

## EUROPEAN FINTECH ASSOCIATION POSITION PAPER TO THE AMLR

*\* This document enumerates the treatment of various issues of interest to EFA within the AMLR by the Commission, Parliament, and Council texts, and presents EFA's views on each. It includes brief explanations of each position. For ease of reference, we highlight the text we support in green.*

### The following details EFA's views as regards AMLR

**a) Exclusion of PISPs from the AMLR scope:** The [EFA](#) together with the [ETPPA](#) would like to highlight that PISPs are “technical service providers” providing software tools by which the payment order is transmitted by the Payment Service User (PSU) to his bank. Therefore, they **cannot be considered “financial institutions” as they do not hold or handle funds and do not conduct any “financial activity”** - it is the Bank that carries out the transaction. **PISPs cannot provide any additional information** to the data already controlled by the credit institutions they work with. Therefore, **Including TPPs as “obliged entities” is not risk-proportionate and duplicates the bank’s AML procedures.**

**b) CDD outsourcing and related information sharing:** EFA members believe that regulated and performed properly, **CDD outsourcing and sub-outsourcing can help SMEs in Europe compete with larger, more established competitors – without compromising on essential efforts to counter financial crime.**

EFA believes that there is value in a regime which allows for specialisation in the conduct of CDD, including through the use of innovative technologies. Specialisation can both increase effectiveness and decrease cost. Increased effectiveness will help counter criminal exploitation of Europe’s economy, and decreased cost will help reduce the margin of the price of goods and services constituted by regulatory compliance costs. These benefits would be particularly impactful for smaller and more innovative businesses, which are less likely to have the budget, bandwidth, or expertise to conduct CDD either well or efficiently. Regulated and performed reasonably and responsibly, CDD outsourcing and sub-outsourcing, as well as cooperation between obliged entities and between fellow group companies can help small and medium-sized businesses (SMBs) and start-ups in Europe compete with larger, more established competitors – without compromising on essential efforts to counter financial crime.

### Therefore, EFA recommends:

1. The exclusion of PISPs from the AMLR scope (See Annex: Joint EFA- ETTPA paper)
2. Broadening the scope of identity verification and authentication methods for the purposes of eKYC
3. Preserving the risk-based approach in setting deadlines for customer identity verification
4. Ensuring harmonization and consistency when requiring enhanced due diligence to obliged entities
5. Enabling reliance on other obliged entities to meet the customer due diligence requirements
6. Allowing obliged entities to outsource CDD to non-EU entities
7. Proportionate requirements to Intra-group outsourcing
8. Promoting regulatory clarity and ensuring obliged entities are able to outsource certain controls
9. Enabling obliged entities to outsource the drawing up of policies, controls and procedures
10. Enabling obliged entities to outsource the attribution of risk profiles
11. Enabling obliged entities to outsource the identification of criteria for detection of suspicious or unusual transactions or activities

12. Enabling external CDD providers to report suspicious activity directly to FIUs on behalf of obliged entities
13. Addition of new provisions at the end of Article 40 – sub-outsourcing, AMLA guidance, and intra-group “outsourcing”
14. Broadening conditions under which obliged entities may disclose certain AML/CFT activities in order to facilitate AML/CFT efforts and compliance
15. Explicitly permitting the processing of personal data by means of automated decision-making, and the exchange of information in efforts to counter ML/TF

## 2. Identification and verification of customers' methods

Commission Text	EP Text	Council Text
<p>Article 18.4.b Obligated entities shall obtain the information, documents and data necessary for the verification of the customer and beneficial owner identity through either of the following:</p> <p>(a) (...);</p> <p>(b) the use of electronic identification means and relevant trust services as set out in Regulation (EU) 910/2014.</p> <p>For the purposes of verifying the information on the beneficial owner(s), obliged entities shall also consult the central registers referred to in Article 10 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final] as well as additional information. Obligated entities shall determine the extent of the additional information to be consulted, having regard to the risks posed by the transaction or the business relationship and the beneficial owner</p>	<p>Article 18.4.b Obligated entities shall obtain the information, documents and data necessary for verification of the customer <del>and beneficial owner identity</del> through either of the following:</p> <p>(a) (...);</p> <p>(b) the use of electronic identification means and relevant trust services as set out in Regulation (EU) 910/2014, <b><i>in a reliable and trustworthy form via secure authentication processes, where appropriate, or other secure remote or electronic identification procedures regulated, recognised, approved or accepted by competent authorities, provided that the level of security designated is at least 'high' or equivalent.</i></b></p> <p><b><i>(ba) where applicable, the submission of proof of registration in the central register referred to in Article 10 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final] for customers who are legal entities incorporated outside the Union, in accordance with Article 48 of this Regulation.</i></b></p> <p><b><i>Where a customer is a legal entity or a trustee or person in equivalent position acting on behalf of the legal arrangement, obliged entities shall take appropriate measures to verify the identity of the beneficial owner(s) of a legal entity or legal arrangement, including, where this is possible, on the basis of identity documents or by means of electronic identification, so that they are satisfied that they know who the beneficial owner is and that they understand the ownership and control structure of the legal entity or legal arrangement.</i></b></p> <p>For the purposes of verifying the information on the beneficial owner(s), obliged entities shall also consult <b>(531, 532)</b> the central registers referred to in Article 10 of Directive [please insert reference – proposal for 6<sup>th</sup> Anti-Money Laundering Directive - COM/2021/423 final], <b><i>irrespective of the Member State of the central register in which the beneficial ownership information is held (533).</i></b></p>	<p>Article 18.4.b Obligated entities shall obtain the information, documents and data necessary for the verification of the identity of the customer, the party to the intermediated transaction and any person purporting to act on behalf of either of them through either of the following means:</p> <p>(a) (...);</p> <p>(b) the use of electronic identification means <del>and relevant trust services as</del> <b>which meet the requirements</b> set out in Regulation (EU) 910/2014 <b>with regard to the assurance levels 'substantial' or 'high' and relevant qualified trust services as set out in Regulation (EU) 910/2014.</b></p> <p><del>For the purposes of verifying the information on the beneficial owner(s), obliged entities shall also consult the central registers referred to in Article 10 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive – COM/2021/423 final] as well as additional information. Obligated entities shall determine the extent of the additional information to be consulted, having regard to the risks posed by the transaction or the business relationship and the beneficial owner.</del></p>

	<p><i>Where appropriate, and on a risk sensitive basis (534, 535), obliged entities shall also <del>as well as</del> consult additional information from the customer or from reliable and independent sources, in particular where the information in central registers does not match the information available to them under Article 18, where they have doubts as to the accuracy of the information or where there is a higher risk of money laundering or terrorist financing.</i></p> <p>Obliged entities shall determine the extent of the additional information to be consulted <i>on a risk basis</i>, having regard to the risks posed by the transaction or the business relationship and the beneficial owner, <i>or the unusual or complex nature of the ownership structures given the nature of the company's business.</i></p> <p><i>Obliged entities shall report to the entity in charge of the central registers any discrepancies they find between the beneficial ownership information available therein and the beneficial ownership information available to them pursuant to this Article. National law pertaining to banking secrecy and confidentiality shall not hinder compliance with <del>that</del> the obligation set out in this subparagraph. (60)</i></p>	
Justification		
<p>EFA recommends adopting the Parliament text.</p> <p>The implementation of the eIDAS Regulation has been fragmented and remote identity verification as well as authentication services are not, to date, individually considered qualified trust services. This is why it is vital to include a reference to remote identity verification and authentication services within Article 18, separate from the reference to qualified trust services. As it stands, the Council's general approach would be unworkable for remote identity verification and authentication service providers that are not part of a qualified trust service. Such an approach would freeze innovation in the trust services sector, as it is through this clause that new technologies, not yet included in the scope of eIDAS, can be certified and used for the purposes of eKYC.</p> <p>To keep such services within scope, the text should also indicate (as it is in the Parliament text) "processes regulated, recognised, approved or accepted by a Member State's relevant national authorities for this purpose shall also be considered regulated, recognised, approved or accepted in all other Members States."</p>		

### 3. Preserving the risk-based approach in setting deadlines for customer identity verification

Commission Text	EP Text	Council Text
<p><b>Article 27(1)</b>            (a) verify the identity of the customer and the beneficial owner after the establishment of the business relationship, provided that the specific lower risk</p>	<p><b>Article 27(1)</b>            (a) verify the identity of the customer and the beneficial owner after the establishment of the business relationship, provided that the specific lower risk identified, <b>in the business-wide risk assessment and the customer risk assessment</b>, justified such postponement but in any case no later than <del>[30 60]</del> days of the relationship being established.</p>	<p><b>Article 27(1)</b>            (a) verify the identity of the customer and the beneficial owner after the establishment of the business relationship, provided that the specific lower risk identified justified such postponement, but in any case no later than <b>3 months or the period set out in regulatory technical standards under Article 22(1), point (c) or what is</b></p>

<p>identified justified such postponement, but in any case no later than 30 days of the relationship being established</p>		<p><b>appropriate with regards to a risk-based approach, whatever is shorter</b>, of the relationship being established;</p>
<p>Justification</p>		
<p>EFA recommends adopting the Council text.  The Council wording introduces the necessary risk-based approach to these provisions by allowing obliged entities to verify a customer’s identity within three months, the period set out in RTS, or what is appropriate per the risk-based approach. Also, we believe that the new Art 27.1.(b) regarding the use of sources of information to verify the identification data of natural or legal persons, with a proportionately lower degree of reliability and independence is also very helpful to ensure we get the right data while at the same time reducing friction during customer onboarding.  The Parliament text’s single 60-day deadline applicable for all the transactions would undermine the Risk-based Approach (RBA) by treating all relationships and transactions in an equivalent manner without considering the risk exposure of the entities and their users.  Fighting financial crime is an ongoing and iterative process that is best managed through regular reassessment of customer risk. We do this by continuously assessing our customers’ risk through dynamic models under which a user’s risk profile is constantly assessed through a number of non-suspicious factors and a full due diligence assessment is triggered the moment the user’s risk profile changes. Introducing a single deadline for verification undermines this dynamic approach. Though all three texts do so, the Council text is most flexible.</p>		

**4. Ensuring harmonization and consistency when requiring enhanced due diligence to obliged entities**

Commission Text	EP Text	Council Text
<p><b>Article 28(5)</b>  With the exception of the cases covered by Section 2 of this Chapter, where Member States identify pursuant to Article 8 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final] cases of higher risk, they may require obliged entities to apply enhanced due diligence measures and, where appropriate, specify those measures. Member States shall notify to the Commission and AMLA the enhanced due diligence requirements imposed upon obliged entities established in their territory within one month</p>	<p><b>Article 28(5)</b>  With the exception of the cases covered by Section 2 of this Chapter, where Member States identify pursuant to Article 8 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final] cases of higher risk, they may require obliged entities to apply enhanced due diligence measures and, where appropriate, specify those measures. Member States shall notify to the Commission and AMLA the enhanced due diligence requirements imposed upon obliged entities established in their territory within one month of their adoption, accompanied by a justification of the money laundering and terrorist financing risks underpinning such decision.   Where the risks identified by the Member States pursuant to the first subparagraph are likely to affect the financial system of the Union, AMLA shall, upon a request from the Commission or on its own initiative, consider updating the guidelines adopted pursuant to Article 26 or, <b><i>if deemed more appropriate, issue draft regulatory technical standards to impose</i></b> enhanced due diligence requirements upon obliged</p>	<p><b>Article 28(5)</b>  With the exception of the cases covered by Section 2 of this Chapter, where Member States identify higher risks pursuant to Article 8 of Directive [please insert reference – proposal for 6th Anti-Money Laundering Directive - COM/2021/423 final] or in the course of any relevant sector- specific risk assessment carried out by the Member States, they may require obliged entities to apply enhanced due diligence measures and, where appropriate, specify those measures. Member States shall notify to the Commission and AMLA the enhanced due diligence requirements imposed upon obliged entities established in their territory within one month of their adoption, accompanied by a justification of the money laundering and terrorist financing risks underpinning such decision.   Where the risks identified by the Member States pursuant to the first subparagraph are likely to affect the financial system of the Union, AMLA shall, upon a request from the Commission or of its own initiative, consider updating the guidelines adopted pursuant to Article 26.</p>

<p>of their adoption, accompanied by a justification of the money laundering and terrorist financing risks underpinning such decision.</p>	<p>entities <i>uniformly in the EU and submit them to the Commission for adoption.</i></p> <p><i>5a. The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 3 of this Article in accordance with Articles 38 to 41 of Regulation [please insert reference – proposal for establishment of an Anti-Money Laundering Authority - COM/2021/421 final].</i></p>	
<b>Justification</b>		
<p>EFA supports the Parliament text as believes that draft regulatory technical standards to impose enhanced due diligence requirements upon obliged entities will allow harmonization and would prevent “gold-plating”. Harmonization would not only create consistency on enhanced due diligence requirements, will also allow compliance simplification and make it less costly.</p> <p>EFA supports the Parliament text as it is most consistent with the objective of European regulatory harmonisation. However, all three texts leave room for “gold-plating,” which would be clearly contrary to the spirit of the AML policy reform package, allowing for regulatory divergence which could make compliance more complex and costly, ultimately to the detriment of European consumers of financial services.</p>		

### 5. Enabling reliance on other obliged entities to meet the customer due diligence requirements

<b>Commission Text</b>	<b>EP Text</b>	<b>Council Text</b>
<p><b>Article 38(1) – introductory part</b> 1. Obligated entities may rely on other obliged entities, whether situated in a Member State or in a third country, to meet the customer due diligence requirements laid down in Article 16(1), points (a), (b) and (c), provided that:</p>	<p><b>Article 38(1) – introductory part</b> Obligated entities may rely on other obliged entities, whether situated in a Member State or in a third country, to meet the customer due diligence requirements laid down in Article 16(1), points (a), (b), (c) and (d), <i>and Article 21 (2) and (3)</i>, provided that:</p>	<p><b>Article 38(1) – introductory part</b> Obligated entities may rely on other obliged entities, whether situated in a Member State or in a third country, to meet the customer due diligence requirements laid down in Article 16(1), points (a), (b) and (c), provided that</p>
<b>Justification</b>		
<p>Obligated entities should be able to work together to meet ongoing business relationship and transaction monitoring requirements. Furthermore, obliged entities should be able to work together to meet their obligations to determine whether their customers (or their customers’ beneficial owners) are politically exposed persons (PEPs).</p> <p>The Commission Text follows the AML Directive with regard to the scope of what is possible to rely on other obliged entities. The EP text extends the scope, allowing reliance also for “ongoing monitoring” (16 (1) d) and with respect to updating customer data (art. 21, (2) and (3)). The Council Text favours the maintenance of the current status.</p> <p>EFA supports the Parliament text as it allows obliged entities to leverage work being carried out by other obliged entities even further, where they are comfortable doing so, which is the principle behind the “reliance” concept (i.e., avoiding duplicative work when possible). EFA also believes that the scope of reliance could be further extended to include politically exposed persons (PEP) and sanctions screening (art. 32, and art. 16 (1) c a - as proposed by the EP).</p>		

## 6. Allowing obliged entities to outsource CDD to non-EU entities

Commission Text	EP Text	Council Text
<p><b>Article 40(1) – introductory part</b></p> <p>Obligated entities may outsource tasks deriving from requirements under this Regulation for the purpose of performing customer due diligence to an agent or external service provider, whether a natural or legal person, with the exception of natural or legal persons residing or established in third countries identified pursuant to Section 2 of this Chapter.</p>	<p><b>Article 40(1)</b></p> <p>Obligated entities may outsource tasks deriving from requirements under this Regulation for the purpose of performing customer due diligence to an agent or external service provider. <b>These tasks can be outsourced to, whether</b> a natural or legal person, with the exception of natural or legal persons residing or established in third countries identified pursuant to Section 2 of this Chapter. (713, 715)</p>	<p><b>Article 6(a)</b></p> <p>Obligated entities may outsource tasks deriving from requirements under this Regulation <del>for the purpose of performing customer due diligence to an agent or a service provider</del>, whether a natural or legal person, with the exception of natural or legal persons residing or established in third countries identified pursuant to Section 2 of this Chapter. <b>The obliged entity shall notify to the supervisor the outsourcing before the service provider starts the activities for the obliged entity.</b></p> <p>The obliged entity shall remain fully liable for any action, whether an act of commission or omission, connected to the outsourced tasks that are carried out by the service provider, and also remains responsible as controller pursuant Article 4, point (7) of Regulation (EU) 2016/679 for any personal data processed for the purpose of the outsourced tasks.</p> <p>Whenever tasks are outsourced, the obliged entity shall in all cases ensure that it understands the rationale behind the activities carried out by the service provider and the approach followed in their implementation, and that it is able to demonstrate to supervisors that these activities mitigate the specific risks that the obliged entity is exposed to.</p>
<b>Justification</b>		
<p>EFA welcomes the Parliament and Council texts. Obligated entities should not be prohibited from outsourcing CDD tasks to AML compliance entities established outside of the EU. EFA believes that there is value in a regime which allows for specialisation in the conduct of CDD; this can both increase the effectiveness, and decrease the cost of controls aimed at countering criminal exploitation of Europe’s economy.</p>		

## 7. Proportionate requirements to Intra-group outsourcing

Commission Text	EP Text	Council Text
<p><b>Recital 62</b></p> <p>Obligated entities may outsource tasks relating to the performance of customer due diligence to an agent or external service provider, unless they are established in third countries that are designated as high-risk, as having compliance weaknesses or as posing a threat to the Union’s financial system. In the case of agency or outsourcing relationships on a contractual basis between obliged entities and external service providers not covered by AML/CFT requirements, any AML/CFT obligations upon those agents or outsourcing service providers could arise only from the contract between the parties and not from this Regulation. Therefore, the responsibility for complying with AML/CFT requirements should remain entirely with the obliged entity itself. The obliged entity should in particular ensure that, where an outsourced service provider is involved for the purposes of remote customer identification, the risk-based approach is respected.</p>	<p><b>Recital 62</b></p> <p>Obligated entities may outsource tasks relating to the performance of customer due diligence to an agent or external service provider <i>that fully comply with GDPR, such as an AML compliance entity</i>, unless they are established in third countries that are designated as high-risk, as having compliance weaknesses or as posing a threat to the Union’s financial system. <i>These outsourcing activities should support obliged entities, to obtain complete, timely and accurate information by using decision-making tools, such as global news, business, regulatory and legal databases.</i> In the case of agency or outsourcing relationships on a contractual basis between obliged entities and external service providers not covered by AML/CFT requirements, any AML/CFT obligations upon those agents or outsourcing service providers could arise only from the contract between the parties and not from this Regulation. Therefore, the responsibility for complying with AML/CFT requirements should remain entirely with the obliged entity itself. The obliged entity should in particular ensure that, where an outsourced service provider is involved for the purposes of remote customer identification, the risk-based approach is respected. <i>The outsourcing of tasks deriving from requirements under this Regulation for the purpose of performing customer due diligence to an agent or external service provider should not exempt the obliged entity from any obligation under Regulation (EU) 2016/679, including Article 28 thereof.</i></p>	<p><b>Recital 62</b></p> <p>Obligated entities may outsource tasks to a service provider, including an agent, distributor and another group member, unless they are established in third countries that are designated as high-risk, as having compliance weaknesses or as posing a threat to the Union’s financial system. In the case of agency or outsourcing relationships on a contractual basis between obliged entities and service providers not covered by AML/CFT requirements, any AML/CFT obligations upon those service providers could arise only from the contract between the parties and not from this Regulation. Therefore, the responsibility for complying with AML/CFT requirements should remain entirely with the obliged entity itself. The obliged entity should in particular ensure that, where an outsourced service provider is involved for the purposes of remote customer identification, the risk-based approach is respected. <i>Intra-group outsourcing should be subject to the same regulatory framework as outsourcing to service providers outside the group.</i></p>



<b>Justification</b>
Intra-group outsourcing is less risky than other outsourcing and should therefore not be subject to the same level of scrutiny. A fellow group company will typically have a closer working relationship with a given obliged entity, and a much deeper understanding of its business and the potential risks it carries, than a third-party firm specialising in AML compliance services.

#### 8. Promoting regulatory clarity and ensuring obliged entities are able to outsource certain controls

<b>Commission Text</b>	<b>EP Text</b>	<b>Council Text</b>
<b>Article 40(2)(b)</b> (b) the internal controls in place pursuant to Article 7;	<b>Article 40(2)(b)</b> (b) the internal controls in place pursuant to Article 7;	<b>Article 40(2)</b>  Deleted  <b>Article 6(a) 2</b> (b) the approval of the obliged entity's policies, controls and procedures pursuant to Article 8;
<b>Justification</b>		
Obliged entities should be able to outsource to specialists the preparation and implementation of the internal controls required by Article 7. The expertise brought by those entities would help obliged entities to increase the effectiveness and efficiency of the processes while decreasing due diligence and compliance costs.		

#### 9. Enabling obliged entities to outsource the drawing up of policies, controls and procedures

<b>Commission Text</b>	<b>EP Text</b>	<b>Council Text</b>
<b>Article 40(2)(c)</b> (c) the drawing up and approval of the obliged entity's policies, controls and procedures to comply with the requirements of this Regulation;	<b>Article 40(2)</b> (c) the <del>drawing up</del> and approval of the obliged entity's policies, controls and procedures to comply with the requirements of this Regulation;	<b>Article 40(2)</b>  Deleted
<b>Justification</b>		
Obliged entities should be able to outsource the drawing up and approval of policies, controls and procedures to comply with the requirements of the AMLR. The expertise brought by those entities would help obliged entities to increase the effectiveness and efficiency of the processes while decreasing due diligence and compliance costs.		

#### 10. Enabling obliged entities to outsource the attribution of risk profiles

Commission Text	EP Text	Council Text
<b>Article 40(2)(d)</b> (d) the attribution of a risk profile to a prospective client and the entering into a business relationship with that client;	<b>Article 40(2)(d)</b> (d) <del>the attribution of a risk profile to a prospective client and the entering</del> <i>decision to enter</i> into a business relationship with that a client <i>based on the attribution of a risk profile</i> ;	<b>Article 40(2)(d)</b> Deleted
<b>Justification</b>		
Obligated entities should be able to outsource the attribution of risk profiles to prospective clients. The expertise brought by those entities would help obliged entities to increase the effectiveness and efficiency of the processes while decreasing due diligence and compliance costs.		

#### 11. Enabling obliged entities to outsource the identification of criteria for detection of suspicious or unusual transactions or activities

Commission Text	EP Text	Council Text
<b>Article 40(2)(e)</b> (e) the identification of criteria for the detection of suspicious or unusual transactions and activities;	<b>Article 40(2)(e)</b> (e) the <del>identification</del> <i>approval</i> of criteria for the detection of suspicious or unusual transactions and activities;	<b>Article 40(2)(e)</b> Deleted
<b>Justification</b>		
Obligated entities should be able to outsource the identification of criteria for the detection of suspicious or unusual transactions and activities. The expertise brought by those entities would help obliged entities to increase the effectiveness and efficiency of the processes while decreasing due diligence and compliance costs.		

#### 12. Enabling external CDD providers to report suspicious activity directly to FIUs on behalf of obliged entities

Commission Text	EP Text	Council Text
<b>Article 40(2)(f)</b> (f) the reporting of suspicious activities or threshold-based declarations to the FIU pursuant to Article 50.	(f) the reporting of suspicious activities or threshold-based declarations to the FIU pursuant to Article 50, <i>unless such activities are outsourced to a service provider belonging to the same group as the obliged entity and which is established in the same Member State as the obliged entity</i> .	<b>Article 40(2)</b> Deleted  <b>Article 6(a)</b> <b>2.c.</b> The reporting of suspicious activities or threshold-based declarations to the FIU pursuant to Article 50, unless such activities are outsourced to a service provider belonging to

		the same group as the obliged entity and which is established in the same Member State as the obliged entity or consent is granted by national competent authority to allow obliged entities participating in a partnership for information sharing in the AML/CFT field to outsource the reporting of suspicious activities within the partnership.
<b>Justification</b>		
Obligated entities should be able to outsource the reporting of suspicious activities or threshold-based declarations to the FIU pursuant to Article 50. Where specialists are responsible for identifying these events, they are best placed to inform authorities.		

### 13. Addition of new provisions at the end of Article 40 – sub-outsourcing, AMLA guidance, and intra-group “outsourcing”

Commission Text	EP Text	Council Text
Article 40 – paragraph (4)(a) – new N/A	Article 40 – paragraph (4)(a) – new N/A	<p><b>Article 40</b></p> <p><b>5. By [3 years after the entry into force of this Regulation], AMLA shall issue guidelines addressed to obliged entities on:</b></p> <p><b>(a) the establishment of outsourcing relationships, including the subsequent outsourcing relationship, in accordance with this article, their governance and procedures for monitoring the implementation of functions by the service provider;</b></p> <p><b>(b) the roles and responsibility of the obliged entity and the service provider within an outsourcing agreement;</b></p> <p><b>(c) supervisory approaches to outsourcing.</b></p>
<b>Justification</b>		
With appropriate, transparent regulatory guardrails in place, and following the same logic of specialisation for first-order outsourcing, sub-outsourcing should be permitted under the AMLR. AMLA guidance on outsourcing and sub-outsourcing is important for ensuring regulatory harmonisation. EFA supports the Council text.		

### 14. Broadening conditions under which obliged entities may disclose certain AML/CFT activities in order to facilitate AML/CFT efforts and compliance

Commission Text	EP Text	Council Text
Article 54(5)	Article 54(5)	Article 54(5)

<p>For obliged entities referred to in Article 3, points (1), (2), (3)(a) and (b), in cases relating to the same customer and the same transaction involving two or more obliged entities, and by way of derogation from paragraph 1, disclosure may take place between the relevant obliged entities provided that they are located in the Union, or with entities in a third country which imposes requirements equivalent to those laid down in this Regulation, and that they are from the same category of obliged entities and are subject to professional secrecy and personal data protection requirements..</p>	<p>For obliged entities referred to in Article 3, points (1), (2), (3)(a) and (b), in cases relating to the same customer and the same transaction involving two or more obliged entities, and by way of derogation from paragraph 1, disclosure may take place between the relevant obliged entities provided that they are located in the Union, or with entities in a third country which imposes requirements equivalent to those laid down in this Regulation, and that they are from the same category of obliged entities and are subject to professional secrecy and personal data protection requirements, <i>in line with the Union acquis on data protection [comparable to those laid down in Regulation (EU) 2016/679]</i>.</p>	<p>For obliged entities referred to in Article 3, points (1), (2), (3)(a) and (b), in cases relating to the same customer and the same transaction involving two or more obliged entities, and by way of derogation from paragraph 1, disclosure may take place between the relevant obliged entities provided that they are located in the Union, or with entities in a third country which imposes requirements equivalent to those laid down in this Regulation, and that they are subject to professional secrecy and personal data protection requirements.</p>
<b>Justification</b>		
<p>Where there is an overlap between the subjects of obliged entities' compliance assessments, they should be able to cooperate and disclose information to one another in order to combat financial crime. This would ideally be allowed whether the nexus is the transaction <i>or</i> the customer, but the Council remains the strongest.</p>		

**15. Explicitly permitting the processing of personal data by means of automated decision-making, and the exchange of information in efforts to counter ML/TF**

Commission Text	EP Text	Council Text
<p><b>Additional sections at the end of Article 55</b> N/A</p>	<p><b>Additional sections at the end of Article 55</b> N/A</p>	<p><b>Article 55(6)</b> Without prejudice to further obligations under Regulation (EU) 2016/679 and Regulation [please insert reference □ EU-AI-Reg; COM(2021) 206 final], the processing of personal data according to paragraph 4 may be conducted by means of automated decision-making, including profiling within the meaning of Article 4, point (4) of Regulation (EU) 2016/679, or artificial- intelligence systems as defined in Article [please insert reference -- Article 3 of Regulation EU-AI- Reg; COM(2021) 206 final], provided that the processing of personal data only comprises data which an obliged entity has collected in the course of performing its customer due diligence obligations under Chapter III, including, in particular, the ongoing monitoring pursuant to Article 20.</p>
<b>Justification</b>		
<p>EFA supports the Council text as believes that obliged entities and AML compliance entities, fellow group companies, or “joint utilities” operating on their behalf, should be allowed to leverage automated decision-making tools to process personal data, where the appropriate safeguards and compliance regimes are in place. This will help facilitate the efficacy and cost-effectiveness of AML/CFT efforts.</p>		