious doubts that they have regarding compliance of the obliged entity with applicable requirements, and that they share any information they hold in this regard with the supervisors of the home Member State.

This paragraph shall also apply in the case of obliged entities that are established in a single Member State and operate under the freedom to provide services in another Member State without any infrastructure, except for cases where the supervision of activities in that other Member State is carried out by the supervisors of that other Member State pursuant to Article 37(1), second subparagraph.

3. Supervisors shall be able to refer to AMLA any of the following situations:

(a) where a supervisor has not communicated the information referred to in paragraph 1, second subparagraph, points (a) and (b) or paragraph 2, first and second subparagraph;

(b) where a request for cooperation has been rejected or has not been acted upon within a reasonable time;

(c) where there is a disagreement on the basis of objective reasons on breaches identified and on the pecuniary sanctions to be imposed on or administrative measures to be applied to the entity to remedy those breaches.

AMLA shall act in accordance with the powers conferred on it under Articles 33 and 38 of Regulation (EU) 2024/1620. AMLA shall provide its opinion on the subject-matter of the request within 1 month.

*Article 48*

**Exchange of information in relation to implementation of group-wide policies in third countries**

Supervisors, including AMLA, shall inform each other of instances in which the law of a third country does not permit the implementation of the policies, procedures and controls required under Article 16 of Regulation (EU) 2024/1624. In such cases, coordinated actions may be taken by supervisors to pursue a solution. In assessing which third countries do not permit the implementation of the policies, procedures and controls required under Article 16 of Regulation (EU) 2024/1624, supervisors shall take into account any legal constraints that may hinder proper implementation of those policies, procedures and controls, including professional secrecy, an insufficient level of data protection and other constraints limiting the exchange of information that may be relevant for that purpose.

*SECTION 2*

***Cooperation within AML/CFT supervisory colleges and with counterparts in third countries***

*Article 49*

**AML/CFT supervisory colleges in the financial sector**

1. Member States shall ensure that dedicated AML/CFT supervisory colleges are set up by the financial supervisor in charge of the parent undertaking of a group of credit institutions or financial institutions or of the head office of a credit institution or financial institution in any of the following situations:

(a) where a credit institution or a financial institution, including groups thereof, has set up establishments in at least two different Member States other than the Member State where its head office is located;

(b) where a third-country credit institution or financial institution has set up establishments in at least three Member States.

2. The permanent members of the college shall be the financial supervisor in charge of the parent undertaking or of the head office, the financial supervisors in charge of establishments in host Member States and the financial supervisors in charge of infrastructure in host Member States pursuant to Article 38.

3. This Article shall not apply when AMLA acts as a supervisor.

4. The activities of the AML/CFT supervisory colleges shall be proportionate to the level of the money laundering and terrorist financing risks to which the credit institution or financial institution or the group is exposed, and to the scale of its cross-border activities.

5. For the purposes of paragraph 1, Member States shall ensure that financial supervisors identify:

(a) all credit institutions or financial institutions that have been authorised in their Member State and that have establishments in other Member States or third countries;

(b) all establishments set up by credit institutions or financial institutions in other Member States or third countries;

(c) establishments set up in their territory by credit institutions or financial institutions from other Member States or third countries.

6. In situations other than those covered by Article 38, where credit institutions or financial institutions carry out activities in other Member States under the freedom to provide services, the financial supervisor of the home Member State may invite the financial supervisors of those Member States to participate in the college as observers.

7. Where a group of credit institutions or financial institutions includes any obliged entity in the non-financial sector, the financial supervisor setting up the college shall invite the supervisors of those obliged entities to participate in the college.

8. Member States may allow the setting-up of AML/CFT supervisory colleges when a credit institution or financial institution established in the Union has set up establishments in at least two third countries. Financial supervisors may invite their counterparts in those third countries to set up such college. The financial supervisors participating in the college shall establish a written agreement detailing the conditions and procedures of the cooperation and exchange of information.

9. Member States shall ensure that colleges are used, among others, for exchanging information, providing mutual assistance or coordinating the supervisory approach to the group or institution, including, where relevant, the taking of appropriate and proportionate measures to address serious breaches of Regulations (EU) 2024/1624 and (EU) 2023/1113 that are detected at the level of the group or of the credit institution or financial institution or across the establishments set up by the group or institution in the jurisdiction of a supervisor participating in the college.

10. AMLA may attend the meetings of the AML/CFT supervisory colleges and shall facilitate their work in accordance with Article 31 of Regulation (EU) 2024/1620. Where AMLA decides to participate in the meetings of an AML/CFT supervisory college, it shall have the status of an observer.

11. Financial supervisors may allow their counterparts in third countries to participate as observers in AML/CFT supervisory colleges in the case referred to in paragraph 1, point (b) or where Union groups or credit institutions or financial institutions operate branches and subsidiaries in those third countries, provided that:

(a) the third-country counterparts submit a request for participation and the members of the college agree with their participation, or the members of the college agree to invite those third-country counterparts;

(b) Union data protection rules concerning data transfers are complied with;

(c) the third-country counterparts sign the written agreement referred to in paragraph 8, third sentence, and share within the college the relevant information they possess for the supervision of the credit institutions or financial institutions or of the group;

(d) the information disclosed is subject to a guarantee of professional secrecy requirements at least equivalent to that referred to in Article 67(1) and is used solely for the purposes of performing the supervisory tasks of the participating financial supervisors or of the counterparts in third countries.

Member States shall ensure that financial supervisors setting up the colleges carry out an assessment of whether the conditions of the first subparagraph are met and submit it to the permanent members of the college. That assessment shall be carried out prior to the third-country counterpart being allowed to join the college and may be repeated as necessary thereafter. The financial supervisors of the home Member State may seek the support of AMLA for the performance of that assessment.

12. Where deemed necessary by the permanent members of the college, additional observers may be invited, provided that confidentiality requirements are complied with. Observers may include prudential supervisors, including the ECB acting in accordance with Council Regulation (EU) No 1024/2013 ([43]), as well as the European Supervisory Authorities and FIUs.

13. Where the members of a college disagree on the measures to be taken in relation to an obliged entity, they may refer the matter to AMLA and request its assistance in accordance with Article 33 of Regulation (EU) 2024/1620.

14. By 10 July 2026, AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall specify:

(a) the general conditions for the functioning, on a risk-sensitive basis, of the AML/CFT supervisory colleges in the financial sector, including the terms of cooperation between permanent members and with observers, and the operational functioning of such colleges;

(b) the template for the written agreement to be signed by financial supervisors pursuant to paragraph 8;

(c) any additional measure to be implemented by the colleges when groups include obliged entities in the non-financial sector;

(d) conditions for the participation of financial supervisors in third countries.

Power is delegated to the Commission to supplement this Directive by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 49 to 52 of Regulation (EU) 2024/1620.

*Article 50*

**AML/CFT supervisory colleges in the non-financial sector**

1. Member States shall ensure that the non-financial supervisors in charge of the parent undertaking of a group of obliged entities in the non-financial sector or of the head office of an obliged entity in the non-financial sector are able to set up dedicated AML/CFT supervisory colleges in any of the following situations:

(a) where an obliged entity in the non-financial sector, or a group thereof, has set up establishments in at least two different Member States other than the Member State where its head office is located;

(b) where a third-country entity subject to AML/CFT requirements other than a credit institution or a financial institution has set up establishments in at least three Member States.

This paragraph shall also apply to structures which share common ownership, management or compliance control, including networks or partnerships to which group-wide requirements apply pursuant to Article 16 of Regulation (EU) 2024/1624.

The permanent members of the college shall be the non-financial supervisor in charge of the parent undertaking or of the head office and the non-financial supervisors in charge of establishments in host Member States or of supervision of that obliged entity in other Member States in the cases covered by Article 37(1), second subparagraph.

2. Member States shall ensure that where the non-financial supervisor in charge of the parent undertaking of a group or of the head office of an obliged entity does not set up a college, non-financial supervisors referred to in paragraph 1, second subparagraph, point (b), can submit an opinion that, having regard to the money laundering and terrorist financing risks to which the obliged entity or group is exposed and the scale of its cross-border activities, a college shall be set up. That opinion shall be submitted by at least two non-financial supervisors and addressed to:

(a) the non-financial supervisor in charge of the parent undertaking of a group or of the head office of an obliged entity;

([43]) Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

(b) AMLA;

(c) all other non-financial supervisors.

Where the non-financial supervisor referred to in point (a) of the first subparagraph of this paragraph is a self-regulatory body, that opinion shall also be submitted to the public authority in charge of overseeing that self-regulatory body pursuant to Article 52.

3. Where, after an opinion is submitted pursuant to paragraph 2, the non-financial supervisor in charge of the parent undertaking of a group or of the head office of an obliged entity still considers that it is not necessary to set up a college, Member States shall ensure that the other non-financial supervisors are able to set up the college, provided that it is composed of at least two members. In those cases, those non-financial supervisors shall decide among them who is the supervisor in charge of the college. The non-financial supervisor in charge of the parent undertaking of a group or of the head office of an obliged entity shall be informed of the activities of the college and be able to join the college at any time.

4. For the purposes of paragraph 1, Member States shall ensure that non-financial supervisors identify:

(a) all obliged entities in the non-financial sector that have their head office in their Member State and that have establishments in other Member States or third countries;

(b) all establishments set up by those obliged entities in other Member States or third countries;

(c) establishments set up in their territory by obliged entities in the non-financial sector from other Member States or third countries.

5. Where obliged entities in the non-financial sector carry out activities in other Member States under the freedom to provide services, the non-financial supervisor of the home Member State may invite the non-financial supervisors of those Member States to participate in the college as observers.

6. Where a group in the non-financial sector includes any credit institution or financial institution, but their presence in the group does not meet the threshold for setting up a college pursuant to Article 49, the supervisor setting up the college shall invite the financial supervisors of those credit institutions or financial institutions to participate in the college.

7. Member States may allow the setting up of AML/CFT supervisory colleges when an obliged entity in the non-financial sector established in the Union has set up establishments in at least two third countries. Non-financial supervisors may invite their counterparts in those third countries to set up such college. The non-financial supervisors participating in the college shall establish a written agreement detailing the conditions and procedures for the cooperation and exchange of information.

Where the college is set up in relation to obliged entities referred to in Article 3, points (3)(a) and (b), of Regulation (EU) 2024/1624 or groups thereof, the written agreement referred to in the first subparagraph of this paragraph shall also include procedures to ensure that no information collected pursuant to Article 21(2) of Regulation (EU) 2024/1624 is shared, unless the second subparagraph of Article 21(2) applies.

8. Member States shall ensure that colleges are used, among others, for exchanging information, providing mutual assistance or coordinating the supervisory approach to the group or obliged entity, including, where relevant, the taking of appropriate and proportionate measures to address serious breaches of Regulations (EU) 2024/1624 and (EU) 2023/1113 that are detected at the level of the group or of the obliged entity, or across the establishments set up by the group or obliged entity in the jurisdiction of a supervisor participating in the college.

9. AMLA may attend the meetings of the AML/CFT supervisory colleges and shall facilitate their work in accordance with Article 36 of Regulation (EU) 2024/1620. Where AMLA decides to participate in the meetings of an AML/CFT supervisory college, it shall have the status of an observer.

10. Non-financial supervisors may allow their counterparts in third countries to participate in AML/CFT supervisory colleges as observers in the case referred to in paragraph 1, point (b), or where Union obliged entities in the non-financial sector or groups thereof operate branches and subsidiaries in those third countries, provided that:

(a) the third-country counterparts submit a request for participation and the members of the college agree with their participation, or the members of the college agree to invite those third-country counterparts;

(b) Union data protection rules concerning data transfers are complied with;

(c) the third-country counterparts sign the written agreement referred to in paragraph 7 and share within the college the relevant information they possess for the supervision of the obliged entity or of the group;

(d) the information disclosed is subject to a guarantee of professional secrecy requirements at least equivalent to that referred to in Article 67(1) and is used solely for the purposes of performing the supervisory tasks of the participating non-financial supervisors or of the counterparts in third countries.

Member States shall ensure that non-financial supervisors in charge of the parent undertaking of a group or of the head office of an obliged entity or, in the cases covered by paragraph 3, of the college carry out an assessment of whether the conditions of the first subparagraph of this paragraph are met and submit it to the permanent members of the college. That assessment shall be carried out prior to the third-country counterpart being allowed to join the college and may be repeated as necessary thereafter. The non-financial supervisors in charge of the assessment may seek the support of AMLA for the performance of that assessment.

11. Where deemed necessary by the permanent members of the college, additional observers may be invited, provided that confidentiality requirements are complied with. Observers may include FIUs.

12. Where the members of a college disagree on the measures to be taken in relation to an obliged entity, they may refer the matter to AMLA and request its assistance in accordance with Article 38 of Regulation (EU) 2024/1620. AMLA shall provide its opinion on the matter of disagreement within 2 months.

13. By 10 July 2026, AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall specify:

(a) the general conditions for the functioning of the AML/CFT supervisory colleges in the non-financial sector, including the terms of cooperation between permanent members and with observers, and the operational functioning of such colleges;

(b) the template for the written agreement to be signed by non-financial supervisors pursuant to paragraph 7;

(c) conditions for the participation of non-financial supervisors in third countries;

(d) any additional measure to be implemented by the colleges when groups include credit institutions or financial institutions.

Power is delegated to the Commission to supplement this Directive by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 49 to 52 of Regulation (EU) 2024/1620.

14. By 10 July 2029 and every 2 years thereafter, AMLA shall issue an opinion on the functioning of AML/CFT supervisory colleges in the non-financial sector. That opinion shall include:

(a) an overview of the colleges set up by non-financial supervisors;

(b) an assessment of the actions taken by those colleges and the level of cooperation attained, including difficulties faced in the functioning of the colleges.

*Article 51*

**Cooperation with supervisors in third countries**

1. Member States shall ensure that supervisors are able to conclude cooperation agreements providing for cooperation and exchanges of confidential information with their counterparts in third countries. Such cooperation agreements shall comply with applicable data protection rules and be concluded on the basis of reciprocity and subject to a guarantee of

professional secrecy requirements at least equivalent to that referred to in Article 67(1). Confidential information exchanged in accordance with those cooperation agreements shall be used for the purpose of performing the supervisory tasks of those authorities only.

Where the information exchanged originates in another Member State, it shall only be disclosed with the explicit consent of the supervisor which shared it and, where appropriate, solely for the purposes for which that supervisor gave its consent.

2. For the purposes of paragraph 1, AMLA shall provide such assistance as necessary to assess the equivalence of professional secrecy requirements applicable to the third-country counterpart.

3. Member States shall ensure that supervisors notify any agreement signed pursuant to this Article to AMLA within 1 month of its signature.

4. By 10 July 2029, AMLA shall develop draft implementing technical standards and submit them to the Commission for adoption. Those draft implementing technical standards shall specify the template to be used for the conclusion of cooperation agreements referred to in paragraph 1.

Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph in accordance with Article 53 of Regulation (EU) 2024/1620.

*SECTION 3*

***Specific provisions relating to self-regulatory bodies***

*Article 52*

**Oversight of self-regulatory bodies**

1. Where Member States decide, pursuant to Article 37(3) of this Directive, to allow self-regulatory bodies to perform supervision of the obliged entities referred to in Article 3, points (3)(a) and (b), of Regulation (EU) 2024/1624, they shall ensure that the activities of such self-regulatory bodies in the performance of such functions are subject to oversight by a public authority.

2. The public authority overseeing self-regulatory bodies shall be responsible for ensuring an adequate and effective supervisory system for the obliged entities referred to in Article 3, points (3)(a) and (b), of Regulation (EU) 2024/1624, including by:

(a) verifying that any self-regulatory body performing the functions or aspiring to perform the functions referred to in Article 37(1) satisfies the requirements of paragraph 3 of that Article;

(b) issuing guidance as regards the performance of the functions referred to in Article 37(1);

(c) ensuring that self-regulatory bodies perform their functions under Section 1 of this Chapter adequately and effectively;

(d) reviewing the exemptions granted by self-regulatory bodies from the obligation to draw up an individual documented risk assessment pursuant to Article 37(5), point (b);

(e) regularly informing self-regulatory bodies of any activity planned or task carried out by AMLA that is relevant for the performance of their supervisory function, and in particular the planning of peer reviews in accordance with Article 35 of Regulation (EU) 2024/1620.

3. Member States shall ensure that the public authority overseeing self-regulatory bodies is granted adequate powers to discharge its responsibilities under paragraph 2. As a minimum, Member States shall ensure that the public authority has the power to:

(a) compel the production of any information that is relevant to monitoring compliance and performing checks, except for any information collected by obliged entities referred to in Article 3, points (3)(a) and (b), of Regulation (EU) 2024/1624 in the course of ascertaining the legal position of their client, subject to the conditions of Article 21(2) of that Regulation, or for performing the task of defending or representing that client in, or concerning, judicial proceedings,

including providing advice on instituting or avoiding such proceedings; whether such information was collected before, during or after such proceedings;

(b) issue instructions to a self-regulatory body for the purpose of remedying a failure to perform its functions under Article 37(1) or to comply with the requirements of paragraph 6 of that Article, or to prevent any such failures.

When issuing instructions to a self-regulatory body in accordance with point (b) of the first subparagraph, the public authority shall consider any relevant guidance it provided or that has been provided by AMLA.

4. Member States shall ensure that the public authority overseeing self-regulatory bodies performs its functions free of undue influence.

Member States shall also ensure that the staff of the public authority overseeing self-regulatory bodies are bound by professional secrecy requirements equivalent to those laid down in Article 67, and that they maintain high professional standards, including high professional standards of confidentiality and data protection, and are of high integrity. Member States shall ensure that the public authority overseeing self-regulatory bodies has in place procedures to prevent and manage conflicts of interest.

5. Member States may provide for effective, proportionate and dissuasive measures or sanctions for failures by self-regulatory bodies to comply with any request or instruction or other measure taken by the authority pursuant to paragraph 2 or 3.

6. Member States shall ensure that the public authority overseeing self-regulatory bodies informs the authorities competent for investigating and prosecuting criminal activities timely, directly or through the FIU, of any breaches which are subject to criminal sanctions that it detects in the performance of its tasks.

7. The public authority overseeing self-regulatory bodies shall publish an annual report containing information about:

(a) the number and nature of breaches detected by each self-regulatory body and the pecuniary sanctions imposed on or administrative measures applied to obliged entities;

(b) the number of suspicious transactions reported by the obliged entities subject to supervision by each self-regulatory body to the FIU, whether submitted directly pursuant to Article 69(1) of Regulation (EU) 2024/1624, or forwarded by each self-regulatory body to the FIU pursuant to Article 70(1) of that Regulation;

(c) the number and description of pecuniary sanctions and periodic penalty payments imposed or administrative measures applied under Section 4 of this Chapter by each self-regulatory body to ensure compliance by obliged entities with Regulation (EU) 2024/1624 referred to in Article 55(1) of this Directive;

(d) the number and description of measures taken by the public authority overseeing self-regulatory bodies under this Article and the number of instructions issued to self-regulatory bodies.

The report referred to in the first subparagraph shall be made available on the website of the public authority overseeing self-regulatory bodies and submitted to the Commission and AMLA.

*SECTION 4*

***Pecuniary sanctions and administrative measures***

*Article 53*

**General provisions**

1. Member States shall ensure that obliged entities can be held liable for breaches of Regulations (EU) 2024/1624 and (EU) 2023/1113 in accordance with this Section.

2. Without prejudice to the right of Member States to provide for and impose criminal sanctions, Member States shall lay down rules on pecuniary sanctions and administrative measures and ensure that supervisors may impose such pecuniary sanctions and apply administrative measures with respect to breaches of Regulation (EU) 2024/1624 or Regulation (EU) 2023/1113 and shall ensure that they are enforced. Any sanction imposed or measure applied pursuant to this Section shall be effective, proportionate and dissuasive.

3. By way of derogation from paragraph 2, where the legal system of a Member State does not provide for administrative sanctions, this Article may be applied in such a manner that the pecuniary sanction is initiated by the supervisor and imposed by a judicial authority, while ensuring that those legal remedies are effective and have an equivalent effect to the pecuniary sanctions imposed by supervisors. In any event, the pecuniary sanctions imposed shall be effective, proportionate and dissuasive.

The Member States referred to in the first subparagraph shall communicate to the Commission the measures of national law which they adopt pursuant to this paragraph by 10 July 2027 and, without delay, any subsequent amendments thereto.

4. In the event of a breach of Regulations (EU) 2024/1624 and (EU) 2023/1113, Member States shall ensure that where obligations apply to legal persons, pecuniary sanctions can be imposed and administrative measures can be applied not only to the legal person, but also to the senior management and to other natural persons who under national law are responsible for the breach.

Member States shall ensure that where supervisors identify breaches which are subject to criminal sanctions, they inform the authorities competent for investigating and prosecuting criminal activities in a timely manner.

5. In accordance with this Directive and with national law, pecuniary sanctions shall be imposed and administrative measures shall be applied in any of the following ways:

(a) directly by the supervisors;

(b) in cooperation between the supervisors and other authorities;

(c) under the responsibility of the supervisors by delegation to other authorities;

(d) by application by the supervisors to the competent judicial authorities.

By 10 October 2027, Member States shall notify to the Commission and AMLA the information as regards the arrangements relating to the imposition of pecuniary sanctions or application of administrative measures pursuant to this paragraph, including, where relevant, information whether certain sanctions or measures require the recourse to a specific procedure.

6. Member States shall ensure that, when determining the type and level of pecuniary sanctions or administrative measures, supervisors take into account all relevant circumstances, including where applicable:

(a) the gravity and the duration of the breach;

(b) the number of instances the breach was repeated;

(c) the degree of responsibility of the natural or legal person held responsible;

(d) the financial strength of the natural or legal person held responsible, including in light of its total turnover or annual income;

(e) the benefit derived from the breach by the natural or legal person held responsible, insofar as it can be determined;

(f) the losses to third parties caused by the breach, insofar as they can be determined;

(g) the level of cooperation of the natural or legal person held responsible with the competent authority;

(h) previous breaches by the natural or legal person held responsible.

7. Member States shall ensure that legal persons can be held liable for the breaches of Regulation (EU) 2024/1624 or Regulation (EU) 2023/1113 committed on their behalf or for their benefit by any person, acting individually or as part of a body of that legal person and having a leading position within that legal person, based on any of the following:

(a) a power to represent the legal person;

(b) an authority to take decisions on behalf of the legal person;

(c) an authority to exercise control within the legal person.

8. Member States shall ensure that legal persons can be held liable where the lack of supervision or control by a person as referred to in paragraph 7 of this Article has made possible the breaches of Regulation (EU) 2024/1624 or Regulation (EU) 2023/1113 by a person under their authority on behalf of or for the benefit of the legal person.

9. In the exercise of their powers to impose pecuniary sanctions and apply administrative measures, supervisors shall cooperate closely and, where relevant, coordinate their actions with other authorities as appropriate, in order to ensure that those pecuniary sanctions or administrative measures produce the desired results and coordinate their action when dealing with cross-border cases.

10. By 10 July 2026, AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall set out:

(a) indicators to classify the level of gravity of breaches;

(b) criteria to be taken into account when setting the level of pecuniary sanctions or applying administrative measures pursuant to this Section;

(c) a methodology for the imposition of periodic penalty payments pursuant to Article 57, including their frequency.

Power is delegated to the Commission to supplement this Directive by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 49 to 52 of Regulation (EU) 2024/1620.

11. By 10 July 2026, AMLA shall issue guidelines on the base amounts for the imposing of pecuniary sanctions relative to turnover, broken down per type of breach and category of obliged entities.

*Article 54*

**Supervisory measures towards establishments of obliged entities and certain activities carried out under the freedom to provide services**

1. In the case of establishments of obliged entities that do not as such qualify as credit institutions or financial institutions or of types of infrastructure of obliged entities over which the supervisor of the host Member State exercises supervision pursuant to Article 38(1), paragraphs 2 to 5 of this Article shall apply.

2. Where the supervisors of the host Member State identify breaches of applicable requirements, they shall request the obliged entities operating through the establishments or types of infrastructure as referred to in paragraph 1 to comply with the applicable requirements and inform the supervisors of the home Member State of the breaches identified within those obliged entities and of the request to comply.

3. Where the obliged entities fail to take the necessary action, the supervisors of the host Member State shall inform the supervisors of the home Member State accordingly.

The supervisors of the home Member State shall act promptly and take all appropriate measures to ensure that the obliged entity concerned remedies the breaches detected in its establishments or types of infrastructure in the host Member State. The supervisors of the home Member State shall inform the supervisors of the host Member State of any actions taken pursuant to this paragraph.

4. By way of derogation from paragraph 3, in situations of serious, repeated or systematic breaches by obliged entities operating through establishments or other types of infrastructure in their territory as referred to in paragraph 1 that require immediate remedies, supervisors of the host Member State shall be allowed at their own initiative to take appropriate and proportionate measures to address those breaches. Those measures shall be temporary and be terminated when the breaches identified are addressed, including with the assistance of or in cooperation with the supervisors of the home Member State of the obliged entity.

Member States shall ensure that the supervisors of the host Member State inform the supervisor of the home Member State of the obliged entity immediately upon identification of the serious, repeated or systematic breaches and upon taking any measure pursuant to the first subparagraph, unless measures are taken in cooperation with the supervisors of the home Member State.

5. Where the supervisors of the home and host Member States disagree on the measures to be taken in relation to an obliged entity, they may refer the matter to AMLA and request its assistance in accordance with Articles 33 and 38 of Regulation (EU) 2024/1620. AMLA shall provide its opinion on the matter of disagreement within 1 month.

*Article 55*

**Pecuniary sanctions**

1. Member States shall ensure that pecuniary sanctions are imposed on obliged entities for serious, repeated or systematic breaches, whether committed intentionally or negligently, of the requirements laid down in the following provisions of Regulation (EU) 2024/1624:

(a) Chapter II (Internal policies, procedures and controls of obliged entities);

(b) Chapter III (Customer due diligence);

(c) Chapter V (Reporting obligations);

(d) Article 77 (Record retention).

Member States shall also ensure that pecuniary sanctions can be imposed where obliged entities have not complied with administrative measures applied to them pursuant to Article 56 of this Directive or for breaches that are not serious, repeated or systematic.

2. Member States shall ensure that in the cases referred to in paragraph 1, first subparagraph, the maximum pecuniary sanctions that can be imposed amount at least to twice the amount of the benefit derived from the breach where that benefit can be determined, or at least EUR 1 000 000, whichever is higher.

For Member States whose currency is not the euro, the value referred to in the first subparagraph shall be the corresponding value in the national currency on 9 July 2024.

3. Member States shall ensure that, by way of derogation from paragraph 2, where the obliged entity concerned is a credit institution or a financial institution, the following pecuniary sanctions can also be imposed:

(a) in the case of a legal person, maximum pecuniary sanctions of at least EUR 10 000 000 or, in the Member States whose currency is not the euro, the corresponding value in the national currency on 9 July 2024, or 10 % of the total annual turnover according to the latest available accounts approved by the management body, whichever is higher; where the obliged entity is a parent undertaking or a subsidiary of a parent undertaking which is required to prepare consolidated financial accounts in accordance with Article 22 of Directive 2013/34/EU of the European Parliament and of the Council ([44]), the relevant total annual turnover shall be the total annual turnover or the corresponding type of income in accordance with the relevant accounting regime according to the last available consolidated accounts approved by the management body of the ultimate parent undertaking;

(b) in the case of a natural person, maximum pecuniary sanctions of at least EUR 5 000 000 or, in the Member States whose currency is not the euro, the corresponding value in the national currency on 9 July 2024.

4. Member States may empower competent authorities to impose pecuniary sanctions exceeding the amounts referred to in paragraphs 2 and 3.

5. Member States shall ensure that, when determining the amount of the pecuniary sanction, the ability of the obliged entity to pay the sanction is taken into account and that, where the pecuniary sanction may affect compliance with prudential regulation, supervisors consult the authorities competent to supervise compliance by the obliged entities with relevant Union legal acts.

([44]) Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).

*Article 56*

**Administrative measures**

1. Member States shall ensure that supervisors are able to apply administrative measures to an obliged entity where they identify:

(a) breaches of Regulation (EU) 2024/1624 or Regulation (EU) 2023/1113, either in combination with pecuniary sanctions for serious, repeated and systematic breaches, or on their own;

(b) weaknesses in the internal policies, procedures and controls of the obliged entity that are likely to result in breaches of the requirements referred to in point (a) and administrative measures can prevent the occurrence of those breaches or reduce the risk thereof;

(c) that the obliged entity has internal policies, procedures and controls that are not commensurate with the risks of money laundering, its predicate offences or terrorist financing to which the entity is exposed.

2. Member States shall ensure that the supervisors are able at least to:

(a) issue recommendations;

(b) order obliged entities to comply, including to implement specific corrective measures;

(c) issue a public statement which identifies the natural or legal person and the nature of the breach;

(d) issue an order requiring the natural or legal person to cease the conduct and to desist from repetition of that conduct;

(e) restrict or limit the business, operations or network of institutions comprising the obliged entity, or to require the divestment of activities;

(f) where an obliged entity is subject to an authorisation, withdraw or suspend the authorisation;

(g) require changes in the governance structure.

3. Member States shall ensure that the supervisors are able, by means of the administrative measures referred to in paragraph 2, in particular to:

(a) require the provision of any data or information necessary for the fulfilment of their tasks pursuant to this Chapter without undue delay, to require the submission of any document, or impose additional or more frequent reporting requirements;

(b) require the reinforcement of the internal policies, procedures and controls;

(c) require the obliged entity to apply a specific policy or requirements relating to categories of or individual clients, transactions, activities or delivery channels that pose high risks;

(d) require the implementation of measures to bring about the reduction of the money laundering or terrorist financing risks inherent in the activities and products of the obliged entity;

(e) impose a temporary ban against any person discharging managerial responsibilities in an obliged entity, or any other natural person who has been held responsible for the breach from exercising managerial functions in obliged entities.

4. The administrative measures referred to in paragraph 2 shall be accompanied, where relevant, by binding deadlines for their implementation. Member States shall ensure that supervisors follow up and assess the implementation by the obliged entity of the actions requested.

5. Member States may empower supervisors to apply additional types of administrative measures to those referred to in paragraph 2.

*Article 57*

**Periodic penalty payments**

1. Member States shall ensure that, where obliged entities fail to comply with administrative measures applied by the supervisor pursuant to Article 56(2), points (b), (d), (e) and (g), within the applicable deadlines, supervisors are able to impose periodic penalty payments in order to compel compliance with those administrative measures.

2. The periodic penalty payments shall be effective and proportionate. The periodic penalty payments shall be imposed until the obliged entity or person concerned complies with the relevant administrative measures.

3. Notwithstanding paragraph 2, in the case of legal persons, the amount of the periodic penalty payment shall not exceed 3 % of their average daily turnover in the preceding business year or, in the case of natural persons, that amount shall not exceed 2 % of their average daily income in the preceding calendar year.

4. Periodic penalty payments shall only be imposed for a period of no more than 6 months following the supervisor's decision. Where, upon expiry of that period, the obliged entity has not yet complied with the administrative measure, Member States shall ensure that supervisors can impose periodic penalty payments for an additional period of no more than 6 months.

5. Member States shall ensure that a decision imposing a periodic penalty payment can be taken as of the date of the application of the administrative measure.

The periodic penalty payment shall apply as of the date when that decision is taken.

*Article 58*

**Publication of pecuniary sanctions, administrative measures and periodic penalty payments**

1. Member States shall ensure that supervisors publish on their website, in an accessible format, decisions imposing pecuniary sanctions, applying administrative measures referred to in Article 56(2), points (c) to (g), pursuant to Article 56 (1), point (a), or imposing periodic penalty payments.

2. Member States shall ensure that the decisions referred to in paragraph 1 are published by the supervisor immediately after the persons responsible for the breach are informed of those decisions.

By way of derogation from the first subparagraph, where the publication concerns administrative measures against which there is an appeal and that do not aim to remedy serious, repeated and systematic breaches, Member States may allow for the publication of those administrative measures to be deferred until expiry of the deadline for lodging an appeal.

Where the publication refers to decisions against which there is an appeal, supervisors shall also publish, immediately, on their website such information and any subsequent information on an appeal, and the outcome of such appeal. Any decision annulling a previous decision to impose a pecuniary sanction, apply an administrative measure, or impose a periodic penalty payment, shall also be published.

3. The publication shall include at least information on the type and nature of the breach and the identity of the persons responsible, as well as, for pecuniary sanctions and periodic penalty payments, their amounts. Member States shall not be obliged to apply this subparagraph to decisions applying administrative measures that are of an investigatory nature, or which are taken pursuant to Article 56(2), points (a) and (c).

Where the publication of the identity of the persons responsible as referred to in the first subparagraph or the personal data of such persons is considered by the supervisors to be disproportionate following a case-by-case assessment, or where publication jeopardises the stability of financial markets or an on-going investigation, supervisors shall:

(a) delay the publication of the decision until the moment at which the reasons for not publishing it cease to exist;

(b) publish the decision on an anonymous basis in a manner in accordance with national law, if such anonymous publication ensures the effective protection of the personal data concerned; in that case, the publication of the relevant data may be postponed for a reasonable period if it is foreseen that within that period the reasons for anonymous publication shall cease to exist;

(c) not publish the decision at all in the event that the options set out in points (a) and (b) are considered insufficient to ensure one of the following:

(i) that the stability of financial markets would not be put in jeopardy;

(ii) the proportionality of the publication of the decision with regard to pecuniary sanctions and administrative measures for breaches which are deemed to be of a minor nature.

4. Member States shall ensure that any publication in accordance with this Article remains on the website of the supervisors for a period of 5 years after its publication. However, personal data contained in the publication shall only be kept on the website of the supervisors for the period which is necessary in accordance with the applicable data protection rules and in any case for no more than 5 years.

*Article 59*

**Exchange of information on pecuniary sanctions and administrative measures**

1. Member States shall ensure that their supervisors and, where relevant, the public authority overseeing self-regulatory bodies in their performance of supervisory functions, inform AMLA of all pecuniary sanctions imposed and administrative measures applied in accordance with this Section, including of any appeal in relation thereto and the outcome thereof. Such information shall also be shared with other supervisors when the pecuniary sanction or administrative measure concerns an entity operating in two or more Member States.

2. AMLA shall maintain on its website links to each supervisor's publication of pecuniary sanctions imposed and administrative measures applied in accordance with Article 58, and shall show the period for which each Member State publishes pecuniary sanctions and administrative measures.

*SECTION 5*

***Reporting of breaches***

*Article 60*

**Reporting of breaches and protection of reporting persons**

1. Directive (EU) 2019/1937 shall apply to the reporting of breaches of Regulations (EU) 2024/1624 and (EU) 2023/1113 and of this Directive, and to the protection of persons reporting such breaches and of the persons concerned by those reports.

2. Supervisory authorities shall be the authorities competent to establish external reporting channels and to follow-up on reports insofar as requirements applicable to obliged entities are concerned, in accordance with Directive (EU) 2019/1937.

3. The public authorities overseeing self-regulatory bodies referred to in Article 52 shall be the authorities competent to establish external reporting channels and to follow up on reports by self-regulatory bodies and their staff insofar as requirements applicable to self-regulatory bodies in the exercise of supervisory functions are concerned.

4. Member States shall ensure that supervisory authorities in the non-financial sector report the following, on an annual basis, to AMLA:

(a) the number of reports received pursuant to paragraph 1 and information on the share of reports that have been or are in the process of being followed-up, including whether they have been closed or are still open, and of the reports that have been dismissed;

(b) the types of irregularities reported;

(c) where reports have been followed-up, a description of the actions taken by the supervisor and, for reports that are still open, the actions which the supervisor intends to take;

(d) where reports have been dismissed, the reasons for dismissing them.

Annual reports as referred to in the first subparagraph shall not contain any information on the identity or occupation of the reporting persons, or any other information that could lead to their identification.

CHAPTER V

**COOPERATION**

*SECTION 1*

***AML/CFT cooperation***

*Article 61*

**General provisions**

1. Member States shall ensure that policy makers, the FIUs, supervisors, including AMLA, and other competent authorities, as well as tax authorities, have effective mechanisms to enable them to cooperate and coordinate domestically concerning the development and implementation of policies and activities to combat money laundering and terrorist financing and to prevent the non-implementation and evasion of targeted financial sanctions, including with a view to fulfilling their obligations under Article 8.

2. With regard to beneficial ownership information obtained by competent authorities pursuant to Chapter IV of Regulation (EU) 2024/1624 and Section 1 of Chapter II of this Directive, Member States shall ensure that competent authorities are able to provide such information to the counterpart competent authorities of other Member States or third countries in a timely manner and free of charge.

3. Member States shall not prohibit or place unreasonable or unduly restrictive conditions on the exchange of information or assistance between competent authorities and their counterparts for the purposes of this Directive. Member States shall ensure that competent authorities do not refuse a request for assistance on the grounds that:

(a) the request is also considered to involve tax matters;

(b) national law requires obliged entities to maintain secrecy or confidentiality, except in those cases where the relevant information that is sought is protected by legal privilege or where legal professional secrecy applies, as provided for in Article 70(2) of Regulation (EU) 2024/1624;

(c) there is an inquiry, investigation, proceeding or FIU analysis underway in the requested Member State, unless the assistance would impede that inquiry, investigation, proceeding or FIU analysis;

(d) the nature or status of the requesting counterpart competent authority is different from that of requested competent authority.

*Article 62*

**Communication of the list of the competent authorities**

1. In order to facilitate and promote effective cooperation, and in particular the exchange of information, Member States shall communicate to the Commission and AMLA:

(a) the list of supervisors responsible for overseeing the compliance of the obliged entities with Regulation (EU) 2024/1624, as well as, where relevant, name of the public authority overseeing self-regulatory bodies in their performance of supervisory functions under this Directive, and their contact details;

(b) the contact details of their FIU;

(c) the list of other competent national authorities.

2. For the purposes of paragraph 1, the following contact details shall be provided:

(a) a contact point or, failing that, the name and role of a contact person;

(b) the email and phone number of the contact point or, failing that, the professional email address and phone number of the contact person.

3. Member States shall ensure that the information provided to the Commission and AMLA pursuant to paragraph 1 is updated as soon as a change takes place.

4. AMLA shall publish a register of the authorities referred to in paragraph 1 on its website and facilitate the exchange of information referred to in paragraph 2 between competent authorities. The authorities in the register shall, within the scope of their powers, serve as a contact point for the counterpart competent authorities. FIUs and supervisory authorities shall also serve as a contact point for AMLA.

*Article 63*

**Cooperation with AMLA**

FIU and supervisory authorities shall cooperate with AMLA and shall provide it with all the information necessary to allow it to carry out its duties under this Directive and under Regulations (EU) 2024/1624 and (EU) 2024/1620.

*SECTION 2*

***Cooperation with other authorities and exchange of confidential information***

*Article 64*

**Cooperation in relation to credit institutions or financial institutions**

1. Member States shall ensure that financial supervisors, FIUs, and authorities competent for the supervision of credit institutions or financial institutions under other Union legal acts, cooperate closely with each other within their respective competences and provide each other with information relevant for the performance of their respective tasks. Such cooperation and information exchange shall not impinge on any ongoing inquiry, FIU analysis, investigation or proceedings in accordance with the criminal or administrative law of the Member State where the financial supervisor or authority entrusted with competences for the supervision of credit institutions or financial institutions under other legal acts is located and shall not affect professional secrecy requirements as provided in Article 67(1).

2. Member States shall ensure that, where financial supervisors identify weaknesses in the AML/CFT internal control system and application of the requirements of Regulation (EU) 2024/1624 of a credit institution which materially increase the risks to which the institution is or might be exposed, the financial supervisor immediately notifies the European Banking Authority (EBA) and the authority or body that supervises the credit institution in accordance with Directive 2013/36/EU, including the ECB acting in accordance with Regulation (EU) No 1024/2013.

In the event of potential increased risk, financial supervisors shall be able to cooperate and share information with the authorities supervising the institution in accordance with Directive 2013/36/EU and draw up a common assessment to be notified to EBA by the supervisor who first sent the notification. AMLA shall be kept informed of any such notifications.

3. Member States shall ensure that, where financial supervisors find that a credit institution has refused to establish or decided to terminate a business relationship but the documented customer due diligence pursuant to Article 21(3) of Regulation (EU) 2024/1624 does not justify such refusal, they shall inform the authority responsible for ensuring compliance by that credit institution with Directives 2014/92/EU or (EU) 2015/2366.

4. Member States shall ensure that financial supervisors cooperate with resolution authorities as defined in Article 2(1), point (18), of Directive 2014/59/EU or designated authorities as defined in Article 2(1), point (18), of Directive 2014/49/EU.

Financial supervisors shall inform the authorities referred to in the first subparagraph where, in the exercise of their supervisory activities, they identify, on AML/CFT grounds, any of the following situations:

(a) an increased likelihood of deposits becoming unavailable;

(b) a risk that a credit institution or a financial institution be deemed to be failing or likely to fail in accordance with Article 32(4) of Directive 2014/59/EU.

Upon request by the authorities referred to in the first subparagraph of this paragraph, where there is an increased likelihood of deposits becoming unavailable or a risk that a credit institution or a financial institution be deemed to be failing or likely to fail in accordance with Article 32(4) of Directive 2014/59/EU, financial supervisors shall inform those authorities of any transaction, account or business relationship under management by that credit institution or financial institution that has been suspended by the FIU pursuant to Article 24.

5. Financial supervisors shall report on an annual basis to AMLA on their cooperation with other authorities pursuant to this Article including involvement of FIUs in that cooperation.

6. By 10 July 2029, AMLA shall, in consultation with EBA, issue guidelines on cooperation between financial supervisors and the authorities referred to in paragraphs 2, 3 and 4, including on the level of involvement of FIUs in such cooperation.

*Article 65*

**Cooperation in relation to auditors**

1. Member States shall ensure that supervisors in charge of auditors and, where relevant, public authorities overseeing self-regulatory bodies pursuant to Chapter IV of this Directive, their FIU and the public authorities competent for overseeing statutory auditors and audit firms pursuant to Article 32 of Directive 2006/43/EC of the European Parliament and of the Council ([45]) and Article 20 of Regulation (EU) No 537/2014 of the European Parliament and of the Council ([46]) cooperate closely with each other within their respective competences and provide each other with information relevant for the performance of their respective tasks.

Confidential information exchanged pursuant to this Article shall be used by the authorities referred to in the first subparagraph solely for the exercise of their functions within the scope of this Directive or the other Union legal acts referred to in the first subparagraph and in the context of administrative or judicial proceedings specifically related to the exercise of those functions.

2. Member States may prohibit the authorities referred to in paragraph 1 from cooperating when such cooperation, including the exchange of information, would impinge on an ongoing inquiry, FIU's analysis, investigation or proceedings in accordance with the criminal or administrative law of the Member State where the authorities are located.

*Article 66*

**Cooperation with authorities in charge of implementing targeted financial sanctions**

1. Member States shall ensure that supervisors, their FIU and the authorities in charge of implementing targeted financial sanctions cooperate closely with each other within their respective competences and provide each other with information relevant for the performance of their respective tasks.

Confidential information exchanged pursuant to this Article shall be used by the authorities referred to in the first subparagraph solely for the exercise of their functions within the scope of this Directive or other Union legal acts and in the context of administrative or judicial proceedings specifically related to the exercise of those functions.

2. Member States may prohibit the authorities referred to in paragraph 1 from cooperating when such cooperation, including the exchange of information, would impinge on an ongoing inquiry, investigation or proceedings in accordance with the criminal or administrative law of the Member State where the authorities are located.

([45]) Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87).

([46]) Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC (OJ L 158, 27.5.2014, p. 77).

*Article 67*

**Professional secrecy requirements**

1. Member States shall require that all persons working for or who have worked for supervisors and the public authorities referred to in Article 52, as well as auditors or experts acting on behalf of those supervisors or authorities be bound by the obligation of professional secrecy.

Without prejudice to cases covered by criminal investigations and prosecutions under Union and national law and information provided to FIUs pursuant to Articles 42 and 43, confidential information which the persons referred to in the first subparagraph receive in the course of their duties under this Directive may be disclosed only in summary or aggregate form, in such a way that individual obliged entities cannot be identified.

2. Paragraph 1 of this Article shall not prevent the exchange of information between:

(a) supervisors, whether within a Member State or in different Member States, including AMLA when acting as a supervisor or public authorities as referred to in Article 52 of this Directive;

(b) supervisors as well as the public authorities referred to in Article 52 of this Directive and FIUs;

(c) supervisors as well as the public authorities referred to in Article 52 of this Directive and competent authorities referred to in Article 2(1), points (44)(c) and (d) of Regulation (EU) 2024/1624;

(d) financial supervisors and authorities in charge of supervising credit institutions and financial institutions in accordance with other Union legal acts relating to the supervision of credit institutions and financial institutions, including the ECB acting in accordance with Regulation (EU) No 1024/2013, whether within a Member State or in different Member States.

For the purposes of point (d) of the first subparagraph of this paragraph, the exchange of information shall be subject to the professional secrecy requirements provided for in paragraph 1.

3. Any authority or self-regulatory body that receives confidential information pursuant to paragraph 2 shall only use this information:

(a) in the discharge of its duties under this Directive or under other Union legal acts in the field of AML/CFT, of prudential regulation and supervision of credit institutions and financial institutions, including sanctioning;

(b) in an appeal against a decision of the authority or self-regulatory body, including court proceedings;

(c) in court proceedings initiated pursuant to special provisions provided for in Union law adopted in the field of this Directive or in the field of prudential regulation and supervision of credit institutions and financial institutions.

*Article 68*

**Exchange of information among supervisors and with other authorities**

1. With the exception of cases covered by Article 70(2) of Regulation (EU) 2024/1624, Member States shall authorise the exchange of information between:

(a) supervisors and the public authorities overseeing self-regulatory bodies pursuant to Chapter IV of this Directive, whether in the same Member State or in different Member States;

(b) supervisors and the authorities responsible by law for the supervision of financial markets in the discharge of their respective supervisory functions;

(c) supervisors in charge of auditors and, where relevant, public authorities overseeing self-regulatory bodies pursuant to Chapter IV of this Directive, and the public authorities competent for overseeing statutory auditors and audit firms pursuant to Article 32 of Directive 2006/43/EC and Article 20 of Regulation (EU) No 537/2014, including authorities in different Member States.

The professional secrecy requirements laid down in Article 67(1) and (3) shall not prevent the exchange of information referred to in the first subparagraph of this paragraph.

Confidential information exchanged pursuant to this paragraph shall only be used in the discharge of the duties of the authorities concerned, and in the context of administrative or judicial proceedings specifically related to the exercise of those functions. The information received shall in any event be subject to professional secrecy requirements at least equivalent to those referred to in Article 67(1).

2. Member States may authorise the disclosure of certain information to other national authorities responsible by law for the supervision of the financial markets, or with designated responsibilities in the field of combating or investigating money laundering, its predicate offences or terrorist financing. The professional secrecy requirements laid down Article 67 (1) and (3) shall not prevent such disclosure.

However, confidential information exchanged pursuant to this paragraph shall only be used for the purpose of performing the legal tasks of the authorities concerned. Persons having access to such information shall be subject to professional secrecy requirements at least equivalent to those referred to in Article 67(1).

3. Member States may authorise the disclosure of certain information relating to the supervision of obliged entities for compliance with Regulation (EU) 2024/1624 to parliamentary inquiry committees, courts of auditors and other entities in charge of inquiries in their Member State, under the following conditions:

(a) the entities have a precise mandate under national law to investigate or scrutinise the actions of supervisors or authorities responsible for laws on such supervision;

(b) the information is strictly necessary for fulfilling the mandate referred to in point (a);

(c) the persons with access to the information are subject to professional secrecy requirements under national law at least equivalent to those referred to in paragraph 1;

(d) where the information originates in another Member State, it shall not be disclosed without the express consent of the supervisor which disclosed it and solely for the purposes for which that supervisor gave its consent.

Member States may also authorise the disclosure of information pursuant to the first subparagraph of this paragraph to temporary committees of inquiry set up by the European Parliament in accordance with Article 226 TFEU and Article 2 of Decision 95/167/EC, Euratom, ECSC of the European Parliament, the Council and the Commission [47], where that disclosure is necessary for the performance of the activities of those committees.

*SECTION 3*

***Guidelines on cooperation***

*Article 69*

**AML/CFT cooperation guidelines**

By 10 July 2029, AMLA shall, in cooperation with the ECB, the European Supervisory Authorities, Europol, Eurojust, and EPPO, issue guidelines on:

(a) the cooperation between competent authorities under Section 1 of this Chapter, as well as with the authorities referred to in Section 2 of this Chapter and the entities in charge of the central registers, to prevent money laundering and terrorist financing;

(b) the procedures to be used by authorities competent for the supervision or oversight of obliged entities under other Union legal acts to take into account money laundering and terrorist financing concerns in the performance of their duties under those Union legal acts.

[47] Decision 95/167/EC, Euratom, ECSC of the European Parliament, the Council and the Commission of 19 April 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry (OJ L 113, 19.5.1995, p. 1).

CHAPTER VI

## DATA PROTECTION

*Article 70*

### Processing of certain categories of personal data

1. To the extent that it is necessary for the purposes of this Directive, competent authorities may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679 and personal data relating to criminal convictions and offences referred to in Article 10 of that Regulation subject to appropriate safeguards for the rights and freedoms of the data subject, in addition to the following safeguards:

(a) processing of such data shall be performed only on a case-by-case basis by the staff of each competent authority that have been specifically designated and authorised to perform those tasks;

(b) staff of the competent authorities shall maintain high professional standards of confidentiality and data protection, they shall be of high integrity and are appropriately skilled, including in relation to the ethical handling of big data sets;

(c) technical and organisational measures shall be in place to ensure the security of the data to high technological standards.

2. The safeguards referred to in paragraph 1 of this Article shall also apply to the processing for the purposes of this Directive of special categories of data referred to in Article 10(1) of Regulation (EU) 2018/1725 and personal data relating to criminal convictions and offences referred to in Article 11 of that Regulation by Union institutions, bodies, offices or agencies.

CHAPTER VII

## FINAL PROVISIONS

*Article 71*

### Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt the delegated acts referred to in Article 10 shall be conferred on the Commission for an indeterminate period of time from 9 July 2024.

3. The delegation of power referred to in Article 10 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 10 shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of 3 months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 3 months at the initiative of the European Parliament or of the Council.

*Article 72*

**Committee procedure**

1. The Commission shall be assisted by the Committee on the Prevention of Money Laundering and Terrorist Financing established by Article 34 of Regulation (EU) 2023/1113. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

*Article 73*

**Transitional management of FIU.net**

By 10 July 2027, the Commission shall transfer to AMLA the management of FIU.net.

Until such transfer is completed, the Commission shall provide the necessary assistance for the operation of FIU.net and the exchange of information between FIUs within the Union. To this end, the Commission shall regularly convene meetings of the EU FIU's Platform composed of representatives from Member States' FIUs in order to oversee the functioning of FIU.net.

*Article 74*

**Amendments to Directive (EU) 2015/849**

Directive (EU) 2015/849 is amended as follows:

(1) in Article 30(5), the first and second subparagraphs are replaced by the following:

'5. Member States shall ensure that the information on the beneficial ownership is accessible in all cases to:

(a) competent authorities and FIUs, without any restriction;

(b) obliged entities, within the framework of customer due diligence in accordance with Chapter II;

(c) any person or organisation that can demonstrate a legitimate interest.

The persons or organisations referred to in point (c) of the first subparagraph shall be permitted to access at least the name, the month and year of birth and the country of residence and nationality of the beneficial owner as well as the nature and extent of the beneficial interest held.';

(2) in Article 31(4), the first and second subparagraphs are replaced by the following:

'4. Member States shall ensure that the information on the beneficial ownership of a trust or a similar legal arrangement is accessible in all cases to:

(a) competent authorities and FIUs, without any restriction;

(b) obliged entities, within the framework of customer due diligence in accordance with Chapter II;

(c) any natural or legal person that can demonstrate a legitimate interest to access beneficial ownership information.

The information accessible to natural or legal persons referred to in point (c) of the first subparagraph shall consist of the name, the month and year of birth and the country of residence and nationality of the beneficial owner, as well as nature and extent of beneficial interest held.'.

*Article 75*

**Amendment to Directive (EU) 2019/1937**

In Directive (EU) 2019/1937, the Annex, Part II, Section A, point 2, the following point is added:

'(iii) Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L, 2024/1624, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1624/oj).'.

*Article 76*

**Review**

By 10 July 2032, and every 3 years thereafter, the Commission shall submit a report to the European Parliament and to the Council on the implementation of this Directive.

*Article 77*

**Repeal**

Directive (EU) 2015/849 is repealed with effect from 10 July 2027.

References to the repealed Directive shall be construed as references to this Directive and to Regulation (EU) 2024/1624 and shall be read in accordance with the correlation table in the Annex to this Directive.

*Article 78*

**Transposition**

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 10 July 2027. They shall immediately inform the Commission thereof.

By way of derogation from the first subparagraph, Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with Article 74 by 10 July 2025, with Articles 11, 12, 13 and 15 by 10 July 2026 and with Article18 by 10 July 2029. They shall immediately inform the Commission thereof.

When Member States adopt the measures referred to in this paragraph, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main measures of national law which they adopt in the field covered by this Directive.

*Article 79*

**Entry into force**

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

*Article 80*

**Addressees**

This Directive is addressed to the Member States.

Done at Brussels, 31 May 2024.

| *For the European Parliament* | *For the Council* |
|---|---|
| *The President* | *The President* |
| R. METSOLA | H. LAHBIB |

*ANNEX*

Correlation table

| Directive (EU) 2015/849 | This Directive | Regulation (EU) 2024/1624 |
|---|---|---|
| Article 1(1) | — | — |
| Article 1(2) | — | — |
| Article 1(3) | — | Article 2(1), point (1) |
| Article 1(4) | — | Article 2(1), point (1) |
| Article 1(5) | — | Article 2(1), point (2) |
| Article 1(6) | — | Article 2(1), points (1) and (2) |
| Article 2(1) | — | Article 3 |
| Article 2(2) | — | Article 4 |
| Article 2(3) | — | Article 6(1) |
| Article 2(4) | — | Article 6(2) |
| Article 2(5) | — | Article 6(3) |
| Article 2(6) | — | Article 6(4) |
| Article 2(7) | — | Article 6(5) |
| Article 2(8) | — | Article 7 |
| Article 2(9) | — | Article 4(3) and Article 6(6) |
| Article 3, point (1) | — | Article 2(1), point (5) |
| Article 3, point (2) | — | Article 2(1), point (6) |
| Article 3, point (3) | — | Article 2(1), point (4) |
| Article 3, point (4) | — | Article 2(1), point (3) |
| Article 3, point (5) | — | Article 2(1), point (47) |
| Article 3, point (6) | — | Article 2(1), point (28) |
| Article 3, point (6) (a) | — | Articles 51 to 55 |
| Article 3, point (6) (b) | — | Article 58 |
| Article 3, point (6) (c) | — | Article 57 |
| Article 3, point (7) | — | Article 2(1), point (11) |
| Article 3, point (8) | — | Article 2(1), point (22) |
| Article 3, point (9) | — | Article 2(1), point (34) and Article 2(2) |
| Article 3, point (10) | — | Article 2(1), point (35) and Article 2(5) |

| Directive (EU) 2015/849 | This Directive | Regulation (EU) 2024/1624 |
|---|---|---|
| Article 3, point (11) | — | Article 2(1), point (36) |
| Article 3, point (12) | — | Article 2(1), point (40) |
| Article 3, point (13) | — | Article 2(1), point (19) |
| Article 3, point (14) | — | Article 2(1), point (12) |
| Article 3, point (15) | — | Article 2(1), point (41) |
| Article 3, point (16) | — | Article 2(1), point (17) |
| Article 3, point (17) | — | Article 2(1), point (23) |
| Article 3, point (18) | — | Article 2(1), point (7) |
| Article 3, point (19) | — | — |
| Article 4 | Article 3 | — |
| Article 5 | — | — |
| Article 6 | Article 7 | — |
| Article 7 | Article 8 | — |
| Article 8(1) | — | Article 10(1) |
| Article 8(2) | — | Article 10(2) and (3) |
| Article 8(3) | — | Article 9(1) |
| Article 8(4) | — | Article 9(2) |
| Article 8(5) | — | Article 9(2) and (3) |
| Article 9 | — | Article 29 |
| Article 10(1) | — | Article 79(1) |
| Article 10(2) | — | Article 79(3) |
| Article 11 | — | Article 19(1), (2) and (5) |
| Article 12 | — | Article 19(7) and Article 79(2) |
| Article 13(1) | — | Article 20(1) |
| Article 13(2) | — | Article 20(2) |
| Article 13(3) | — | Article 20(2) |
| Article 13(4) | — | Article 20(4) |
| Article 13(5) | — | Article 47 |
| Article 13(6) | — | Article 22(4) |
| Article 14(1) | — | Article 23(1) and (4) |
| Article 14(2) | — | Article 23(2) |

| Directive (EU) 2015/849 | This Directive | Regulation (EU) 2024/1624 |
|---|---|---|
| Article 14(3) | — | Article 23(3) |
| Article 14(4) | — | Article 21(1) and (2) |
| Article 14(5) | — | Article 26(2) and (3) |
| Article 15 | — | Article 20(2), second subparagraph and Article 33 |
| Article 16 | — | Article 33(1) and (8) |
| Article 17 | — | — |
| Article 18(1) | — | Article 34(1) |
| Article 18(2) | — | Article 34(2) |
| Article 18(3) | — | Article 34(3) |
| Article 18(4) | — | — |
| Article 18a(1) | — | Article 29(4) |
| Article 18a(2) | — | Article 29(5) and (6) and Article 35, point (a) |
| Article 18a(3) | — | Article 29(5) and (6) and Article 35, point (b) |
| Article 18a(4) | — | — |
| Article 18a(5) | — | Article 29(6) |
| Article 19 | — | Article 36 |
| Article 20 | — | Article 9(2), Article 20(1) and Article 42 (1) |
| Article 20, point (a) | — | Article 9(2), point (a)(iii) and Article 20 (1), point (g) |
| Article 20, point (b) | — | Article 42(1) |
| Article 20a | — | Article 43 |
| Article 21 | — | Article 44 |
| Article 22 | — | Article 45 |
| Article 23 | — | Article 46 |
| Article 24 | — | Article 39 |
| Article 25 | — | Article 48(1) |
| Article 26 | — | Article 48 |
| Article 27 | — | Article 49 |
| Article 28 | — | Article 48(3) |
| Article 29 | — | — |

| Directive (EU) 2015/849 | This Directive | Regulation (EU) 2024/1624 |
|---|---|---|
| Article 30(1) | — | Article 63(1), (2), second subparagraph and (4) and Article 68 |
| Article 30(2) | — | Article 63(5) |
| Article 30(3) | Article 10(1) | — |
| Article 30(4) | Article 10(7) and (10) | Article 24 |
| Article 30(5), first subparagraph | Article 11 and Article 12(2) | — |
| Article 30(5), second subparagraph | Article 12(1) | — |
| Article 30(5), third subparagraph | — | — |
| Article 30(5a) | Article 11(4) and Article 13(12) | — |
| Article 30(6) | Article 11(1), (2) and (3) | — |
| Article 30(7) | Article 61(2) | — |
| Article 30(8) | — | Article 22(7) |
| Article 30(9) | Article 15 | — |
| Article 30(10) | Article 10(19) and (20) | — |
| Article 31(1) | — | Articles 58, Article 64(1) and Article 68 |
| Article 31(2) | — | Article 64(3) |
| Article 31(3) | — | Article 64(5) |
| Article 31(3a) | Article 10(1), (2) and (3) | Article 67 |
| Article 31(4), first subparagraph | Article 11 and Article 12(2) | — |
| Article 31(4), second subparagraph | Article 12(1) | — |
| Article 31(4), third subparagraph | — | — |
| Article 31(4), fourth subparagraph | Article 11(2) | — |
| Article 31(4a) | Article 11(4) and Article 13(12) | — |
| Article 31(5) | Article 10(7) and (10) | Article 24 |
| Article 31(6) | — | Article 22(7) |
| Article 31(7) | Article 61(2) | — |
| Article 31(7a) | Article 15 | — |
| Article 31(9) | Article 10(19) and (20) | — |
| Article 31(10) | — | Article 58(4) |
| Article 31a | Article 17(1) | — |
| Article 32(1) | Article 19(1) | — |

| Directive (EU) 2015/849 | This Directive | Regulation (EU) 2024/1624 |
|---|---|---|
| Article 32(2) | Article 62(1) | — |
| Article 32(3) | Article 19(2), (3), first subparagraph, (4) and (5) | — |
| Article 32(4) | Articles 21(1) and Article 22(1), first subparagraph | — |
| Article 32(5) | Article 22(1), second subparagraph | — |
| Article 32(6) | Article 22(2) | — |
| Article 32(7) | Article 24(1) | — |
| Article 32(8) | Article 19(3), second subparagraph | — |
| Article 32(9) | Article 21(4) | — |
| Article 32a(1) | Article 16(1) | — |
| Article 32a(2) | Article 16(2) | — |
| Article 32a(3) | Article 16(3) | — |
| Article 32a(4) | Article 16(5) | — |
| Article 32b | Article 18 | — |
| Article 33(1) | — | Article 69(1) |
| Article 33(2) | — | Article 69(6) |
| Article 34(1) | — | Article 70(1) |
| Article 34(2) | — | Article 70(2) |
| Article 34(3) | Article 40(5) | — |
| Article 35 | — | Article 71 |
| Article 36 | Article 42 | — |
| Article 37 | — | Article 72 |
| Article 38 | Article 60 | Article 11(2), fourth subparagraph, and (4), Article 14 and Article 69(7) |
| Article 39 | — | Article 73 |
| Article 40 | — | Article 77 |
| Article 41 | Article 70 | Article 76 |
| Article 42 | — | Article 78 |
| Article 43 | — | — |
| Article 44(1) | Article 9(1) | — |
| Article 44(2) | Article 9(2) | — |

| Directive (EU) 2015/849 | This Directive | Regulation (EU) 2024/1624 |
|---|---|---|
| Article 44(3) | — | — |
| Article 44(4) | Article 9(3) and (6) | — |
| Article 45(1) | — | Article 16(1) |
| Article 45(2) | — | Article 8(3), (4) and (5) |
| Article 45(3) | — | Article 17(1) |
| Article 45(4) | Article 48 | — |
| Article 45(5) | — | Article 17(2) |
| Article 45(6) | — | Article 17(3) |
| Article 45(7) | — | Article 17(4) |
| Article 45(8) | — | Article 16(3) |
| Article 45(9) | Article 41(1) | — |
| Article 45(10) | Article 41(2) | — |
| Article 45(11) | Article 41(3) | — |
| Article 46(1) | — | Articles 12 and 15 |
| Article 46(2) | Article 39(2) | — |
| Article 46(3) | Article 28(1) | — |
| Article 46(4) | — | Article 11(1) |
| Article 47(1) | Article 4(1) and (2) | — |
| Article 47(2) | Article 6(1) | — |
| Article 47(3) | Article 6(2) | — |
| Article 48(1) | Article 37(1) | — |
| Article 48(1a) | Article 37(5) and Article 62(1) | — |
| Article 48(2) | Article 37(2) and (6) | — |
| Article 48(3) | Article 37(7) | — |
| Article 48(4) | Article 37(1), first subparagraph, Article 46 and Article 54(4) | — |
| Article 48(5) | Article 46(2) and (3) and Article 47 | — |
| Article 48(6) | Article 40(1) | — |
| Article 48(7) | Article 40(2) | — |
| Article 48(8) | Article 40(4) | — |
| Article 48(9) | Article 37(3) | — |

| Directive (EU) 2015/849 | This Directive | Regulation (EU) 2024/1624 |
|---|---|---|
| Article 48(10) | Article 40(3) | — |
| Article 49 | Article 61(1) | — |
| Article 50 | Article 63 | — |
| Article 50a | Article 61(3) | — |
| Article 51 | — | — |
| Article 52 | Article 29 | — |
| Article 53 | Article 31 | — |
| Article 54 | Article 33 | — |
| Article 55 | Article 34 | — |
| Article 56 | Article 30(2) and (3) | — |
| Article 57 | Article 35 | — |
| Article 57a(1) | Article 67(1) | — |
| Article 57a(2) | Article 67(2) | — |
| Article 57a(3) | Article 67(3) | — |
| Article 57a(4) | Article 44, Article 46(1) and Article 47(1) | — |
| Article 57a(5) | Article 51 | — |
| Article 57b | Article 68 | — |
| Article 58(1) | Article 53(1) | — |
| Article 58(2) | Article 53(2) and (3) | — |
| Article 58(3) | Article 53(4) | — |
| Article 58(4) | — | — |
| Article 58(5) | Article 53(5) | — |
| Article 59(1) | Article 55(1) | — |
| Article 59(2) | Article 55(2) and Article 56(2) and (3) | — |
| Article 59(3) | Article 55(3) | — |
| Article 59(4) | Article 55(4) | — |
| Article 60(1) | Article 58(1), (2), first subparagraph and (3) | — |
| Article 60(2) | Article 58(2), third subparagraph | — |
| Article 60(3) | Article 58(4) | — |
| Article 60(4) | Article 53(6) | — |

| Directive (EU) 2015/849 | This Directive | Regulation (EU) 2024/1624 |
|---|---|---|
| Article 60(5) | Article 53(7) | — |
| Article 60(6) | Article 53(8) | — |
| Article 61 | Article 60 | — |
| Article 62(1) | Article 59(1) | — |
| Article 62(2) | Article 6(6) | — |
| Article 62(3) | Article 59(2) | — |
| Article 63 | — | — |
| Article 64 | — | Article 85 |
| Article 64a | Article 72 | Article 86 |
| Article 65 | — | — |
| Article 66 | — | — |
| Article 67 | — | — |
| Article 68 | — | — |
| Article 69 | — | — |
| Annex I | — | Annex I |
| Annex II | — | Annex II |
| Annex III | — | Annex III |
| Annex IV | — | — |