Electronic Money Association
68 Square Marie-Louise
Brussels 1000
Belgium
Telephone: +32 2 320 3156
www.e-ma.org

European Commission
(Submission via online form)

18 July 2025

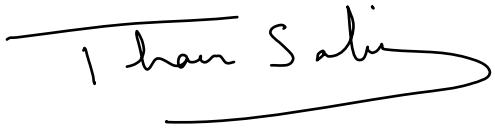
Dear European Commission

Re: EMA response to European Commission consultation on high-risk AI systems

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our comments and proposals.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response

Do you have or know practical examples of AI systems that could fall under the exception mentioned in Point 5 of Annex III to the AI Act and recital 58 AI Act?

If you have or know practical examples of AI systems related to essential private services and essential public services and benefits where you need further clarification regarding the distinction from prohibited AI systems, in particular Art. 5(1)(c) AI Act, please specify.

We would welcome further clarification around the boundary between those systems prohibited under Article 5(1)(c) and high-risk systems, particularly in the context of behavioural analytics or identity verification systems. Many firms use AI tools to detect behavioural anomalies (e.g. typing patterns) for security or fraud prevention purposes, but these are not designed to exploit user vulnerabilities. However, some systems may process data from vulnerable users (e.g. elderly customers) to offer extra protections or accessibility, which raises questions about how the law defines "exploitation" versus "support."

Greater clarity is needed to ensure that well-intentioned protective measures are not mischaracterised as manipulative or harmful, especially when they are aimed at reducing financial exclusion or preventing fraud.

Recital 58 of the AI Act explicitly exempts AI systems used for detecting financial fraud and for prudential regulatory purposes from being classified as high-risk. We believe there is a strong rationale to consider AML and broader fraud compliance systems as part of this same exemption; so the Act can maintain consistency in recognising AI systems that have a legitimate risk-prevention purpose, while ensuring focus remains on AI applications that pose a direct and significant risk to individuals' fundamental rights.

Do you see the need for clarification of one of the various use cases of high-risk classification in Point 5 of Annex III to the AI Act and its interplay with other Union or national legislation, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

Yes, we see a need for clarification around the interplay between Point 5(b) of Annex III of the AI Act and existing obligations under the General Data Protection Regulation (GDPR), particularly in relation to Article 22 GDPR, which governs automated decision-making, including profiling.

Many firms use AI systems to support creditworthiness assessments (during onboarding processes). These systems are already subject to GDPR safeguards (transparency, data minimisation, the right to human review, and purpose limitation). The introduction of a parallel 'high-risk AI' classification under the AI Act may create uncertainty as to which regulation takes priority.

Guidance would also be welcome on whether GDPR-compliant systems that include safeguards such as meaningful human involvement could be considered to fall under one of the exemptions in Article 6(3) of the AI Act.

Do you have or know practical examples of AI systems that could fall under the exception mentioned in Point 5 of Annex III to the AI Act and recital 58 AI Act?

Horizontal Aspects of the High-Risk Classification

The classification of AI systems as high-risk is made depending on the intended purpose of the AI system. The intended purpose is defined by Article 3(12) AI Act as *"the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation."*

Are there aspects of the definition of the intended purpose, as outlined in Article 3(12) AI Act, that need additional clarification?

No comment.

Does the definition of intended purpose permit a provider to impose a condition of use to prohibit deployers from using its AI systems:

- as a safety related component in a wider system,
- or more generally, using its AI systems in any high-risk contexts.

What obligation or liability is there on providers of AI systems to detect such misuse?

If you have or know practical examples of AI systems that in your opinion could be relevant for the high-risk classification according to creditworthiness, please specify the concrete AI system, how it is used in practice and how all the necessary elements described above are fulfilled

No comment.

Obligations for High-Risk AI Systems and Value Chain Obligations

The AI Act sets mandatory requirements for high-risk AI systems around risk management (Article 9), data and data governance (Article 10), technical documentation (Article 11) and record-keeping (Article 12), transparency and the provision of information to deployers (Article 13), human oversight (Article 14), and robustness, accuracy and cybersecurity (Article 15).

Beyond the technical standards under preparation by the European Standardisation Organisations, are there further aspects related to the AI Act's requirements for high-risk AI systems in Articles 9-15 for which you would seek clarification, for example through guidelines?

Furthermore, are there aspects related to the requirements for high-risk AI systems in Articles 9-15 which require clarification regarding their interplay with other Union legislation?

Articles 9–15 overlap significantly with obligations under the GDPR, such as Article 5 (data principles), Article 13/14 (information obligations), and Article 22 (automated decisions). Clarification is needed when meeting GDPR requirements is enough to also satisfy the AI Act's obligations.

Obligations for providers of high-risk AI systems.

A provider of an AI system is a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge; (Article 3(1)).

Beyond ensuring that a high-risk AI system is compliant with the requirements in Articles 9-15, providers of high-risk AI systems have several other obligations as listed in Article 16 and further specified in other corresponding provisions of the AI Act. These include:

- Indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trademark, the address at which they can be contacted;
- Have a quality management system in place which complies with Article 17;
- Keep the documentation referred to in Article 18;
- When under their control, keep the logs automatically generated by their high-risk AI systems, as referred to in Article 19;
- Ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43;
- Draw up an EU declaration of conformity in accordance with Article 47;
- Affix the CE marking to the high-risk AI system, in accordance with Article 48;
- Comply with the registration obligations referred to in Article 49(1);
- Take the necessary corrective actions and provide information as required in Article 20;
- Cooperate with national competent authorities as required in Article 21;

- Ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.

Are there aspects related to the AI Act's obligations for providers of high-risk AI systems for which you would seek clarification, for example through guidelines? And are there aspects related to the obligations for providers of high-risk AI systems which require clarification regarding their interplay with other Union legislation?

No comment.

Obligations for deployers of high-risk AI systems.

A deployer is a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity; (Article 3 (4)).
Deployers of high-risk AI systems have specific responsibilities under the AI Act. Transversally, Article 26 obliges all deployers of high-risk AI systems to:

- Take appropriate technical and organisational measures to ensure that AI systems are used in accordance with the instructions accompanying the AI systems;
- Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support;
- Ensure that input data is relevant and sufficiently representative, considering the intended purpose of the high-risk AI system;
- Monitor the operation of the high-risk AI system based on the instructions for use and, where relevant, inform providers in accordance with Article 72;
- Keep the logs automatically generated by that high-risk AI system, to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system of at least six months.

Article 26 foresees the following obligations in specific cases including (Annex III creditworthiness): Deployers of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system.

Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems listed in Article 26 for which you would seek clarification, for example through guidelines?

Yes, clarification is needed on whether the obligation to retain logs applies to all systems, including low-impact ones used in risk scoring or transaction monitoring.

Clarification is also required on what constitutes adequate human oversight in practice, particularly where AI systems offer decision support rather than make fully automated decisions.

Are there aspects related to the obligations for deployers of high-risk AI systems listed in Article 26 which require clarification regarding their interplay with other Union legislation?

No comment.

Assessment impact

Annex III decisions related to creditworthiness require an assessment of the impact on fundamental rights that the use of such a system may produce. The AI Office is currently preparing a template that should facilitate compliance with this obligation.

Article 27 specifies that where any of its obligations are already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment.

Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems for the fundamental rights impact assessment for which you would seek clarification in the template?

Yes, clarification is needed on how the impact assessment is expected to interact with the existing GDPR Data Protection Impact Assessment.

And how can complementarity of the fundamental rights impact assessment and the data protection impact assessment be ensured, while avoiding overlaps?

No comment.

Deployers of high-risk AI systems may have to provide an explanation to an affected person upon their request. This right is granted by Article 86 AI Act to affected persons which are subject to a decision, which is taken on the basis of the output from a high-risk AI system listed in Annex III and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights.

Are there aspects related to the AI Act's right to request an explanation in Article 86 for which you would seek clarification, for example through guidelines?

Yes, clarification is needed on what constitutes a sufficient explanation to an affected person.

Substantial modification

Article 3 (23) defines a substantial modification as a change to an AI system after placing it on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider. As a result of such a change, the compliance of the AI system with the requirements for high-risk AI systems is either affected or results in a modification to the intended purpose for which the AI system has been assessed.

The concept of 'substantial modification' is central to the understanding of the requirement for the system to undergo a new conformity assessment. Pursuant to Article 43(4), the high-risk AI system

should be considered a new AI system which should undergo a new conformity assessment in the event of a substantial modification.

This concept is also central for the understanding of the scope of obligations between a provider of a high-risk AI system and other actors operating in the value chain (distributor, importer or deployer of a high-risk AI system). Pursuant to Article 25, any distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system and shall be subject to the obligations of the provider, in any of the following circumstances:

(a), they put their name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated;

(b), they make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in such a way that it remains a high-risk AI system;

(c), they modify the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system.

Do you have any feedback on issues that need clarification as well as practical examples on the application of the concept of 'substantial modification' to a high-risk AI system.

Yes, we would welcome clear examples which distinguish between permitted adaptations and substantial modifications to provide greater clarity. Clarity is needed about the threshold at which modifications trigger reclassification as a provider and require a full conformity reassessment.

Article 43(4) describes the circumstances under which the change does not qualify as a substantial modification: 'For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.'

Do you have any feedback on issues that need clarification as well as practical example of pre-determined changes which should not be considered as a substantial modification within the meaning the Article 43(4) of the AI Act.

No comment.

Value chain roles and obligations

Throughout the AI value chain, multiple parties contribute to the development of AI systems by supplying tools, services, components, or processes. These parties play a crucial role in ensuring the provider of the high-risk AI system can comply with regulatory obligations. To facilitate compliance with regulatory obligations, Article 25(4) require these parties to provide the high-risk AI system provider with necessary information, capabilities, technical access and other assistance through written agreements, enabling them to fully meet the requirements outlined in the AI Act.

However, third parties making tools, services, or AI components available under free and open-source licenses are exempt from complying with value chain obligations. Instead, providers of free and open-source AI solutions are encouraged to adopt widely accepted documentation practices, such as model cards and datasheets, to facilitate information sharing and promote trustworthy AI. To support cooperation along the value chain, the Commission may develop and recommend voluntary model contractual terms between providers of high-risk AI systems and third-party suppliers.

From your organisation's perspective, can you describe the current distribution of roles in the AI value chain, including the relationships between providers, suppliers, developers, and other stakeholders that your organisation interacts with?

The EMA Membership spans a range of business models from Payment Service Providers, Cryptoasset Service Providers and e-wallet providers. The AI value chain is therefore often varied and multi-layered. Providers of high-risk AI systems frequently rely on third parties for machine learning models, APIs, data infrastructure, and other critical components; many of which are developed externally and integrated or adapted in-house.

Do you have any feedback on potential dependencies and relationships throughout the AI value chain that should be taken into consideration when implementing the AI Act's obligations, including any upstream or downstream dependencies between providers, suppliers, developers, and other stakeholders, which might impact the allocation of obligations and responsibilities between various actors under the AI Act? In particular, indicate how these dependencies affect SMEs, including start-ups.

We welcome the recognition in Article 25(4) that parties along the value chain must support compliance through contractual arrangements. In practice, this is often challenging where smaller firms rely on third-party tools or services that are not easily modifiable, or where open-source software is involved. The exemption for open-source providers may create a gap in accountability, especially where those components play a meaningful role in high-risk system outputs.

There is a power imbalance risk for smaller firms, who may lack the bargaining power to negotiate tailored contractual terms. Clear guidance or Commission approved contractual clauses as mentioned in the AI Act would be especially valuable for smaller market participants.

What information, capabilities, technical access and other assistance do you think are necessary for providers of high-risk AI systems to comply with the obligations under the AI Act, and how should these be further specified through written agreements?

In terms of written agreements, members would benefit from a standard structure that outlines the nature of support expected from third parties (e.g. technical access, documentation, or audit logs) depending on the role of the component.

Please specify the challenges in the application of the value chain obligations in your organisation for compliance with the AI Act's obligations for high-risk AI systems and the issues for which you need further clarification; please provide practical examples.

Many firms use third-party AI tools as part of their systems, often supplied by large technology providers who are unwilling to share the full technical documentation or transparency reports needed for downstream compliance. This creates operational uncertainty for providers who remain ultimately responsible under the AI Act.

Possible amendments of high-risk use cases in Annex III and of prohibited practices in Article 5

Pursuant to Article 112(1) AI Act, the Commission shall assess the need to amend the list of use cases set out in Annex III and of the list of prohibited AI practices laid down in Article 5 by 2 August 2025 and once a year from then onwards.

The Commission is empowered to adopt delegated acts to amend Annex III by adding or modifying use-cases of high-risk AI systems pursuant to Article 7(1) AI Act. The findings of the assessment carried out under Article 112(1) AI Act are relevant in this context. The empowerment to amend Annex III requires that both of the following conditions are fulfilled:

- the AI systems are intended to be used in any of the areas listed in Annex III (thus including creditworthiness) and
- the AI systems pose a risk of harm to health and safety, or an adverse impact on fundamental rights, and that risk is equivalent to, or greater than, the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

Article 7(2) AI Act further specifies the criteria that the Commission shall take into account in order to evaluate the latter condition, including:

(a) the intended purpose of the AI system;

(b) the extent to which an AI system has been used or is likely to be used;

(c) the nature and amount of the data processed and used by the AI system, in particular whether special categories of personal data are processed;

(d) the extent to which the AI system acts autonomously and the possibility for a human to override a decision or recommendations that may lead to potential harm;

(e) the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect multiple persons or to disproportionately affect a particular group of persons;

(f) the extent to which the use of an AI system has already caused harm to health and safety, has had an adverse impact on fundamental rights or has given rise to significant concerns in relation to the likelihood of such harm or adverse impact, as demonstrated, for example, by reports or documented allegations submitted to national competent authorities or by other reports, as appropriate;

(g) the extent to which persons who are potentially harmed or suffer an adverse impact are dependent on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;

(h) the extent to which there is an imbalance of power, or the persons who are potentially harmed or suffer an adverse impact are in a vulnerable position in relation to the deployer of an AI system, in particular due to status, authority, knowledge, economic or social circumstances, or age;

(i) the extent to which the outcome produced involving an AI system is easily corrigible or reversible, taking into account the technical solutions available to correct or reverse it, whereby outcomes having an adverse impact on health, safety or fundamental rights, shall not be considered to be easily corrigible or reversible;

(j) the magnitude and likelihood of benefit of the deployment of the AI system for individuals, groups, or society at large, including possible improvements in product safety;

(k) the extent to which existing Union law provides for:

- effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;

- effective measures to prevent or substantially minimise those risks.

Do you have or know concrete examples of AI systems that in your opinion need to be added to the list of use cases in Annex III, among the existing 8 areas, in the light of the criteria and the conditions in Article 7(1) and (2) and should be integrated into the assessment pursuant to Article 112(1) AI Act?

We encourage the Commission, in applying Article 7(1) and (2), to maintain a clear boundary between AI systems used for risk scoring related to credit access (which are already in scope) and those used solely for anti-fraud or compliance monitoring.

Those used solely for anti-fraud or compliance monitoring should not be considered high risk AI systems.

Do you consider that some of the use cases listed in Annex III require adaptation in order to fulfil the conditions laid down pursuant to Article 7(3) AI Act and should therefore be amended and should be integrated into the assessment pursuant to Article 112(1) AI Act?

No comment.

Do you consider that some of the use cases listed in Annex III no longer fulfil the conditions laid down pursuant to Article 7(3) AI Act and should therefore be removed from the list of use cases in Annex III and should be integrated into the assessment pursuant to Article 112(1) AI Act?

No comment.

Pursuant to Article 112(1) AI Act, the European Commission shall assess the need for amendment of the list of prohibited AI practices laid down in Article 5 once a year. In order to gather evidence of potential needs for amendments, respondents are invited to answer the following questions.

Do you have or know concrete examples of AI practices that in your opinion contradict Union values of respect for human dignity, freedom, equality and no discrimination, democracy and the rule of law and fundamental rights enshrined in the Charter and for which there is a regulatory gap because they are not addressed by other Union legislation?

No comment.

Do you consider that some of the prohibitions listed in Article 5 AI Act are already sufficiently addressed by other Union legislation and should therefore be removed from the list of prohibited practices in Article 5 AI Act?

No comment.

Members of the EMA, as of January 2024

AAVE LIMITED
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
Amazon
American Express
ArcaPay UAB
Banked
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
CashFlows
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crypto.com
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
eToro Money
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
Flex-e-card
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
HUBUC
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
J. P. Morgan Mobility Payments Solutions S. A.
Modulr Finance B.V.
MONAVATE
MONETLEY LTD
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Payments Ltd
Nuvei Financial Services Ltd
OFX
OKG Payment Services Ltd
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Park Card Services Limited
Paymentsense Limited
Paynt
Payoneer Europe Limited
PayPal Europe Ltd
Paysafe Group
Paysend EU DAC
Plaid
PPRO Financial Ltd
PPS
Ramp Swaps Ltd
Remitly
Revolut
Ripple
Securiclick Limited
Segpay
Skrill Limited
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Swile Payment
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
VallettaPay
Vitesse PSP Ltd
Viva Payments SA
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst
Worldpay
Yapily Ltd