**European Parliament**
2019-2024

*Committee on Economic and Monetary Affairs*
*Committee on Civil Liberties, Justice and Home Affairs*

5.10.2022

# PROVISIONAL AGREEMENT RESULTING FROM INTERINSTITUTIONAL NEGOTIATIONS

**Subject:** **Proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) (COM(2021)0442 – C9-0341/2021 – 2021/0241(COD))**

The interinstitutional negotiations on the aforementioned proposal for a regulation have led to a compromise. In accordance with Rule 74(4) of the Rules of Procedure, the provisional agreement, reproduced below, is submitted as a whole to the Committee on Economic and Monetary Affairs Committee on Civil Liberties, Justice and Home Affairs for decision by way of a single vote.

**Proposal for a**
**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**
**on information accompanying transfers of funds and certain crypto-assets (recast)**
(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,

1 OJ C […], […], p. […].
2 OJ C […], […], p. […].

Whereas:

(1) Regulation (EU) 2015/847 of the European Parliament and of the Council[3] has been substantially amended[4]. Since further amendments are to be made, that Regulation should be recast in the interests of clarity.

(2) Regulation (EU) 2015/847 was adopted to ensure that the Financial Action Task Force (FATF) requirements on wire transfers services providers, and in particular the obligation on payment service providers to accompany transfers of funds with information on the payer and the payee, were applied uniformly throughout the Union. The latest changes introduced in June 2019 in the FATF standards on new technologies, aiming at regulating so called virtual assets and virtual asset service providers, have provided new and similar obligations for virtual asset service providers, with the purpose to facilitate the traceability of transfers of virtual assets. Thus, under those new requirements, virtual asset transfer service providers must accompany transfers of virtual assets with information on their originators and beneficiaries, that they must obtain, hold, share with counterpart at the other hand of the virtual assets transfer and make available on request to competent authorities.

(3) Given that Regulation (EU) 2015/847 currently only applies to transfer of funds, in the meaning of banknotes and coins, scriptural money and electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC, it is appropriate to extend the scope in order to also cover transfer of virtual assets.

---

**3** Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (OJ L 141, 5.6.2015, p. 1).

**4** See Annex I.

(4) Flows of illicit money through transfers of funds and crypto-assets can damage the integrity, stability and reputation of the financial sector, and threaten the internal market of the Union as well as international development. Money laundering, terrorist financing and organised crime remain significant problems which should be addressed at Union level. The soundness, integrity and stability of the system of transfers of funds and crypto-assets and confidence in the financial system as a whole, could be seriously jeopardised by the efforts of criminals and their associates to disguise the origin of criminal proceeds or to transfer funds or crypto-assets for criminal activities or terrorist purposes.

(5) In order to facilitate their criminal activities, money launderers and financers of terrorism are likely to take advantage of the freedom of capital movements within the Union's integrated financial area unless certain coordinating measures are adopted at Union level. International cooperation within the framework of FATF and the global implementation of its recommendations aim to prevent money laundering and terrorist financing while transferring funds or crypto-assets .

(6) By reason of the scale of the action to be undertaken, the Union should ensure that the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation adopted by FATF on 16 February 2012 and then on 21 June 2019 (revised FATF Recommendations), and, in particular, FATF Recommendation 15 on new technologies (‘FATF Recommendation 15’), FATF Recommendation 16 on wire transfers (‘FATF Recommendation 16’) and the revised interpretative notes on those Recommendations, are applied uniformly throughout the Union and that, in particular, there is no discrimination or discrepancy between, on the one hand, national payments or transfers of crypto-assets within a Member State and, on the other, cross-border payments or transfers of crypto-assets between Member States. Uncoordinated action by Member States acting alone in the field of cross-border transfers of funds and crypto-assets could have a significant impact on the smooth functioning of payment systems and crypto-asset services at Union level and could therefore damage the internal market in the field of financial services.

(7) In order to foster a coherent approach in the international context and to increase the effectiveness of the fight against money laundering and terrorist financing, further Union action should take account of developments at international level, in particular the revised FATF Recommendations.

(7a) The global reach, the speed at which transactions can be carried out and the possible anonymity offered by their transfer, particularly expose crypto assets to the risk of criminal misuse in and across jurisdictions. In order to effectively address the risks posed by the misuse of crypto-assets for money laundering and terrorist financing purposes, the Union should promote the implementation at global level of the standards established under this Regulation and also to develop the international and cross-jurisdictional dimension of the regulation and supervision of transfers of crypto-assets in relation to money laundering and terrorist financing.

(8) Directive (EU) 2018/843 of the European Parliament and of the Council[5] introduced a definition of virtual currencies and recognised providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers among the entities submitted to anti-money laundering and countering terrorism financing requirements in the Union legal framework. The latest international developments, notably within the FATF, now implies the need to regulate additional categories of virtual asset service providers not yet covered as well as to broaden the current definition of virtual currency.

(9) It is to be noted that the definition of crypto-assets in Regulation[6] [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final] corresponds to the definition of virtual assets set out in the recommendations of FATF, and the list of crypto-asset services and crypto-asset service providers covered in that Regulation also encompass the virtual asset services providers identified as such by FATF and considered as likely to raise money-laundering concerns. In order to ensure the coherency of the Union legal framework, this proposal should refer to those definitions of crypto-assets and crypto-asset service providers.

---

**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).

**6** References to MiCA to be added once the text adopted

(10) The implementation and enforcement of this Regulation represent relevant and effective means of preventing and combating money-laundering and terrorist financing.

(11) This Regulation is not intended to impose unnecessary burdens or costs on payment service providers , crypto-asset service providers or on persons who use their services. In this regard, the preventive approach should be targeted and proportionate and should be in full compliance with the free movement of capital, which is guaranteed throughout the Union.

(12) In the Union's Revised Strategy on Terrorist Financing of 17 July 2008 (the 'Revised Strategy'), it was pointed out that efforts must be maintained to prevent terrorist financing and to control the use by suspected terrorists of their own financial resources. It is recognised that FATF is constantly seeking to improve its Recommendations and is working towards a common understanding of how they should be implemented. It is noted in the Revised Strategy that implementation of the revised FATF Recommendations by all FATF members and members of FATF-style regional bodies is assessed on a regular basis and that a common approach to implementation by Member States is therefore important.

(13) In addition, the Commission Action Plan of 7 May 2020 for a comprehensive Union policy on preventing money laundering and terrorism financing[7] identified six priority areas for urgent action to improve the Union's anti-money laundering and countering financing of terrorism regime, including the establishment of a coherent regulatory framework for that regime in the Union to obtain more detailed and harmonised rules, notably to address the implications of technological innovation and developments in international standards and avoid diverging implementation of existing rules. Work at international level suggests a need to expand the scope of sectors or entities covered by the anti-money laundering and countering financing of terrorism rules and to assess how they should apply to crypto-assets service providers not covered so far.

---

7 Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing (C(2020) 2800 final).

(14) In order to prevent terrorist financing, measures with the purpose of freezing the funds and the economic resources of certain persons, groups and entities have been taken, including Council Regulations (EC) No 2580/2001[8], (EC) No 881/2002[9] and (EU) No 356/2010[10]. To the same end, measures with the purpose of protecting the financial system against the channelling of funds and economic resources for terrorist purposes have also been taken. Directive (EU) 2015/849 of the European Parliament and of the Council[11] contains a number of such measures. Those measures do not, however, fully prevent terrorists or other criminals from accessing payment systems for transferring their funds.

(15) The traceability of transfers of funds and crypto-assets can be a particularly important and valuable tool in the prevention, detection and investigation of money laundering and terrorist financing, as well as in the implementation of restrictive measures, in particular those imposed by Regulations (EC) No 2580/2001, (EC) No 881/2002 and (EU) No 356/2010, in compliance with Union regulations implementing such measures. It is therefore appropriate, in order to ensure the transmission of information throughout the payment or transfers of crypto-assets chain, to provide for a system imposing the obligation on payment service providers and crypto-asset service providers to accompany transfers of funds with information on the payer and the payee and transfers of crypto-assets with information on the originator and the beneficiary .

---

**8** Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (OJ L 344, 28.12.2001, p. 70).

**9** Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with the ISIL (Da'esh) and Al-Qaida organisations (OJ L 139, 29.5.2002, p. 9).

**10** Council Regulation (EU) No 356/2010 of 26 April 2010 imposing certain specific restrictive measures directed against certain natural or legal persons, entities or bodies, in view of the situation in Somalia (OJ L 105, 27.4.2010, p. 1).

**11** 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 purpose 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 (see page 73 of this Official Journal).

(15a) Certain transfers of crypto-assets entail specific high-risk factors of money-laundering, terrorist financing and other criminal activities, in particular transfers related to products, transactions or technologies designed to enhance anonymity, including mixers or tumblers. To ensure the traceability of such transfers, the EBA should clarify, in particular, how the risk factors listed in Annex III of the AMLD Directive are to be taken into account by crypto-asset service providers, including when performing transactions with non-EU entities that are not regulated, not registered or not licensed in any third country, or with self-hosted wallets. Where situations of higher risk are identified, the EBA guidelines should specify which enhanced due diligence measures obliged entities should consider applying to mitigate such risks, including the adoption of appropriate procedures, including the use of DLT analytic tools, to detect the origin or destination of crypto-assets.

(16) This Regulation should apply without prejudice to the national restrictive measures and Union restrictive measures imposed by regulations based on Article 215 of the Treaty on the Functioning of the European Union (TFEU), such as Regulations (EC) No 2580/2001, (EC) No 881/2002, (EU) No 356/2010, (EU) No 2016/1686, (EU) 2017/1509 and (EU) 267/2012 , which may require that payment service providers of payers and of payees, crypto asset service providers of originators and beneficiaries, intermediary payment service providers, as well intermediary crypto-asset service provider, take appropriate action to freeze certain funds and crypto-assets or that they comply with specific restrictions concerning certain transfers of funds or crypto-assets. Payment service providers and crypto-assets service providers should have in place internal policies, procedures and controls to ensure implementation of those restrictive measures and targeted financial sanctions, including screening measures against national and EU list of designated persons. The EBA should issue guidelines specifying those internal policies, procedures and controls. It is intended that the requirements of this Regulation on internal policies, procedures and controls related to restrictive measures will be repealed in the near future by the [insert reference to AML Regulation].

(17) Processing of personal data under this Regulation should take place in full compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council[12]. Further processing of personal data for commercial purposes should be strictly prohibited. The fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States. In applying this Regulation, the transfer of personal data to a third country must be carried out in accordance with Chapter V of Regulation (EU) 2016/679 . It is important that payment service providers and crypto-asset service providers operating in multiple jurisdictions with branches or subsidiaries located outside the Union should not be prevented from transferring data about suspicious transactions within the same organisation, provided that they apply adequate safeguards. In addition, the crypto-asset service providers of the originator and of the beneficiary, the payment service providers of the payer and of the payee and the intermediary payment service providers and intermediary crypto-asset service providers should have in place appropriate technical and organisational measures to protect personal data against accidental loss, alteration, or unauthorised disclosure or access.

(18) Persons that merely convert paper documents into electronic data and are acting under a contract with a payment service provider and persons that provide payment service providers solely with messaging or other support systems for transmitting funds or with clearing and settlement systems should not fall within the scope of this Regulation.

(18a) Persons that only provide ancillary infrastructure that enables another entity to provide crypto-asset transfer services, such as internet services, cloud services, or software developers, should not fall within the scope of this Regulation unless they perform transfers of crypto-assets.

(18b) This Regulation should not apply to person-to-person transfers of crypto-assets conducted without the involvement of a crypto-asset service provider, or when both the originator and the beneficiary are providers of crypto-asset transfers acting on their own behalf.

---

**12** 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).

(19) Transfers of funds corresponding to services referred to in Article 3, points (a) to (m) and point (o) of Directive (EU) 2015/2366[13] do not fall within the scope of this Regulation. It is also appropriate to exclude from the scope of this Regulation transfers of funds and electronic money tokens as defined in Article 3(1) point 4 of [MiCA], that represent a low risk of money laundering or terrorist financing. Such exclusions should cover payment cards, electronic money instruments, mobile phones or other digital or information technology (IT) prepaid or postpaid devices with similar characteristics, where they are used exclusively for the purchase of goods or services and the number of the card, instrument or device accompanies all transfers. However, the use of a payment card, an electronic money instrument, a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics in order to effect a transfer of funds or electronic money tokens between natural persons acting as consumers for purposes other than trade, business or profession, falls within the scope of this Regulation. In addition, Automated Teller Machine withdrawals, payments of taxes, fines or other levies, transfers of funds carried out through cheque images exchanges, including truncated cheques, or bills of exchange, and transfers of funds where both the payer and the payee are payment service providers acting on their own behalf should be excluded from the scope of this Regulation.

(19a) Crypto assets that are unique and not fungible are not subject to the travel rule unless they are classified as crypto-assets or funds under MiCA Regulation.

(19b) Crypto-ATMs can enable users to perform transfers of crypto-assets to a crypto-asset address by depositing cash, often without any form of customer identification and verification. Crypto-ATMs are particularly exposed to money laundering risks because the anonymity they provide and the possibility of operating with cash of unknown origin make them an ideal vehicle for illicit activities. Given their role in providing or actively facilitating transfers of crypto-assets, transfers of crypto-assets linked to crypto-ATMs should fall under the scope of this Regulation.

---

**13** 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).

(20) In order to reflect the special characteristics of national payment systems, and provided that it is always possible to trace the transfer of funds back to the payer, Member States should be able to exempt from the scope of this Regulation certain domestic low-value transfers of funds, including electronic giro payments, used for the purchase of goods or services.

(20a) Due to the inherent borderless nature and global reach of transfers of crypto-assets and of the provision of services in crypto-assets, there are no objective reasons to distinguish the money laundering and terrorism financing risk of national transfers compared to cross-border transfers. In order to reflect those specific features, an exemption from the scope of this Regulation for domestic low-value transfers of crypto-assets is therefore not appropriate, in line with FATF expectation to treat transfers of crypto-asset as cross-border transfer in nature.

(21) Payment service providers and crypto-asset service providers should ensure that the information on the payer and the payee or the originator and the beneficiary is not missing or incomplete.

(22) In order not to impair the efficiency of payment systems and in order to balance the risk of driving transactions underground as a result of overly strict identification requirements against the potential terrorist threat posed by small transfers of funds, the obligation to check whether information on the payer or the payee is accurate should, in the case of transfers of funds where verification has not yet taken place, be imposed only in respect of individual transfers of funds that exceed EUR 1000, unless the transfer appears to be linked to other transfers of funds which together would exceed EUR 1000, the funds have been received or paid out in cash or in anonymous electronic money, or where there are reasonable grounds for suspecting money laundering or terrorist financing.

(22a) Compared to funds transfers, transfers in crypto-assets can be carried out across multiple jurisdictions at larger scale and higher speed due to their global reach and technological characteristics. In addition to the pseudo-anonymity of crypto assets, this offers criminals the opportunity to carry out at high speed large illicit transfers while circumventing traceability obligations and avoiding detection, by structuring a large transaction into smaller amounts, using multiple seemingly unrelated DLT addresses, including one-time use DLT addresses, and automated processes. Most crypto-assets are also highly volatile and their value can fluctuate significantly within a very short time-frame that makes the calculation of linked transaction more uncertain. In order to reflect those specific features, transfers of crypto-assets should be submitted to the same requirements without consideration for their amount and regardless of whether they are domestic or cross-border.

(23) For transfers of funds or for transfers of crypto-assets where verification is deemed to have taken place, payment service providers and crypto-asset service providers should not be required to verify information on the payer or the payee accompanying each transfer of funds, or on the originator and the beneficiary accompanying each transfer of crypto-assets, provided that the obligations laid down in Directive (EU) 2015/849 are met.

(24) In view of the Union legislative acts in respect of payment services, namely Regulation (EC) No 924/2009 of the European Parliament and of the Council[14], Regulation (EU) No 260/2012 of the European Parliament and of the Council[15] and Directive (EU) 2015/2366, it should be sufficient to provide that only simplified information accompany transfers of funds within the Union, such as the payment account number(s) or a unique transaction identifier.

(24a) (deleted)

---

**14** Regulation (EC) No 924/2009 of the European Parliament and of the Council of 16 September 2009 on cross-border payments in the Community and repealing Regulation (EC) No 2560/2001 (OJ L 266, 9.10.2009, p. 11).

**15** Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009 (OJ L 94, 30.3.2012, p. 22).

(25) In order to allow the authorities responsible for combating money laundering or terrorist financing in third countries to trace the source of funds or crypto-assets used for those purposes, transfers of funds or transfer of crypto-assets from the Union to outside the Union should carry complete information on the payer and the payee as well as on the originator and the beneficiary, respectively. Complete information on the payer and the payee should include the Legal Entity Identifier (LEI), or any equivalent official identifier, when this information is provided by the payer to the payer's service provider, since that would allow for better identification of the parties involved in a transfer of funds and could easily be included in existing payment message formats such as the one developed by the International Organisation for Standardisation for electronic data interchange between financial institutions. The authorities responsible for combating money laundering or terrorist financing in third countries should be granted access to complete information on the payer and the payee as well as on the originator and the beneficiary only for the purposes of preventing, detecting and investigating money laundering and terrorist financing.

(25a) Crypto-assets exist in a borderless virtual reality and can be transferred to any crypto-asset service provider, whether or not it is registered in a jurisdiction. Many non-Union jurisdictions have in place rules relating to data protection and enforcement that differ from those in the Union. When transferring crypto-assets on behalf of a customer to a crypto-asset service provider that is not registered in the Union, the crypto-asset service provider of the originator should assess the ability of the crypto-asset service provider of the beneficiary to receive and retain the information required under this Regulation in compliance with Regulation (EU) 2016/679, using, where appropriate, the options available in Chapter V of that Regulation. The European Data Protection Board should, after consultation of the European Banking Authority, issue guidelines on the practical implementation of data protection requirements for transfers of personal data to third countries in the context of transfers of crypto-assets. Situations may occur where personal data cannot be sent because the requirements of Regulation (EU) 2016/679 cannot be fulfilled. The EBA should issue guidelines on suitable procedures for determining whether in such cases the transfer of crypto-assets should be executed, rejected or suspended.

(26) The Member State authorities responsible for combating money laundering and terrorist financing, and relevant judicial and law enforcement authorities in the Member States and at Union level , should intensify cooperation with each other and with relevant third country authorities, including those in developing countries, in order further to strengthen transparency and the sharing of information and best practices.

(27) Regarding transfers of crypto-assets, the requirements of this Regulation should apply to all transfers including transfers of crypto-assets to or from a self-hosted address, as long as there is a crypto-asset service provider involved.

(28) (deleted)

(29) The crypto-asset service provider of the originator should ensure that transfers of crypto-assets are accompanied by the name of the originator, the originator's distributed ledger address, where a transfer of crypto-assets is registered on a network using distributed ledger technology or similar technology, the originator’s crypto-asset account number, where such an account exists and is used to process the transaction, and the originator’s address, including the name of the country, official personal document number, and the customer identification number, or alternatively, date and place of birth and the current LEI of the originator, or any other available equivalent official identifier, subject to the existence of the necessary field in the relevant message format and where provided by the originator to its crypto-asset service provider. The information should be submitted in a secure manner and in advance of, or simultaneously or concurrently with, the transfer of crypto-assets.

(29a) The crypto-asset service provider of the originator should also ensure that transfers of crypto-assets are accompanied by the name of the beneficiary, the beneficiary's distributed ledger address, where a transfer of crypto-assets is registered on a network using distributed ledger technology or similar technology, the beneficiary's account number where such an account exists and is used to process the transaction , and, subject to the existence of the necessary field in the relevant message format, and where provided by the originator to its crypto-asset service provider, the current LEI of the beneficiary or any other available equivalent official identifier. The information should be submitted in a secure manner and in advance of, or simultaneously or concurrently with, the transfer of crypto-assets.

(29b) (deleted)

(29b) In case of a transfer to or from a self-hosted address, the crypto-asset service provider should collect the information on both the originator and the beneficiary, usually from their customer. The crypto-asset service provider should in principle not be required to verify the information on the user of the self-hosted address. Nonetheless, in case of a transfer whose amount exceeds EUR 1 000 and is sent or received on behalf of a customer of a crypto-asset service provider to or from a self-hosted address, that crypto-asset service provider should verify whether such self-hosted address is effectively owned or controlled by that customer.

(30) As regards transfers of funds from a single payer to several payees that are to be sent in batch files containing individual transfers from the Union to outside the Union, provision should be made for such individual transfers to carry only the payment account number of the payer or the unique transaction identifier, as well as complete information on the payee, provided that the batch file contains complete information on the payer that is verified for accuracy and complete information on the payee that is fully traceable.

(31) As regards transfers of crypto-assets, the submission of originator and beneficiary information in batches should be accepted, as long as submission occurs immediately and securely. It should not be permitted to submit the required information after the transfer, as submission must occur before or at the moment the transaction is completed, and crypto-asset service providers or other obliged entities should submit the required information simultaneously with the batch crypto-assets transfer itself.

(32) In order to check whether the required information on the payer and the payee accompanies transfers of funds, and to help identify suspicious transactions, the payment service provider of the payee and the intermediary payment service provider should have effective procedures in place to detect whether information on the payer and the payee is missing or incomplete. Those procedures should include monitoring after or during the transfers where appropriate. Competent authorities should ensure that payment service providers include the required transaction information with the wire transfer or related message throughout the payment chain.

(33) As regards transfers of crypto-assets, the crypto-asset service provider of the beneficiary should implement effective procedures to detect whether the information on the originator or the beneficiary is missing or incomplete. These procedures should include, where appropriate, monitoring after or during the transfers, in order to detect whether the required information on the originator or the beneficiary is missing or incomplete. It should not be required that the information is attached directly to the transfer of crypto-assets itself, as long as it is submitted in advance of, simultaneously or concurrently with, the transfer of crypto-assets, and is available upon request to appropriate authorities.

(33a) (deleted)

(34) Given the potential threat of money laundering and terrorist financing presented by anonymous transfers, it is appropriate to require payment service providers to request information on the payer and the payee. In line with the risk-based approach developed by FATF, it is appropriate to identify areas of higher and lower risk, with a view to better targeting the risk of money laundering and terrorist financing. Accordingly, the crypto-asset service provider of the beneficiary, the payment service provider of the payee and the intermediary payment service provider should have effective risk-based procedures that apply where a transfer of funds lacks the required information on the payer or the payee, or where a transfer of crypto-assets lacks the required information on the originator or the beneficiary, in order to allow them to decide whether to execute, reject or suspend that transfer and to determine the appropriate follow-up action to take.

(34a) Crypto-asset service providers, as all obliged entities, should assess and monitor the risk related to their clients, products and delivery channels. Crypto-asset service providers should also assess the risk related to their transaction, including where performing transfers to or from self-hosted address.
In the case the crypto-asset service provider is or becomes aware that the information on the originator or beneficiary of the self-hosted address is inaccurate, or where facing unusual or suspicious patterns of transactions or situations of higher risks of money laundering and financing of terrorism associated with transfers involving self-hosted address, crypto-asset service providers should implement, where appropriate, enhanced due diligence to manage and mitigate the risks appropriately and take this into account when assessing whether a transfer of crypto-assets, or any related transaction, is unusual and whether it is to be reported to the Financial Intelligence Unit (FIU) in accordance with Directive (EU) 2015/849.

(34b) (deleted)

(34c) (deleted)

(34d) (deleted)

(34e) (deleted)

(34f) This Regulation should be reviewed in the context of the adoption of the [AMLR] and [AMLA] in order to ensure consistency with the relevant provisions.

(35) The payment service provider of the payee, the intermediary payment service provider and the crypto-asset service provider of the beneficiary should exercise special vigilance, assessing the risks, when either becomes aware that information on the payer or the payee , or the originator or the beneficiary is missing or incomplete, or where a transfer of crypto-assets is required to be considered suspicious based on the origin or destination of the crypto-assets concerned and should report suspicious transactions to the competent authorities in accordance with the reporting obligations set out in Directive (EU) 2015/849.

(35a) Similar to transfers of funds between payment service providers, transfers of crypto-assets involving intermediary providers of crypto-asset transfers might facilitate transfers as an intermediate element in a chain of transfers of crypto-assets. In line with international standards, such intermediary providers should also be subject to the requirements set out in this Regulation, in the same way as existing obligations on intermediary payment service providers.

(36) The provisions on transfers of funds and transfers of crypto-assets in relation to which information on the payer or the payee or the originator or the beneficiary is missing or incomplete and in relation to which transfers of crypto-assets are required to be considered suspicious based on the origin or destination of the crypto-assets concerned, apply without prejudice to any obligations on payment service providers, intermediary payment service providers and crypto-asset service providers, to suspend and/or reject transfers of funds and transfers of crypto-assets which breach a provision of civil, administrative or criminal law.

(36a) In order to ensure technology neutrality, this Regulation should not mandate for the use of a particular technology when crypto-asset service providers transfer transaction information. To ensure the efficient implementation of requirements applicable to crypto-asset service providers under this Regulation, standard setting initiatives involving or led by the crypto-asset industry will be critical. Those protocols should be interoperable through the use of international or Union-wide standards in order to allow for a swift exchange of information.

(37) With the aim of assisting payment service providers and crypto-asset service providers to put effective procedures in place to detect cases in which they receive transfers of funds or transfers of crypto-assets with missing or incomplete payer, payee, originator or beneficiary information and to take effective follow-up actions, the European Supervisory Authority ( European Banking Authority), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council (EBA), the European Supervisory Authority (European Insurance and Occupational Pensions Authority ), established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council[16] (EIOPA), and the European Supervisory Authority (European Securities and Markets Authority), established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council[17] (ESMA), should issue guidelines.

(38) To enable prompt action to be taken in the fight against money laundering and terrorist financing, payment service providers and crypto-asset service providers should respond promptly to requests for information on the payer and the payee or on the originator and the beneficiary from the authorities responsible for combating money laundering or terrorist financing in the Member State where those payment service providers and crypto-asset service provider are established.

(39) The number of working days in the Member State of the payment service provider of the payer or crypto-asset service provider of the originator determines the number of days to respond to requests for information on the payer or the originator .

---

**16** Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decisio n 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

**17** Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

(40) As it may not be possible in criminal investigations to identify the data required or the individuals involved in a transaction until many months, or even years, after the original transfer of funds or transfer of crypto-assets , and in order to be able to have access to essential evidence in the context of investigations, it is appropriate to require payment service providers or crypto-asset service providers to keep records of information on the payer and the payee or the originator and the beneficiary for a period of time for the purposes of preventing, detecting and investigating money laundering and terrorist financing. That period should be limited to five years, after which all personal data should be deleted unless national law provides otherwise. If necessary for the purposes of preventing, detecting or investigating money laundering or terrorist financing, and after carrying out an assessment of the necessity and proportionality of the measure, Member States should be able to allow or require retention of records for a further period of no more than five years, without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings and in full compliance with Directive (EU) 2016/680 of the European Parliament and of the Council. Those measures could be reviewed in light of the adoption of the [add reference to AML Regulation].

(41) In order to improve compliance with this Regulation, and in accordance with the Commission Communication of 9 December 2010 entitled 'Reinforcing sanctioning regimes in the financial services sector', the power to adopt supervisory measures and the sanctioning powers of competent authorities should be enhanced. Administrative sanctions and measures should be provided for and, given the importance of the fight against money laundering and terrorist financing, Member States should lay down sanctions and measures that are effective, proportionate and dissuasive. Member States should notify the Commission and the Joint Committee of EBA, EIOPA and ESMA (the 'ESAs') thereof.

(42) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[18].

---

**18** 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 Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(43) A number of countries and territories which do not form part of the territory of the Union share a monetary union with a Member State, form part of the currency area of a Member State or have signed a monetary convention with the Union represented by a Member State, and have payment service providers that participate directly or indirectly in the payment and settlement systems of that Member State. In order to avoid the application of this Regulation to transfers of funds between the Member States concerned and those countries or territories having a significant negative effect on the economies of those countries or territories, it is appropriate to provide for the possibility for such transfers of funds to be treated as transfers of funds within the Member States concerned.

(44) Since the objectives of this Regulation , namely to fight money laundering and the financing of terrorism, including by implementing International Standards, by ensuring the availability of basic information on payers and payees of transfer of funds, and on originators and beneficiaries of transfers of crypto-assets, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale or 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 (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(44a) Given the potential high risks associated with, and the technological and regulatory complexity posed by self-hosted addresses, including in relation to the verification of the ownership information, by ... [12 months after the date of application of this Regulation], the Commission should assess the need for additional specific measures to mitigate the risks posed by transfers from and to self-hosted addresses, including the introduction of possible restrictions, and assess the effectiveness and proportionality of the mechanisms used to verify the accuracy of the information concerning the ownership of self-hosted addresses.

(44b) (deleted)

(44c) At present, Directive (EU) 2015/849 only applies to two categories of providers of crypto-asset services, namely, custodial wallets and crypto-to-fiat exchanges. In order to close existing loopholes in the anti-money laundering and terrorist financing framework and align Union legislation with international recommendations, Directive (EU) 2015/849 should be amended to include all categories of crypto-asset service providers as defined in [Regulation on Markets in Crypto-assets], which covers a broader range of crypto-asset service providers. In particular, with a view to ensuring that crypto-asset service providers are subject to the same requirements and level of supervision as credit and financial institutions, it is appropriate to update the list of obliged entities by including crypto-asset service providers within the category of financial institutions for the purpose of that Directive. In addition, taking into account that traditional financial institutions also fall within the definition of crypto-asset service providers when offering such services, the identification of crypto-asset service providers as financial institutions allows for a single consistent set of rules that applies to entities providing both traditional financial services and crypto-assets services. Directive (EU) 2015/849 should also be amended in order to ensure that crypto-asset service providers are able to appropriately mitigate the money laundering and terrorist financing risks to which they are exposed.

(44d) Relationships established between crypto-asset service providers and entities established in third countries for the purpose of executing crypto-asset transfers or the provision of similar crypto-asset services present similarities to correspondent banking relationships established with a third-country's respondent institution. As they are characterised by an ongoing and repetitive nature, they should be considered as a type of correspondent relationship and be subject to specific enhanced due diligence measures similar in principle to those applied in the context of banking and financial services.
In particular, crypto-asset service providers should, when establishing a new correspondent relationship with a respondent entity, apply specific enhanced due diligence measures in order to identify and assess the risk exposure of this respondent, based on its reputation, the quality of supervision and its AML/CFT controls.

Based on the information gathered, the correspondent crypto-asset service providers should implement appropriate risk mitigating measures, which should take into account in particular the potential higher risk of money laundering and terrorist financing posed by unregistered and unlicensed entities. This is especially relevant as long as the implementation of the FATF standards relating to crypto-assets at global level remains uneven, which poses additional risks and challenges.
The EBA should provide guidance on how crypto-asset service providers should conduct the enhanced due diligence and specify the appropriate risk mitigating measures, including the minimum action to be taken, when interacting with unregistered or unlicensed entities which provide crypto-asset services.

(44e) Directive (EU) 2015/849 was amended by Directive (EU) 2018/843, introducing a requirement that providers of exchange services between virtual currencies and fiat currencies, as well as custodian wallet providers, be subject to registration. Regulation [please insert reference to MiCA Regulation] has established a comprehensive regulatory framework for crypto-asset service providers, which harmonises the rules pertaining to authorisation and operation of crypto-asset service providers across the Union. In order to avoid duplication of requirements, Directive (EU) 2015/849 should be amended to remove registration requirements in relation to those categories of crypto-asset service providers which will become subject to a single licensing regime under [MICA Regulation].

(45) This Regulation is subject to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 of the European Parliament and of the Council[19]. It respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private and family life (Article 7), the right to the protection of personal data (Article 8), the right to an effective remedy and to a fair trial (Article 47) and the principle of ne bis in idem.

**19** 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).

(45a) In order to ensure consistency with [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final], this Regulation should apply from the date of application of Regulation [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final]. From such date, Member States should also transpose the aforementioned amendment to Directive (EU) 2015/849.

(46) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on […][20],

HAVE ADOPTED THIS REGULATION:

## CHAPTER I
## SUBJECT MATTER, SCOPE AND DEFINITIONS

### Article 1
### Subject matter

This Regulation lays down rules on the information on payers and payees, accompanying transfers of funds, in any currency, and the information on originators and beneficiaries, accompanying transfers of crypto-assets, for the purposes of preventing, detecting and investigating money laundering and terrorist financing, where at least one of the payment or crypto-asset service providers involved in the transfer of funds or crypto-assets is established in the Union. In addition this Regulation lays down rules on internal policies, procedures and controls to ensure implementation of restrictive measures where at least one of the payment or crypto-asset service providers involved in the transfer of funds or crypto-assets is established in the Union.

**20** [OJ reference of that opinion]

Article 2
Scope

1. This Regulation shall apply to transfers of funds, in any currency, which are sent or received by a payment service provider or an intermediary payment service provider established in the Union. It shall also apply to transfers of crypto-assets as defined in Article 3(10) of this Regulation including transfers of crypto-assets executed by means of crypto-asset automated teller machines ('crypto-ATMs') where the crypto-asset service provider of the originator or the beneficiary is established in the Union.

2. This Regulation shall not apply to the services listed in Article 3, points (a) to (m) and point (o), of Directive (EU) 2015/2366.

2a. (deleted)

3. This Regulation shall not apply to transfers of funds and transfers of electronic money tokens as defined in article 3(1) point 4 of [MiCA] carried out using a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics, where the following conditions are met:

(a) that card, instrument or device is used exclusively to pay for goods or services; and

(b) the number of that card, instrument or device accompanies all transfers flowing from the transaction.

However, this Regulation shall apply when a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics, is used in order to effect a transfer of funds or electronic money tokens between natural persons acting, as consumers, for purposes other than trade, business or profession.

4. This Regulation shall not apply to persons that have no activity other than to convert paper documents into electronic data and that do so pursuant to a contract with a payment service provider, or to persons that have no activity other than to provide payment service providers with messaging or other support systems for transmitting funds or with clearing and settlement systems.

(deleted)

This Regulation shall not apply to transfers of funds if any of the following conditions is fulfilled:

(a) they involve the payer withdrawing cash from the payer's own payment account;

(b) they constitute transfers of funds to a public authority as payment for taxes, fines or other levies within a Member State;

(c) both the payer and the payee are payment service providers acting on their own behalf;

(d) they are carried out through cheque images exchanges, including truncated cheques.

This Regulation shall not apply to transfers of crypto-assets that fulfil any of the following conditions:

(a) both the originator and the beneficiary are crypto-asset service providers acting on their own behalf;

(b) the transfers constitute person-to-person transfers of crypto-assets carried out without the involvement of a crypto-asset service provider.

Electronic money tokens, as defined in Article 3(1), point 4 of Regulation [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937- COM/2020/593 final] shall be treated as crypto-assets under this Regulation.

(deleted)

5. A Member State may decide not to apply this Regulation to transfers of funds within its territory to a payee's payment account permitting payment exclusively for the provision of goods or services where all of the following conditions are met:

(a) the payment service provider of the payee is subject to Directive (EU) 2015/849 ;

(b) the payment service provider of the payee is able to trace back, through the payee, by means of a unique transaction identifier, the transfer of funds from the person who has an agreement with the payee for the provision of goods or services;

(c) the amount of the transfer of funds does not exceed EUR 1000.

Article 3
Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'terrorist financing' means terrorist financing as defined in Article 1(5) of Directive (EU) 2015/849;

(2) 'money laundering' means the money laundering activities referred to in Article 1(3) and (4) of Directive (EU) 2015/849;

(3) 'payer' means a person that holds a payment account and allows a transfer of funds from that payment account, or, where there is no payment account, that gives a transfer of funds order;

(4) 'payee' means a person that is the intended recipient of the transfer of funds;

(5) ‘payment service provider’ means the categories of payment service provider referred to in Article 1(1) of Directive (EU) 2015/2366, natural or legal persons benefiting from a waiver pursuant to Article 32 thereof and legal persons benefiting from a waiver pursuant to Article 9 of Directive 2009/110/EC of the European Parliament and of the Council[21], providing transfer of funds services;

(6) ‘intermediary payment service provider’ means a payment service provider that is not the payment service provider of the payer or of the payee and that receives and transmits a transfer of funds on behalf of the payment service provider of the payer or of the payee or of another intermediary payment service provider;

(7) ‘payment account’ means a payment account as defined in Article 4, point (12), of Directive (EU) 2015/2366;

(8) ‘funds’ means funds as defined in Article 4, point (25), of Directive (EU) 2015/2366;

(9) ‘transfer of funds’ means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including:

(a) a credit transfer as defined in Article 4, point (24), of Directive (EU) 2015/2366;

(b) a direct debit as defined in Article 4, point (23), of Directive (EU) 2015/2366;

(c) a money remittance as defined in Article 4, point (22), of Directive (EU) 2015/2366, whether national or cross border;

---

**21** 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).

(d) a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics;

(10) ‘transfer of crypto-assets’ means any transaction with the aim of moving crypto-assets from one distributed ledger address, crypto-asset account or any other device allowing to store crypto-assets to another, carried out by at least one crypto-asset service provider acting on behalf of either an originator or a beneficiary, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the crypto-asset service provider of the originator and that of the beneficiary are one and the same.

(11) ‘batch file transfer’ means a bundle of several individual transfers of funds or crypto-assets put together for transmission;

(12) ‘unique transaction identifier’ means a combination of letters, numbers or symbols determined by the payment service provider, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, or determined by a crypto-asset service provider, which permits the traceability of the transaction back to the payer and the payee or the traceability of transfer of crypto-assets back to the originator and the beneficiary;

(13) (deleted)

(14) ‘person-to-person transfer of crypto-assets’ means a transfer of crypto-assets without the involvement of any crypto-asset service providers;

(15) ‘crypto-asset’ means a crypto-asset as defined in Article 3(1), point 2, of Regulation [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final] except when falling under the categories listed in Article 2(2) and 2(2a) of that Regulation or otherwise qualifying as funds.

(16) ‘crypto-asset service provider ’means a crypto-asset service provider as defined in Article 3(1), point (8), of [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final] where performing one or more crypto-asset services as defined in Article 3(1), point (9), of [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final];

(16a) ‘intermediary crypto-asset service provider’ means a crypto-asset service provider that is not the crypto-asset service provider of the originator or of the beneficiary and that receives and transmits a transfer of crypto-assets on behalf of the crypto-asset service provider of the originator or of the beneficiary, or of another intermediary crypto-asset service provider;

(16b) ‘crypto-asset automated teller machines (‘crypto-ATMs’)’ are physical or on-line electronic terminals that enable a crypto asset service provider to perform, in particular, the activity of transfer of crypto-assets, as referred to in [Article 3(1), point (9) (j)], of [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final].

(17) ‘ distributed ledger address’ means an alphanumeric code that identifies an address on a network using distributed ledger technology or similar technology where crypto-assets can be sent or received;

(18) ‘ crypto-asset account’ means an account held by a crypto-asset service provider in the name of one or more natural or legal persons which can be used for the execution of transfers of crypto-assets;

(18a) "self-hosted address" means a distributed ledger address not linked to either of the following:
a) a crypto-asset service provider;
b) an entity not established in the EU and providing similar services.

(19) ‘originator’ means a person that holds a crypto-asset account with a crypto-asset service provider, a distributed ledger address or any other device allowing to store crypto-assets, and allows a transfer of crypto-assets from that account, distributed ledger address, or such device, or, where there is no account, distributed ledger address, or such device, that orders or initiates a transfer of crypto-assets ;

(20) ‘beneficiary’ means a person that is the intended recipient of the transfer of crypto-assets;

(21) ‘legal entity identifier’ (LEI) means a unique alphanumeric reference code based on the ISO 17442 standard assigned to a legal entity.

## CHAPTER II
## OBLIGATIONS ON PAYMENT SERVICE PROVIDERS

### SECTION 1 Obligations on the payment service provider of the payer

#### Article 4
#### Information accompanying transfers of funds

1. The payment service provider of the payer shall ensure that transfers of funds are accompanied by the following information on the payer:

(a) the name of the payer;

(b) the payer's payment account number;

(c) the payer's address, including the name of the country, official personal document number, and the customer identification number or, alternatively, date and place of birth .

(d) subject to the existence of the necessary field in the relevant payments message format, and where provided by the payer to the payer's Payment service provider, the current Legal Entity Identifier of the payer or, in its absence, any available equivalent official identifier.

2. The payment service provider of the payer shall ensure that transfers of funds are accompanied by the following information on the payee:

(a) the name of the payee;

(b) the payee's payment account number;

(c) subject to the existence of the necessary field in the relevant payments message format, and where provided by the payer to the payer's Payment service provider, the current Legal Entity Identifier of the payee or, in its absence, any available equivalent official identifier.

3. By way of derogation from paragraph 1 , point (b), and paragraph 2, point (b), in the case of a transfer not made from or to a payment account, the payment service provider of the payer shall ensure that the transfer of funds is accompanied by a unique transaction identifier rather than the payment account number(s).

4. Before transferring funds, the payment service provider of the payer shall verify the accuracy of the information referred to in paragraph 1 and, where applicable, in paragraph 3, on the basis of documents, data or information obtained from a reliable and independent source.

5. Verification as referred to in paragraph 4 shall be deemed to have taken place where:

(a) a payer's identity has been verified in accordance with Article 13 of Directive (EU) 2015/849 and the information obtained pursuant to that verification has been stored in accordance with Article 40 of that Directive; or

(b) Article 14(5) of Directive (EU) 2015/849 applies to the payer.

6. Without prejudice to the derogations provided for in Articles 5 and 6, the payment service provider of the payer shall not execute any transfer of funds before ensuring full compliance with this Article.

Article 5
Transfers of funds within the Union

1. By way of derogation from Article 4(1) and (2), where all payment service providers involved in the payment chain are established in the Union, transfers of funds shall be accompanied by at least the payment account number of both the payer and the payee or, where Article 4(3) applies, the unique transaction identifier, without prejudice to the information requirements laid down in Regulation (EU) No 260/2012, where applicable.

2. Notwithstanding paragraph 1, the payment service provider of the payer shall, within three working days of receiving a request for information from the payment service provider of the payee or from the intermediary payment service provider, make available the following:

(a) for transfers of funds exceeding EUR 1000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked, the information on the payer or the payee in accordance with Article 4;

(b) for transfers of funds not exceeding EUR 1000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1000, at least:

(i) the names of the payer and of the payee; and

(ii) the payment account numbers of the payer and of the payee or, where Article 4(3) applies, the unique transaction identifier.

3. By way of derogation from Article 4(4), in the case of transfers of funds referred to in paragraph 2, point (b), of this Article, the payment service provider of the payer need not verify the information on the payer unless the payment service provider of the payer:

(a) has received the funds to be transferred in cash or in anonymous electronic money; or

(b) has reasonable grounds for suspecting money laundering or terrorist financing.

Article 6
Transfers of funds to outside the Union

1. In the case of a batch file transfer from a single payer where the payment service providers of the payees are established outside the Union, Article 4(1) shall not apply to the individual transfers bundled together therein, provided that the batch file contains the information referred to in Article 4(1), (2) and (3), that that information has been verified in accordance with Article 4(4) and (5), and that the individual transfers carry the payment account number of the payer or, where Article 4(3) applies, the unique transaction identifier.

2. By way of derogation from Article 4(1), and, where applicable, without prejudice to the information required in accordance with Regulation (EU) No 260/2012, where the payment service provider of the payee is established outside the Union, transfers of funds not exceeding EUR 1000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1000, shall be accompanied by at least:

(a) the names of the payer and of the payee; and

(b) the payment account numbers of the payer and of the payee or, where Article 4(3) applies, the unique transaction identifier.

By way of derogation from Article 4(4), the payment service provider of the payer need not verify the information on the payer referred to in this paragraph unless the payment service provider of the payer:

(a) has received the funds to be transferred in cash or in anonymous electronic money; or

(b) has reasonable grounds for suspecting money laundering or terrorist financing.

## SECTION 2 Obligations on the payment service provider of the payee

### Article 7
### Detection of missing information on the payer or the payee

1. The payment service provider of the payee shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system.

2. The payment service provider of the payee shall implement effective procedures, including, where appropriate, monitoring after or during the transfers , in order to detect whether the following information on the payer or the payee is missing:

(a) for transfers of funds where the payment service provider of the payer is established in the Union, the information referred to in Article 5;

(b) for transfers of funds where the payment service provider of the payer is established outside the Union, the information referred to in Article 4(1), points (a), (b) and (c), and Article 4(2), points (a) and (b);

(c) for batch file transfers where the payment service provider of the payer is established outside the Union, the information referred to in Article 4(1), points (a), (b) and (c), and Article 4(2), points (a) and (b), in respect of that batch file transfer.

3. In the case of transfers of funds exceeding EUR 1000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked, before crediting the payee's payment account or making the funds available to the payee, the payment service provider of the payee shall verify the accuracy of the information on the payee referred to in paragraph 2 of this Article on the basis of documents, data or information obtained from a reliable and independent source, without prejudice to the requirements laid down in Articles 83 and 84 of Directive (EU) 2015/2366 .

4. In the case of transfers of funds not exceeding EUR 1000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1000, the payment service provider of the payee need not verify the accuracy of the information on the payee, unless the payment service provider of the payee:

(a) effects the pay-out of the funds in cash or in anonymous electronic money; or

(b) has reasonable grounds for suspecting money laundering or terrorist financing.

5. Verification as referred to in paragraphs 3 and 4 shall be deemed to have taken place where:

(a) a payee's identity has been verified in accordance with Article 13 of Directive (EU) 2015/849 and the information obtained pursuant to that verification has been stored in accordance with Article 40 of that Directive; or

(b) Article 14(5) of Directive (EU) 2015/849 applies to the payee.

Article 8

Transfers of funds with missing or incomplete information on the payer or the payee

1. The payment service provider of the payee shall implement effective risk-based procedures, including procedures based on the risk-sensitive basis referred to in Article 13 of Directive (EU) 2015/849 for determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up action.

Where the payment service provider of the payee becomes aware, when receiving transfers of funds, that the information referred to in Article 4(1), points (a), (b) and (c), Article 4(2), points (a) and (b), Article 5(1) or Article 6 is missing or incomplete or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in Article 7(1), the payment service provider of the payee shall on a risk-sensitive basis:

(a) reject the transfer or

(b) ask for the required information on the payer and the payee before or after crediting the payee's payment account or making the funds available to the payee.

2. Where a payment service provider repeatedly fails to provide the required information on the payer or the payee, the payment service provider of the payee shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider, or restricting or terminating its business relationship with that payment service provider.

The payment service provider of the payee shall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.

Article 9
Assessment and reporting

The payment service provider of the payee shall take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it is to be reported to the Financial Intelligence Unit (FIU) in accordance with Directive (EU) 2015/849.

SECTION 3 Obligations on intermediary payment service providers

Article 10
Retention of information on the payer and the payee with the transfer

Intermediary payment service providers shall ensure that all the information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer.

Article 11
Detection of missing information on the payer or the payee

1. The intermediary payment service provider shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system.

2. The intermediary payment service provider shall implement effective procedures, including, where appropriate, monitoring after or during the transfers, in order to detect whether the following information on the payer or the payee is missing:

(a) for transfers of funds where the payment service providers of the payer and the payee are established in the Union, the information referred to in Article 5;

(b) for transfers of funds where the payment service provider of the payer or of the payee is established outside the Union, the information referred to in Article 4(1), points (a), (b) and (c), and Article 4(2), points (a) and (b);

(c) for batch file transfers where the payment service provider of the payer or of the payee is established outside the Union, the information referred to in Article 4(1) and (2) in respect of that batch file transfer.

Article 12
Transfers of funds with missing information on the payer or the payee

1. The intermediary payment service provider shall establish effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information and for taking the appropriate follow up action.

Where the intermediary payment service provider becomes aware, when receiving transfers of funds, that the information referred to in Article 4(1), points (a), (b) and (c), Article 4, points (2)(a) and (b), Article 5(1) or Article 6 is missing or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in Article 7(1) it shall reject the transfer or ask for the required information on the payer and the payee before or after the transmission of the transfer of funds, on a risk-sensitive basis.

2. Where a payment service provider repeatedly fails to provide the required information on the payer or the payee, the intermediary payment service provider shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider, or restricting or terminating its business relationship with that payment service provider.

The intermediary payment service provider shall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.

Article 13
Assessment and reporting

The intermediary payment service provider shall take into account missing information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious, and whether it is to be reported to the FIU in accordance with Directive (EU) 2015/849.

CHAPTER III
Obligations on crypto-asset service providers

SECTION 1 Obligations on the crypto-asset service provider of the originator

Article 14
Information accompanying transfers of crypto-assets

1. The crypto-asset service provider of the originator shall ensure that transfers of crypto-assets are accompanied by the following information on the originator:

(a) the name of the originator;

(b) the originator's distributed ledger address, where a transfer of crypto-assets is registered on a network using distributed ledger technology or similar technology, and the crypto-asset account number of the originator, where such an account exists and is used to process the transaction;

(ba) the originator's crypto-asset account number, where a transfer of crypto-assets is not registered on a network using distributed ledger technology or similar technology;

(c) the originator's address, including the name of the country, official personal document number, and the customer identification number or, alternatively, date and place of birth.

(ca) subject to the existence of the necessary field in the relevant message format, and where provided by the originator to the originator's crypto-assets service provider, the current LEI of the originator or any other available equivalent official identifier.

2. The crypto-asset service provider of the originator shall ensure that transfers of crypto-assets are accompanied by the following information on the beneficiary:

(a) the name of the beneficiary;

(b) the beneficiary's distributed ledger address, where a transfer of crypto-assets is registered on a network using distributed ledger technology or similar technology and, the beneficiary's crypto-asset account number, where such an account exists and is used to process the transaction;

(ba) the beneficiary's crypto-asset account number, where a transfer of crypto-assets is not registered on a network using distributed ledger technology or similar technology;

(bb) subject to the existence of the necessary field in the relevant message format, and where provided by the originator to its crypto-asset service provider, the current LEI of the beneficiary or any other available equivalent official identifier.

3. By way of derogation from paragraph 1, point (ba), and paragraph 2, point (ba), in the case of a transfer of crypto-assets not registered on a network using distributed ledger technology or similar technology and not made from or to a crypto-asset account, the crypto-asset service provider of the originator shall ensure that the transfer of crypto-assets is accompanied by a unique transaction identifier.

4. The information referred to in paragraphs 1 and 2 shall be submitted in advance of, or simultaneously or concurrently with, the transfer of crypto-assets and in a secure manner and in line with the provisions and obligations of Regulation (EU) 2016/679.

The information referred to in paragraphs 1 and 2 does not have to be attached directly to, or be included in, the transfer of crypto-assets.

4a. In the case of a transfer of crypto-assets made to a self-hosted address, the crypto-asset service provider of the originator shall obtain and hold information referred to in paragraphs 1 and 2 and ensure that the transfer of crypto-assets can be individually identified.

Without prejudice to specific measures in accordance with AMLD article 19b, in case of a transfer whose amount exceeds EUR 1,000 to a self-hosted address, the crypto-asset service provider of the originator shall take adequate measures to assess if such address is owned or controlled by the originator.

4b. (deleted)

5. Before transferring crypto-assets, the crypto-asset service provider of the originator shall verify the accuracy of the information referred to in paragraph 1 on the basis of documents, data or information obtained from a reliable and independent source.

5a. (deleted)

5b. (deleted)

6. Verification as referred to in paragraph 5 shall be deemed to have taken place where

(a) the identity of the originator has been verified in accordance with Article 13 of Directive (EU) 2015/849 and the information obtained pursuant to that verification has been stored in accordance with Article 40 of that Directive or

(b) Article 14(5) of Directive (EU) 2015/849 applies to the originator.

6a. (deleted)

7. The crypto-asset service provider of the originator shall not allow for the initiation of or execute any transfer of crypto-assets before ensuring full compliance with this Article.

Article 15
Transfers of crypto-assets

1. In the case of a batch file transfer from a single originator, Article 14(1) shall not apply to the individual transfers bundled together therein, provided that the batch file contains the information referred to in Article 14(1), (2) and (3), that that information has been verified in accordance with Article 14(5) and (6), and that the individual transfers carry the distributed ledger address of the originator, where Article 14(2)(b) applies, the crypto-asset account number of the originator , where Article 14(2)(ba) applies, or the individual identification of the transfer, where Article 14(3) applies.

2. (deleted)

(a) (deleted)

(b) (deleted)

(deleted)

(a) (deleted)

(b) (deleted)

SECTION 2 Obligations on the crypto-asset service provider of the beneficiary

Article 16
Detection of missing information on the originator or the beneficiary

1. The crypto-asset service provider of the beneficiary shall implement effective procedures, including, where appropriate, monitoring after or during the transfers, in order to detect whether the information referred to in Article 14(1) and (2), on the originator and the beneficiary is included in, or follows, the transfer of crypto-assets or batch file transfer.

1a. In the case of a transfer of crypto-assets made from a self-hosted address, the crypto-asset service provider of the beneficiary shall obtain and hold information referred to in article 14 (1) and (2) and ensure that the transfer of crypto-assets can be individually identified.

Without prejudice to specific measures in accordance with AMLD article 19b, in case of a transfer whose amount exceeds EUR 1,000 from self-hosted address, the crypto-asset service provider of the beneficiary shall take adequate measures to assess if such address is owned or controlled by the beneficiary.

2. Before making the crypto-assets available to the beneficiary, the crypto-asset service provider of the beneficiary shall verify the accuracy of the information on the beneficiary referred to in Article 14 paragraph 2, on the basis of documents, data or information obtained from a reliable and independent source .

2a. (deleted)

3. (deleted)

(a) (deleted)

(b) (deleted)

4. Verification as referred to in paragraphs 1a and 2 shall be deemed to have taken place where one of the following applies:

(a) the identity of the crypto-assets transfer beneficiary has been verified in accordance with Article 13 of Directive (EU) 2015/849 and the information obtained pursuant to that verification has been stored in accordance with Article 40 of that Directive;

(b) Article 14(5) of Directive (EU) 2015/849 applies to the crypto-assets transfer beneficiary.

4a. (deleted)

Article 17

Transfers of crypto-assets with missing or incomplete information on the originator or the beneficiary

1. The crypto-asset service provider of the beneficiary shall implement effective risk-based procedures, including procedures based on the risk-sensitive basis referred to in Article 13 of Directive (EU) 2015/849, for determining whether to execute or reject or suspend a transfer of crypto-assets lacking the required complete originator and beneficiary information and for taking the appropriate follow-up action.

Where the crypto-asset service provider of the beneficiary becomes aware, that the information referred to in Article 14(1) or (2) or Article 15 is missing or incomplete, the crypto-asset service provider shall before making the crypto-assets available to the beneficiary, on a risk-sensitive basis and without undue delay:

(a) reject the transfer or return the transferred crypto-assets to the originator's crypto-asset account; or

(b) ask for the required information on the originator and the beneficiary before making the crypto-assets available to the beneficiary.

(c) (deleted)

2. Where a crypto-asset service provider repeatedly fails to provide the required information on the originator or the beneficiary, the provider of crypto-asset provider of the beneficiary shall:

a) take steps, which may initially include the issuing of warnings and setting of deadlines ; or

b) reject any future transfers of crypto-assets from or to, or restrict or terminate its business relationship with, a provider of crypto-asset transfers that fails to provide the required information.

The crypto-asset service provider of the beneficiary shall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.

(deleted)

Article 18
Assessment and reporting

The crypto-asset service provider of the beneficiary shall take into account missing or incomplete information on the originator or the beneficiary as a factor when assessing whether a transfer of crypto-assets, or any related transaction, is suspicious and whether it is to be reported to the FIU in accordance with Directive (EU) 2015/849 .

SECTION 2 a
Obligations on intermediary crypto-asset service providers

Article 18 a
Retention of information on the originator and the beneficiary with the transfer

Intermediary crypto-asset service providers shall ensure that all the information received on the originator and the beneficiary that accompanies a transfer of crypto-assets is transmitted with the transfer and that records of such information are retained and made available on request to the competent authorities.

Article 18 b
Detection of missing information on the originator or the beneficiary

The intermediary crypto-asset service provider shall implement effective procedures, including, where appropriate, monitoring after or during the transfers, to detect whether the information referred to in Article 14(1) points (a), (b) and (c) and Article 14 (2) points (a), (b) and (ba) on the originator or the beneficiary is submitted previously, simultaneously or concurrently with with the transfer of crypto-assets or batch file transfer, including where the transfer is made from or to a self-hosted address.

Article 18 c

Transfers of crypto-assets with missing information on the originator or the beneficiary

1. The intermediary crypto-asset service provider shall establish effective risk-based procedures, including procedures based on the risk-sensitive basis referred to in Article 13 of Directive (EU) 2015/849, for determining whether to execute, reject or suspend a transfer of crypto-assets lacking the required originator and beneficiary information and for taking the appropriate follow up action. Where the intermediary crypto-asset service provider becomes aware, when receiving transfers of crypto-assets, that the information referred to in Article 14(1) points (a), (b) and (c) and Article 14 (2) points (a), (b) and (ba) or Article 15(1) is missing or incomplete, it shall, before making the transmission of the transfer of crypto-assets, on a risk-sensitive basis and without undue delay:

(a) reject the transfer or return the transferred crypto-assets ;
or
(b) ask for the required information on the originator and the beneficiary;

2. Where the crypto-asset service provider repeatedly fails to provide the required information on the originator or the beneficiary, the intermediary crypto-asset service provider:

(a) shall take steps, which may initially include the issuing of warnings and setting of deadlines; or
(b) reject any future transfers of crypto-assets from or to, or restrict or terminate its business relationship with that crypto-asset services provider.

The intermediary crypto-asset service provider shall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.

Article 18 d
Assessment and reporting

The intermediary crypto-asset service provider shall take into account missing information on the originator or the beneficiary as a factor when assessing whether a transfer of crypto-asset, or any related transaction, is suspicious, and whether it is to be reported to the FIU in accordance with Directive (EU) 2015/849.

Chapter IIIa
(deleted)

Article 18b
(deleted)

1. (deleted)

2. (deleted)

(a) (deleted)

(b) (deleted)

3. (deleted)

Article 18c
(deleted)

1. (deleted)

(a) (deleted)

(b) (deleted)

(c) (deleted)

(d) (deleted)

Article 18d
(deleted)

1. (deleted)

2. (deleted)

(1) (deleted)

(a) (deleted)

(1) (deleted)

(b) (deleted)

(c) (deleted)

(d) (deleted)

(1) (deleted)

(e) (deleted)

(f) (deleted)

3. (deleted)

4. (deleted)

Article 18e
(deleted)

1. (deleted)

(a) (deleted)

(b) (deleted)

(c) (deleted)

2. (deleted)

3. (deleted)

4. (deleted)

5. (deleted)

6. (deleted)

CHAPTER IIIb
COMMON MEASURES APPLICABLE BY PAYMENT SERVICE PROVIDERS AND CRYPTO-ASSET SERVICE PROVIDERS

Article 18ad
Internal policies, procedures and controls to ensure implementation of restrictive measures

Payment service providers and crypto asset service providers shall have in place internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures when performing transfers of funds and crypto assets under this regulation.

EBA shall issue guidelines by [18 months after entry into force of this Regulation] specifying the measures referred to in this Article.

CHAPTER IV
INFORMATION, DATA PROTECTION AND RECORD-RETENTION

Article 19
Provision of information

Payment service providers and crypto-asset service providers shall respond fully and without delay, including by means of a central contact point in accordance with Article 45(9) of Directive (EU) 2015/849, where such a contact point has been appointed, and in accordance with the procedural requirements laid down in the national law of the Member State in which they are established, to enquiries exclusively from the authorities responsible for preventing and combating money laundering or terrorist financing of that Member State concerning the information required under this Regulation.

Article 20
Data protection

1. The processing of personal data under this Regulation is subject to Regulation (EU) 2016/679 . Personal data that is processed pursuant to this Regulation by the Commission or EBA is subject to Regulation (EU) 2018/1725 .

2. Personal data shall be processed by payment service providers and crypto-asset service providers on the basis of this Regulation only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Regulation for commercial purposes shall be prohibited.

3. Payment service providers and crypto-asset service providers shall provide new clients with the information required pursuant to Article 13 of Regulation (EU) 2016/679 before establishing a business relationship or carrying out an occasional transaction. That information shall be provided in a concise, transparent, intelligible and easily accessible form in accordance with article 12 of [insert reference to GDPR], and shall in particular include a general notice concerning the legal obligations of payment service providers and crypto-asset service providers under this Regulation when processing personal data for the purposes of the prevention of money laundering and terrorist financing.

4. Payment and crypto-asset service providers shall ensure at all times that the transmission of information on the parties involved in a transfer is conducted in accordance with the data protection requirements under Regulation (EU) 2016/679 [GDPR].

The European Data Protection Board shall, after consultation of the EBA, issue guidelines on the practical implementation of data protection requirements for transfers of personal data to third countries in the context of transfers of crypto-assets. The EBA shall issue guidelines on suitable procedures for determining whether to execute, reject or suspend a transfer of crypto-assets, in situations where compliance with data protection requirements for the transfer of personal data to third countries cannot be ensured.

Article 21
Record retention

1. Information on the payer and the payee , or, for transfers of crypto-assets, on the originator and beneficiary, shall not be retained for longer than strictly necessary. Payment service providers of the payer and of the payee shall retain records of the information referred to in Articles 4 to 7 and crypto-asset service providers of the originator and beneficiary shall retain records of the information referred to in Articles 14 to 16, for a period of five years.

2. Upon expiry of the retention period referred to in paragraph 1, payment service providers and crypto-asset service providers shall ensure that the personal data is deleted, unless otherwise provided for by national law, which determines under which circumstances payment service providers and crypto-asset service providers may or shall further retain the data. Member States may allow or require further retention only after they have carried out a thorough assessment of the necessity and proportionality of such further retention, and where they consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. That further retention period shall not exceed five years.

3. Where, on 25 June 2015, legal proceedings concerned with the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing are pending in a Member State, and a payment service provider holds information or documents relating to those pending proceedings, the payment service provider may retain that information or those documents in accordance with national law for a period of five years from 25 June 2015. Member States may, without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings, allow or require the retention of such information or documents for a further period of five years where the necessity and proportionality of such further retention has been established for the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing.

Article 21a
Cooperation among competent authorities

The exchange of information among national competent authorities and with relevant third-country authorities under this Regulation shall be subject to the provisions laid down in Directive (EU) 2015/849.

CHAPTER V
SANCTIONS AND MONITORING

Article 22
Administrative sanctions and measures

1. Without prejudice to the right to provide for and impose criminal sanctions, Member States shall lay down the rules on administrative sanctions and measures applicable to breaches of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. The sanctions and measures provided for shall be effective, proportionate and dissuasive and shall be consistent with those laid down in accordance with Chapter VI, Section 4, of Directive (EU) 2015/849 .

Member States may decide not to lay down rules on administrative sanctions or measures for breach of the provisions of this Regulation which are subject to criminal sanctions in their national law. In that case, Member States shall communicate to the Commission the relevant criminal law provisions.

2. Member States shall ensure that where obligations apply to payment service providers and crypto-asset service providers , in the event of a breach of provisions of this Regulation, sanctions or measures can, subject to national law, be applied to the members of the management body and to any other natural person who, under national law, is responsible for the breach.

3. Member States shall notify the rules referred to in paragraph 1 to the Commission and to the Joint Committee of the ESAs. Member States shall notify the Commission and EBA without undue delay of any subsequent amendments thereto.

4. In accordance with Article 58(4) of Directive (EU) 2015/849 , competent authorities shall have all the supervisory and investigatory powers that are necessary for the exercise of their functions. In the exercise of their powers to impose administrative sanctions and measures, competent authorities shall cooperate closely to ensure that those administrative sanctions or measures produce the desired results and coordinate their action when dealing with cross-border cases.

5. Member States shall ensure that legal persons can be held liable for the breaches referred to in Article 23 committed for their benefit by any person acting individually or as part of an organ of that legal person, and having a leading position within the legal person based on any of the following:

(a) power to represent the legal person;

(b) authority to take decisions on behalf of the legal person; or

(c) authority to exercise control within the legal person.

6. Member States shall also ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 5 has made it possible to commit one of the breaches referred to in Article 23 for the benefit of that legal person by a person under its authority.

7. Competent authorities shall exercise their powers to impose administrative sanctions and measures in accordance with this Regulation in any of the following ways:

(a) directly;

(b) in collaboration with other authorities;

(c) under their responsibility by delegation to such other authorities;

(d) by application to the competent judicial authorities.

In the exercise of their powers to impose administrative sanctions and measures, competent authorities shall cooperate closely in order to ensure that those administrative sanctions or measures produce the desired results and coordinate their action when dealing with cross-border cases.

Article 23
Specific provisions

Member States shall ensure that their administrative sanctions and measures include at least those laid down in Article 59(2) and (3) of Directive (EU) 2015/849 in the event of the following breaches of this Regulation:

(a) repeated or systematic failure by a payment service provider to include the required information on the payer or the payee, in breach of Article 4, 5 or 6 or by a crypto-asset service provider to include the required information on the originator and beneficiary, in breach of Articles 14 and 15 ;

(b) repeated, systematic or serious failure by a payment service provider or crypto-asset service provider to retain records, in breach of Article 21;

(c) failure by a payment service provider to implement effective risk-based procedures, in breach of Article 8 or 12 or by a crypto-asset service provider to implement effective risk-based procedures, in breach of Article 17 ;

(d) serious failure by an intermediary payment service provider to comply with Article 11 or 12.

(da) (deleted)

Article 24
Publication of sanctions and measures

In accordance with Article 60(1), (2) and (3) of Directive (EU) 2015/849 , the competent authorities shall publish administrative sanctions and measures imposed in the cases referred to in Articles 22 and 23 of this Regulation without undue delay, including information on the type and nature of the breach and the identity of the persons responsible for it, if necessary and proportionate after a case-by-case evaluation.

Article 25
Application of sanctions and measures by the competent authorities

1. When determining the type of administrative sanctions or measures and the level of administrative pecuniary sanctions, the competent authorities shall take into account all relevant circumstances, including those listed in Article 60(4) of Directive (EU) 2015/849.

2. As regards administrative sanctions and measures imposed in accordance with this Regulation, Article 62 of Directive (EU) 2015/849 shall apply.

Article 26
Reporting of breaches

1. Member States shall establish effective mechanisms to encourage the reporting to competent authorities of breaches of this Regulation.

Those mechanisms shall include at least those referred to in Article 61(2) of Directive (EU) 2015/849.

2. Payment service providers and crypto-asset service providers , in cooperation with the competent authorities, shall establish appropriate internal procedures for their employees, or persons in a comparable position, to report breaches internally through a secure, independent, specific and anonymous channel, proportionate to the nature and size of the payment service provider or the crypto-asset service provider concerned.

Article 27
Monitoring

1. Member States shall require competent authorities to monitor effectively and to take the measures necessary to ensure compliance with this Regulation and encourage, through effective mechanisms, the reporting of breaches of the provisions of this Regulation to competent authorities.

2. Two years after the application of this Regulation and every three years thereafter , the Commission shall submit a report to the European Parliament and to the Council on the application of Chapter V, with particular regard to cross-border cases.

CHAPTER VI
IMPLEMENTING POWERS

Article 28
Committee procedure

1. The Commission shall be assisted by the Committee on the Prevention of Money Laundering and Terrorist Financing. 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.

CHAPTER VII
DEROGATIONS

Article 29
Agreements with countries and territories which do not form part of the territory of the Union

1. The Commission may authorise any Member State to conclude an agreement with a third country or with a territory outside the territorial scope of the TEU and the TFEU as referred to in Article 355 TFEU (the 'country or territory concerned'), which contains derogations from this Regulation, in order to allow transfers of funds between that country or territory and the Member State concerned to be treated as transfers of funds within that Member State.

Such agreements may be authorised only where all of the following conditions are met:

(a) the country or territory concerned shares a monetary union with the Member State concerned, forms part of the currency area of that Member State or has signed a monetary convention with the Union represented by a Member State;

(b) payment service providers in the country or territory concerned participate directly or indirectly in payment and settlement systems in that Member State;

(c) the country or territory concerned requires payment service providers under its jurisdiction to apply the same rules as those established under this Regulation.

2. A Member State wishing to conclude an agreement as referred to in paragraph 1 shall submit a request to the Commission and provide it with all the information necessary for the appraisal of the request.

3. Upon receipt by the Commission of such a request, transfers of funds between that Member State and the country or territory concerned shall be provisionally treated as transfers of funds within that Member State until a decision is reached in accordance with this Article.

4. If, within two months of receipt of the request, the Commission considers that it does not have all the information necessary for the appraisal of the request, it shall contact the Member State concerned and specify the additional information required.

5. Within one month of receipt of all the information that it considers to be necessary for the appraisal of the request, the Commission shall notify the requesting Member State accordingly and shall transmit copies of the request to the other Member States.

6. Within three months of the notification referred to in paragraph 5 of this Article, the Commission shall decide whether to authorise the Member State concerned to conclude the agreement that is the subject of the request. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 28(2).

The Commission shall, in any event, adopt a decision as referred to in the first subparagraph within 18 months of receipt of the request.

Chapter VIIa
OTHER PROVISIONS

Article 30
Guidelines

The ESAs shall issue guidelines addressed to the competent authorities and the payment service providers in accordance with Article 16 of Regulation (EU) No 1093/2010 on measures to be taken in accordance with this Regulation, in particular as regards the implementation of Articles 7, 8, 11 and 12 of this Regulation. By [12 months after entry into force of this Regulation], EBA shall issue guidelines addressed to the competent authorities and to the crypto-asset service providers on measures to be taken as regards the implementation of Articles 14, 15, 16, 17, 18a, 18b, 18c, 18d of this Regulation .

The EBA shall issue guidelines specifying technical aspects of the application of this Regulation to direct debits as well as the measures to be taken by payment initiation service providers under this Regulation, taking into account their limited role in payment transactions.

The EBA shall issue guidelines, addressed to competent authorities, on the characteristics of a risk-based approach to supervision of crypto-asset service providers and the steps to be taken when conducting supervision on a risk-based basis.

The EBA shall ensure a regular dialogue with stakeholders on the development of technical interoperable solutions with the view of facilitating the implementation of the requirements laid down in that Regulation.

Article 30a
Review Clause

1. [By 12 months after the entry into force of Regulation [Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849], the Commission shall review this Regulation and shall, if appropriate, propose amendments in order to ensure a consistent approach and alignment with [Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849].]

2. No later than [18 months after the date of application of this Regulation], the Commission, after consulting EBA, shall issue a report assessing the risks posed by transfers from or to self-hosted addresses or entities not established in the EU, as well as the need for specific measures to mitigate those risks, and propose, if appropriate, amendments to this Regulation.

3. By ... [please insert date - 4 years after the date of entry into force of this Regulation], the Commission shall submit to the European Parliament and to the Council a report on the application and enforcement of this Regulation accompanied, if appropriate, by a legislative proposal.

That report shall include the following elements:

(a) an assessment of the effectiveness of the measures provided for in this Regulation and the compliance with this Regulation by payment service providers and crypto asset service providers;

(aa) an assessment of the technological solutions for complying with the obligations imposed on crypto asset service providers under this Regulation, including the latest developments of technologically sound and interoperable solutions for complying this regulation and the use of blockchain analysis for identifying the origin and destination of transfers in crypto-assets and know your transaction (KYT) assessment;

(ab) an assessment of the effectiveness and suitability of the de minimis thresholds related to transfers of funds, in particular with respect to the scope of application and the set of information accompanying transfers, and an assessment of the need of lowering or removing such threshold related to transfer of funds;

(ac) assessment of the costs and benefits of introducing de minimis thresholds related to the set of information accompanying transfers of crypto-assets, including an assessment of the related money laundering and terrorist financing risks;

(b) (deleted)

(c) (deleted)

(d) (deleted)

(e) an analysis of the trends in the use of self-hosted addresses to perform transfers without the involvement of a third party, together with an assessment of the related money laundering and terrorist financing risks and an evaluation of the need, effectiveness and enforceability of additional mitigation measures, including specific obligations on providers of hardware and software wallets and limitations, control or prohibition of transfers involving self-hosted addresses;

(f) (deleted)

The Report shall take into account the developments as well as relevant evaluations, assessments and reports drawn up by international organisations and standard setters in the field of preventing money laundering and combating terrorist financing, law enforcement authorities and intelligence agencies and any information provided by crypto-asset service providers or other reliable sources.

CHAPTER VIII
FINAL PROVISIONS

Article 30b
Amendments to Directive (EU) 2015/849

Directive (EU) 2015/849 is amended as follows:

(1) Article 2(1), point 3, is amended as follows:

(a) point (g) is deleted.

(deleted)

(b) point (h) is deleted;

(2) Article 3 is amended as follows:

(a) In point 2, the following point is inserted:
‘(g) crypto-asset service providers’;

(b) point (8) is replaced by the following:

(8) ‘correspondent relationship’ means:

(a) the provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;

(b) the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers or relationships established for crypto-asset services including crypto-asset transfers;

(c) point 18 is replaced by the following:

‘(18) ‘crypto-asset’ means a crypto-asset as defined in Article 3(1), point (2), of [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM/2020/593 final] except when falling under the categories listed in Article 2(2) and (2a) of that Regulation or otherwise qualifying as funds;’;

(d) point 19 is replaced by the following:

‘(19) ‘crypto-asset service providers ’ means a crypto-asset service provider as defined in Article 3(1), point (8), of Regulation [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM/2020/593 final] where performing one or more crypto-asset services as defined in Article 3(1), point (9), of that Regulation, with the exception of providing advice on crypto-assets as defined in point (9)(h) of that Article.’;

(e) point 19a is inserted:
'(19a) self-hosted address means as defined in Article 3(1) point 18a of [Funds Transfer Regulation]'

(3) in article 18 the following paragraphs are added:

‘5. By ... [18 months after the entry into force of the Regulation on Markets in Crypto-assets] the EBA shall issue guidelines on risk variables and risk factors to be taken into account by crypto-asset service providers when entering into business relationships or carrying out transactions in crypto-assets.

6. The EBA shall clarify, in particular, how the risk factors listed in Annex III shall be taken into account by crypto-asset service providers including when performing transactions with persons and entities which are not covered by this Directive. To that end, the EBA shall pay particular attention to products, transactions and technologies that may favor anonymity such as privacy wallets, mixers or tumblers.

Where situations of higher risk are identified, the guidelines shall include enhanced due diligence measures that obliged entities shall consider applying to mitigate such risks, including the adoption of appropriate procedures to detect the origin or destination of crypto-assets.'

(4) the following article is inserted:

'Article 19a

1. Member States shall require the crypto-asset service providers to identify and assess the risk of money laundering and financing of terrorism associated with transfers of crypto-assets directed to or originating from a self-hosted address. To that end, crypto-asset service providers shall have in place internal policies, procedures and controls. Member States shall require crypto-asset service providers to apply mitigating measures commensurate with the risks identified. Those mitigating measures shall include one or more of the following:

(a) taking risk-based measures to identify, and verify the identity of, the originator or beneficiary of a transfer made from or to a self-hosted address or beneficial owner of such originator or beneficiary, including through reliance on third parties;

(b) requiring additional information on the origin and destination of the crypto-assets;

(c) conducting enhanced ongoing monitoring of those transactions.

(d) any other measure to mitigate and manage the risks of money laundering and financing of terrorism as well as the risk of non-implementation and evasion of targeted financial sanctions and proliferation financing-related targeted financial sanctions.

2. By [18 months from the date of entry into force of this Regulation], EBA shall issue guidelines to specify the measures referred to in this Article, including the criteria and means for identification and verification of the identity of, the originator or beneficiary of a transfer made from or to a self-hosted address, including through reliance on third parties, taking into account the latest technological developments;'

(5) the following article is inserted:

'Article 19b

1. By way of derogation from Article 19, with respect to cross-border correspondent relationships involving the execution of crypto-asset services as defined in MiCA with a respondent entity not established in the EU and providing similar services, including transfers of crypto-assets, Member States shall, in addition to the customer due diligence measures laid down in article 13, require crypto-asset service providers, when entering into a business relationship, to:

(a) determine if the respondent entity is licensed or registered;

(b) gather sufficient information about the respondent entity to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the entity and the quality of supervision;

(c) assess the respondent entity AML/CFT controls;

(d) obtain approval from senior management before establishing new correspondent relationships;

(e) document the respective responsibilities of each party to the correspondent relationship;

(f) with respect to payable-through crypto-asset accounts, be satisfied that the respondent entity has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the correspondent entity, and that it is able to provide relevant customer due diligence data to the correspondent entity, upon request.

Where crypto-asset service providers decide to terminate correspondent relationships for reasons relating to anti-money laundering and counter-terrorist financing policy, they shall document and record their decision.

Crypto-asset service providers shall update the due diligence information for the correspondent relationship on a regular basis or when new risks emerge in relation to the respondent entity.

2. Member States shall ensure crypto-asset service providers take into account the information referred to in the first paragraph in order to determine, on a risk sensitive basis, the appropriate measures to be taken to mitigate the risks associated with the respondent entity.

3. By [12 months from the date of entry into force of this Regulation], EBA shall issue guidelines to specify the criteria and elements that crypto-asset services providers shall take into account for conducting the assessment referred to in paragraph 1 and the risk mitigating measures referred to in paragraph 2, including the minimum action to be taken by crypto-asset service providers where the respondent entity is not registered or licensed. '

(6) The following article is inserted

'Article 24a

By 1 January 2024, EBA shall issue guidelines specifying how the enhanced customer due diligence in this Section apply when obliged entities perform services as defined in article 3(1) point 9 of [MICA] as well as transfers of crypto-asset as defined in Article 3 point 10 of [TFR]. In particular EBA shall specify how and when those obliged entities shall obtain additional information on the originator and beneficiary.'

(7) In Article 45, Paragraph 9 is replaced by the following:

‘9. Member States may require electronic money issuers as defined in Article 2(3) of Directive 2009/110/EC, payment service providers as defined in Article 4(11) of Directive (EU) 2015/2366 and crypto-assets service providers established on their territory in forms other than a branch, and whose head office is situated in another Member State, to appoint a central contact point in their territory. That central contact point shall ensure, on behalf of the entity operating on a cross-border basis, compliance with AML/CFT rules and shall facilitate supervision by supervisors, including by providing supervisors with documents and information on request.’

(8) in Article 47, paragraph 1 is replaced by the following:
1. Member States shall ensure that currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered, and that providers of gambling services are regulated.

(deleted)

(9) in Article 67, the following paragraph is added:
‘2a. By ... [date of application of MiCA], Member States shall adopt and publish the provisions necessary to comply with Article 2(1), Article 3, points 2(g), 8, 18 and 19, 19a, Article 19a, paragraph 1, Article 19b, paragraphs 1 and 2, Article 45(9) and Article 47(1), and shall communicate them to the Commission. They shall apply those provisions from ... [date of application of MiCA].’

Article 30c
(deleted)

1. (deleted)

2. (deleted)

3. (deleted)

4. (deleted)

5. (deleted)

Article 30d
(deleted)

(deleted)

Article 31
Repeal

Regulation (EU) 2015/847 is repealed with effect from the date of application of this Regulation.

References to the repealed Regulation shall be construed as references to this Regulation and shall be read in accordance with the correlation table in Annex II.

Article 32
Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from [please insert reference to the date of application of proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final].

(deleted)

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament

The President

For the Council

The President

## Annex I

**Repealed Regulation with the amendment thereto**

Regulation (EU) 2015/847
of the European Parliament and of the Council
(OJ L 141, 5.6.2015, p. 1)

Regulation (EU) 2019/2175 (Only Article 6)
of the European Parliament and of the Council
(OJ L 334, 27.12.2019, p. 1)

**Annex II**

**Correlation Table**

| Regulation (EU) 2015/847 | This Regulation |
|---|---|
| Article 1 | Article 1 |
| Article 2(1), (2) and (3) | Article 2(1), (2) and (3) |
| Article 2(4), first and second subparagraphs | Article 2(4), first and second subparagraphs |
| - | Article 2(4), third and fourth subparagraphs |
| Article 2(5) | Article 2(5) |
| Article 3, introductory wording | Article 3, introductory wording |
| Article 3, points 1 to 9 | Article 3, points 1 to 9 |
| - | Article 3, point 10 |
| Article 3, point 10 | Article 3, point 11 |
| Article 3, point 11 | Article 3, point 12 |
| Article 3, point 12 | - |
| - | Article 3, points 14 to 21 |
| Article 4(1), introductory wording | Article 4(1), introductory wording |
| Article 4(1), points (a), (b) and (c) | Article 4(1), points (a), (b) and (c) |

| Regulation (EU) 2015/847 | This Regulation |
|---|---|
| - | Article 4(1), point (d) |
| Article 4(2), introductory wording | Article 4(2), introductory wording |
| Article 4(2), points (a) and (b) | Article 4(2), points (a) and (b) |
| - | Article 4(2), point (c) |
| Article 4(3) to (6) | Article 4(3) to (6) |
| Articles 5 to 13 | Articles 5 to 13 |
| - | Articles 14 to 18ad |
| Article 14 | Article 19 |
| Article 15(1), (2) and (3) | Article 20(1), (2) and (3) |
| Article 15(4), sole subparagraph | Article 20(4), first subparagraph |
| - | Article 20(4), second subparagraph |
| Article 16 | Article 21 |
| - | Article 21a |
| Article 17 | Article 22 |
| Article 18 | Article 23 |
| Article 19 | Article 24 |

| Regulation (EU) 2015/847 | This Regulation |
|---|---|
| Article 20 | Article 25 |
| Article 21 | Article 26 |
| Article 22 | Article 27 |
| Article 23 | Article 28 |
| Article 24(1) to (6) | Article 29(1) to (6) |
| Article 24(7) | - |
| Article 25, sole subparagraph | Article 30, first subparagraph |
| - | Article 30, second, third and fourth subparagraph |
| - | Article 30a |
| - | Article 30b |
| Article 26 | Article 31 |
| Article 27 | Article 32 |
| Annex | - |
| - | Annex I |
| - | Annex II |