Ecommerce Europe's comments to the ongoing negotiations on the Artificial Intelligence Act

Ecommerce Europe and its members are always invested in enhancing the competitiveness of European businesses by adapting to new innovative solutions and technologies that can ensure a greater customer experience and increase economic growth. In relation to this, Ecommerce Europe strongly believes that artificial intelligence is and will even increase to be instrumental for the development of the digital commerce sector. E-commerce companies understand the increased use and uptake of artificial intelligence solutions as opportunities that can improve the day-to-day running of businesses in a manner that benefits not only the businesses themselves, but also consumers and society as a whole. Currently, online retailers primarily are *users* of AI systems in their everyday business models, using such systems to tailor their services to the needs of customers, while also improving internal efficiency. Simultaneously, actors within the digital commerce sector are increasingly starting to innovate and develop their own technical solutions within the field of artificial intelligence. Such AI solutions applied or developed by retailers generally carry no or very low risks to individuals – an aspect also recognised by the European Commission in its AI White Paper.

Key Recommendations

With trilogue negotiations approaching, Ecommerce Europe calls on the EU policymakers to ensure that the upcoming AI Act:

1. **Adopts the new definition of AI systems to ensure greater legal certainty for businesses using and developing AI systems.**
2. **Provides greater clarification of aspects related to prohibited AI practices.**
3. **Incorporates a limited and more defined scope of high-risk AI systems.**
4. **Lays down regulatory requirements for general-purpose AI that are fair and feasible.**

Improved definition of AI systems

The increased uptake and use of AI solutions is crucial to businesses. When regulating AI, it is therefore of key importance that policymakers pursue a targeted approach and avoid the risk of unintentionally regulating many traditional technologies, also beyond AI, as this could create excessive burdens and barriers to growth and innovation. Ecommerce Europe has previously called out the definition of AI, as laid down in the European Commission's legislative proposal on the AI Act, for being too broad in scope due to the inclusion of widely used standard software applications, such as statistical approaches, Bayesian estimation, search and optimisation models etc., thereby going beyond what is commonly considered to be AI systems. **Therefore, Ecommerce Europe welcomes the suggested modifications introduced by the European Parliament co-Rapporteurs, which defines AI systems as "[…] a machine-based**

system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments." Ecommerce Europe believes that adopting the abovementioned definition of AI into the AI Act legislative framework will narrow down the scope of the regulation and thus provide the necessary legal certainty for businesses using and developing AI systems.

Clarification of scope of prohibited AI practices

While Ecommerce Europe naturally supports the inclusion of provisions on prohibited AI practices to avoid the application of AI systems that are incompatible with Union values, such as fundamental rights, we urge **European policymakers to ensure greater legal clarification of the scope of prohibited AI systems, as defined under Article 5 of the AI Act.** More specifically, Ecommerce Europe reiterates its call for clarification of the legally non-defined term of "subliminal techniques (beyond a person's consciousness, ed.)" to not be interpreted as prohibition of the use and development of marketing, personalisation, and search recommendations AI systems. These are all commonly used techniques within the digital commerce sector, and since these are not found to cause any material, physical or psychological harm, we strongly suggest that it should be clearly stated in the legislative text that such techniques are excluded from the scope of the Regulation to avoid legal ambiguity.

A limited and more defined scope of high-risk AI systems

Furthermore, Ecommerce Europe calls on the European policymakers to be mindful when classifying the AI systems falling under the high-risk category, to ensure legal certainty. We have previously requested policymakers to address the potential issue of AI systems being inadvertently classified as high risk, with the appertaining burdensome obligations that such classification will entail, since the originally proposed text on the matter appeared to capture all AI systems used within certain high-risk products or industries, independently of how that AI system would be used in a particular context and whether said use would create a material risk of harm. Based on this perception, Ecommerce Europe therefore suggested that in order for an AI system to be classified as high risk, it should make final decisions creating a material adverse risk to an individual's fundamental rights, health or safety. As such, **we are pleased to see that the involved European Parliament Rapporteurs have addressed this issue, and we thus support the changes introduced in relation to Article 6(2) and the new Article 6(3):**

> Art. 6(2): "[…] The Commission shall, 6 months prior to the entry into force of this Regulation, following consultation with the AI Office and relevant stakeholders, provide guidelines clearly specifying the circumstances where the output of AI systems referred to in Annex III would pose a significant risk of harm to the health, safety or fundamental rights of natural persons or cases in which it would not."

> Art. 6(3) (New): "Where providers falling under one or more of the critical areas and use cases referred to in Annex III consider that their AI system does not pose a significant risk as described in paragraph 2, they shall submit a reasoned notification to the National Supervisory Authority that they are not subject to the requirements of Title III Chapter 2 of this Regulation […]."

Moreover, Ecommerce Europe welcomes the changes proposed by the Rapporteurs in Annex III on high-risk AI systems and use cases, and more specifically the addition made to point 1 on biometric and biometrics-based systems, which now emphasises that "Point 1 shall not include AI systems intended to

be used for authentication whose sole purpose is to confirm that a specific natural person is the person he or she claims to be […]". For the digital commerce sector, this amendment to the Annex is of key importance, seeing that in recent years the use of fingerprints, facial patterns, or voice recognition have become increasingly prevalent in e-commerce for the sake of customer verification in relation to payments and thus to prevent fraud. **We therefore support adding the abovementioned wording to the European Parliament's text, as it will ensure greater legal clarity for businesses making use of such AI systems for verification purposes**.

With that being said, Ecommerce Europe, however, has strong reservations towards the added wording in Annex III, Point 8:

> Annex III, Point 8 (ad) (New): "AI systems intended to be used by very large online platforms within the meaning of Article 33 of Regulation EU 2022/2065, in their recommender systems to recommend to the recipient of the service user-generated content available on the platform".

We are highly concerned of the incorporation of the concept 'very large online platforms' (VLOPs), rooted in the Digital Services Act (DSA) (Regulation EU 2022/2065) as a 'risk category' for the dissemination of illegal content based only on how large a platform is. As such, Ecommerce Europe firmly believes that policymakers should refrain from using this categorisation as a means to determine other levels of risks, or additional responsibilities, outside the scope the concept was originally created for. More specifically, **we fear that online retail platforms, designated as VLOPs under the DSA, would (unintentionally) be affected by this added wording in the AI Act, even if their use of AI systems to recommend products to users on their platforms does not pose a risk of harm.** Ecommerce Europe therefore urges policymakers to exclude this generic use of VLOPs in the AI Act.

Feasibility of obligations for general-purpose AI and 'foundational models'

Ecommerce Europe calls on policymakers to be mindful when laying down new regulatory requirements for general-purpose AI, including 'foundational models', as we find certain obligations introduced under Article 28 on responsibilities along the AI value chain, and subsequent articles on general-purpose AI, to lack fairness and feasibility. Notably, we argue that it would go against the risk-based approach of the AI Act to subject foundational models, not intended by their providers for high-risk uses, to the strict legal requirements envisaged by Article 28b, since such systems do not constitute a particular risk of harm to European consumers and businesses. We thus **urge policymakers to ensure that Article 28b only focuses on the high-risk use cases and excludes foundational models that are not intended for use in high-risk applications**.

Furthermore, **Ecommerce Europe finds the obligations on disclosure of training data sets to be unrealistic, since the proposed transparency requirements do not appear to consider that most AI models train on webcrawled data** – not offline data sets – meaning that the sources of training, validation, testing and input data are the entire open web. As web data is dynamic of nature, it would be practically impossible to disclose all content on the web, and we therefore call on policymakers to ensure that any disclosure obligation for training data sets under the AI Act shall be limited solely to the use of well-defined, contained sources.

Moreover, we are concerned of the 'know your business customer' requirements under Article 28b, requiring providers of foundational models to perform random sample checks of its downstream providers.

Such obligation would raise serious issues regarding business secrecy and privacy. Moreover, since such compliance checks normally are conducted by the competent regulatory authorities, we call on policymakers to ensure that this will also be the case under the AI Act.

Lastly, regarding safeguards against illegal content, we would like to remind policymakers that foundational models are often developed at a global scale, meaning that most commonly there will only be one foundational model to be marketed globally. The interpretation of whether specific content is interpreted to be illegal, however, highly depends on national jurisdictions. As such**, in a field that extends across borders, the proposed provisions on this matter would significantly complicate business compliance in this fragmented legal landscape.** We therefore encourage policymakers to revise the relevant provisions to ensure that compliance is legally feasible.