Position Paper
December 2021

Draft EU Artificial Intelligence Act

About EuroCommerce

EuroCommerce is the principal European organisation representing the retail and wholesale sector. It embraces national associations in 28 countries and 5 million companies, both leading global players such as Carrefour, Ikea, Metro and Tesco, and many small businesses. Retail and wholesale is the link between producers and consumers. Over a billion times a day, retailers and wholesalers distribute goods and provide an essential service to millions of business and individual customers. The sector generates 1 in 7 jobs, offering a varied career to 26 million Europeans, many of them young people. It also supports millions of further jobs throughout the supply chain, from small local suppliers to international businesses. EuroCommerce is the recognised European social partner for the retail and wholesale sector.

EuroCommerce key recommendations to the AI Act:

(i) **The broad definition of AI** – We need a clarified definition of AI. This will create legal certainty and avoid creating unnecessary burdens for companies.

(ii) **The list of "high-risk applications"**: High-risk AI applications should be limited to specific use cases with actual high risk. Specifying categories and providing concrete examples will guide companies in deciding whether a specific practice is considered high risk and offer a future proof framework.

(iii) **Prohibited AI uses**: It must be ensured that Article 5(1a) does not prohibit AI-based algorithms for automatic product recommendations and advertisement and that only passive, mass identification from a distance is prohibited and not the active authentication of individuals.

(iv) **Legal consistency**: Alignment with existing legislation should be ensured and the duplication should be avoided.

(v) **Responsibilities of different actors in the AI value chain**: The responsibilities in the AI Act allocated to different economic operators should be clear and transparent to ensure legal certainty. Any kind of confusion will create an additional burden for developers, business users and end-users.

(vi) **Changes to the legislation:** Changes to the classification of systems as high-risk AI should not be implemented by delegated act, but rather in the co-decision procedure.

(vii) **Feasible obligations**: Obligations imposed on providers, producers, importers, distributors and users of AI systems should be proportionate, easy in the implementation and practical.

(viii) **Access to source code**: There is a need to strike the right balance between transparency and safeguarding trade secrets (such as the source code). There is a risk of distortion of competition if the core content of algorithms has to be disclosed.

(ix) **Enforcement**: The proposed fines are not proportionate and need to be at the level of the General Data Protection Regulation and to be reduced to a maximum of 4 percent of the annual turnover.

(x) **Regulatory sandboxes:** The creation of voluntary regulatory sandboxes to promote the development, testing and validation of innovative AI systems is very welcomed. The framework must be flexible and future proof and leave room to test whether the legal framework still fits in with new developments and adapt when necessary.

(xi) **Guidelines for developers**: The Commission should present a practical and comprehensible guideline for developers after the conclusion of the legislative process.

Introduction

Retailers and wholesalers are users and developers of AI systems and recognize the many opportunities they offer for growth, benefiting consumers, businesses, society and innovation in the sector. Artificial Intelligence is a prerequisite to unlocking Europe's potential to meet EU's digital targets for 2030 and providing support for EU industries in future crises, as it did during the **COVID19 pandemic**. Artificial Intelligence and automation technologies have been utilised for many years by retailers to improve their competitiveness and provide choice and competitive prices for consumers. Using algorithms allows retailers to process highly complex and large amounts of data in real time and generate an optimal solution that meets customer expectations and demands. This has helped the sector to improve its operations and better meet customer expectations by ensuring faster delivery, anticipating customer demand, stock management, fraud detection, safer payments and making it more sustainable. In most cases, AI applications and automation technologies used by retailers and wholesalers carry no direct impact or risks for individuals but improve the shopping experience and internal efficiencies. This is evident by the fact that **the European Commission recognised the retail and wholesale sector as a safe sector in the AI White Paper.**

EuroCommerce welcomes the **draft Regulation laying down harmonised rules on artificial intelligence ('AI Act')** and the overall cross-border harmonization approach in the Digital Single Market and support the EU's effort to create a framework based on EU values. We believe that it is essential to promote a positive narrative on AI technologies and create a framework that would respect existing EU rules and build customers' acceptance and trust. We nevertheless would like to share with you a few concrete comments and recommendations on areas where further clarifications are needed in order to ensure the establishment of a future-proof and technology-neutral legal framework.

Definitions

Definition of Artificial Intelligence

The Act adopts a very broad definition of Artificial Intelligence (AI). This risks to create legal uncertainty to companies which would have to assess whether their systems would fall under the scope, although they are traditionally not considered as AI. As it is currently worded, the definition would encompass most modern software applications and make it extremely difficult to assess which areas fall within the scope of this regulation. We note that the High-Level expert group suggested in their last report a more concrete definition[1].

More particularly, the list of techniques and approaches in Annex I covers many applications which are not necessarily AI systems. For example, in Annex I (c) the legislation covers "*logic-based and statistical approaches, Bayesian estimation, search and optimisation methods*". In most cases statistical approaches and search and optimization methods have been applied for years across the

[1] "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions."

sector and are generally not considered AI. **We believe that statistical approaches should not be included under the scope.** We also observe that the list provided in Annex I is not specific enough, as proven by the phrase included in point (a) "using a wide variety of methods". This is likely to create legal uncertainty for companies trying to implement the rules in the future.

EuroCommerce therefore advocates that the definition be clarified. Based on a clarified definition, the definition of high risk practices needs to be narrowed to focus on the areas where the highest and most far-reaching risks[2] are expected. This will create legal certainty and avoid creating unnecessary burdens for companies.

Prohibited uses (Article 5)

The AI Act includes a list of prohibited AI uses that manipulate negatively human behaviour, opinions or decisions, provided that such use inflicts physical or psychological harm, target vulnerabilities in vulnerable groups, engage in social scoring or can be used for real-time remote biometric identification in law enforcement. In this section the Commission has included on its website an example of a product that will be banned in the future namely "*toys with a voice assistant that encourage minors to engage in dangerous behaviour*". However, it is unclear in defining what constitutes in each case "*dangerous behaviour*", as this may in many cases not be accompanied by "physical or psychological harm" as defined in subparagraph (a) and (b).

It goes without saying that we endorse the objective of avoiding harmful use of AI. However we believe that this definition needs to provide further clarity on what falls under the scope of the prohibitions such as of "subliminal techniques" in subparagraph (a). Commonly used techniques in retail (e.g. advertisement or recommendation systems based on AI) should not in advertently fall within its scope. Retailers use recommendations to help customers navigate through virtual shelves and choose among hundreds of millions of items and large masses of information and not to "limit free choice" or to put humans at risk of physical and psychological harm. The search result customers receive is based on the individuals' own preferences, and retail companies using these techniques are compliant with the GDPR, and perform risk assessments to mitigate any risks. In addition, advertisement, such as personalised advertisement, may include AI and is a crucial means for retailers and particularly SMEs to reach specific customer groups.

We expect further clarification on which areas are under the scope and advocate for these types of systems, when used in the context of the retail sector to not be covered by the AI regulation.

High-Risk AI applications (Article 6, ANNEX II/III)

The AI Act indicates a list of high-risk AI systems, including among others the use of AI for education and training purposes, for recruitment and evaluation of personnel, for assessing the creditworthiness of individuals and for remote biometric identification of natural persons.

We believe that a legally secure framework should ensure, on the one hand, the integrity and right to

[2] When for example the legislators identify systems/methods that present physical or psychological harm, detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected, detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity etc.

private and other interests and on the other hand, it should allow companies to develop and use innovative and employee-friendly AI applications in a balanced way. The blanket assumption that AI applications in these fields are associated with a high level of risk leads to considerable legal uncertainties for companies and could also lead to disproportionate overregulation.

Many EuroCommerce members use in certain cases AI and automated systems, for education and training, as well as employment and human resource management purposes, but **are always mindful of the privacy risks and are proactive in ensuring the protection of the individuals involved and the elimination of any discrimination or bias in the decisions made**. These tools are important for increasing productivity and effective division of labour between humans and machines. In addition, many retail companies rely on being able to use data-driven decision-making to ensure strategic and effective business decisions that align with the companies' business goals. However, such data-driven decision-making would still involve human intervention and oversight at one or more points and does thus not present any of the risks that this regulation aims to address. In order to be high risk, an AI system must also be used in connection with decisions that create a substantial risk to a person's fundamental rights or health and safety, or produce legal effects or similarly significantly effects to that person, without human intervention or review.

We therefore ask that the areas listed in Annex III be limited to specific use cases with actual high risk (see more below). Furthermore the classification of high risk should be based on the concrete use and context of the AI system as well as the probability and likelihood of the worst case scenario, the severity of harm and its irreversibility.

Biometric identification: **We underline the need to cover only private actors' passive, mass identification from a distance and not the active identification (authentication) of individuals**, e.g. at the point of sale (for example: to prevent misuse of bank accounts; to prevent access by non-authorised personnel where necessary for safety; etc.). Only in this way can certain biometric authentication needed for significant innovations in retail, such as payment by fingerprint or cashierless shops, be possible. In addition, we note that in certain cases using biometrics might be even safer than using passwords, particularly when data are duly encrypted, as well as when data minimalization and other privacy safeguards are in place. Furthermore, the distinction between "biometric remote identification" on the one hand and "biometric categorisation system" (Art. 52 para. 2) on the other hand must be clear and unambiguous. In the latter case, no collected data is compared with stored data - i.e. identified - but only a rough categorisation is carried out, e.g. on the basis of age.

Scope

Risk-based approach (scope)

EuroCommerce welcomes the risk-based approach adopted by the European Commission in the AI Act. This is in line with existing technology-neutral legislation, such as the Product Liability Directive and the General Data Protection Regulation. **At the same time, we support a risk-based approach that is not too complicated and multi-layered**.

The European Commission regulates three categories of AI: unacceptable applications that are banned, high-risk and low-risk AI, leaving a large part of AI applications in Europe largely unregulated and potentially allowing manufacturers to bring many further applications to market by self-assessment. It is essential that "high-risk AI applications" are defined in a clear, future-proof manner that ensure legal certainty. We see good approaches with the lists of laws and uses in Annexes II and III of the regulation but we believe that it is important to specify the list of high-risk AI systems based on concrete use cases and examples of the techniques that fall under the scope as to ensure that the boundaries between the categories are clearly defined and remain easily understandable, especially by smaller players**.** This will provide more legal clarity on what really constitutes high-risk and avoid diverging implementation.

An example of potential confusion concerns **chatbots** – they are by definition characterized as minimal risk (which in principle is only subject to the transparency requirements under Article 52 but they could also qualify as a prohibited AI if they potentially cause "physical or psychological harm" (subject to conformity assessment requirements).

The Commission finally needs to ensure that the framework is future-proof and technology neutral, as to avoid very frequent updates to add more techniques and methods under the high-risk AI definition in the future. If updates are required such as changes to the classification list should follow a transparent and accountable regulatory process with the involvement of relevant stakeholders and representatives of the industry. On the basis of Article 4 in conjunction with Article 73, the Commission can amend definitions - including the central AI definition - by delegated act. The list of high-risk AI applications from Annex III is also to be amended by delegated act (Article 7) every two years. We believe that this should both be done under the regular co-decision procedure in consultation with the European Artificial Intelligence Board and the evaluation timeframe should be extended as it is currently very short.

We believe that specifying categories and providing concrete examples will guide companies in deciding whether a specific practice is considered high risk and offer a future proof framework, than trying to pre-identify all applications and products that might fit the definition of high-risk.

Existing legislation

Businesses should not be overburdened with conflicting or overlapping legislation. A distinction should be made on how the AI-Act should interact with other regulatory frameworks. AI such as techniques related to software falls within the scope of various European and national legislation, some of which are now under review, including the Product Liability Directive (PLD), the General Product Safety Directive (GPSD), the Machinery Regulation, the General Data Protection Regulation (GDPR), the EU Cybersecurity Act and is linked to fundamental rights such as the prohibition of discrimination and the principle of equality.

An example of such ambiguity in the Act is the relationship with the GDPR. Under the GDPR framework there is an obligation to carry out a risk assessment before processing personal data with new technologies. It is important that the new obligations under the Act are aligned with existing ones. Although the legal text in Article 10 paragraph 5 of the draft proposal provides for a legal ground for processing special categories to mitigate bias by providers, the Act gives rise to uncertainty about this provision due to the explicit wording in (the last sentence of) recital 41 stating: "*This Regulation should not be understood as providing for the legal ground for processing of personal data, including special* *categories of personal data, where relevant*." It is necessary to provide as much clarity as possible in the Act. **We therefore suggest deleting the last sentence of recital 41.** The regulation should ensure a harmonized approach to processing special categories of personal data to prevent discrimination (accompanied with adequate safeguards).

Finally, **the AI Act should build upon the New Legislative Framework (NLF) for placing products on the EU market.** This means, for instance, ensuring that new requirements can be integrated into existing conformity assessments with as little additional effort as possible and guarantee the greatest possible consistency with existing regulations. This applies in particular to the coordination and cooperation of the authorities involved (market surveillance, nationally competent AI authority, conformity assessment bodies, standardisation bodies, etc.) in the interaction between the AI Act and existing legislation on the NLF.

In summary, in order to ensure legal certainty and avoid unnecessary bureaucratic burdens, as well as ambiguity and complexity in the implementation of the act, further alignment with existing legislation should be ensured and the duplication should be avoided. We believe that when sector specific legislation should have precedence, this should be clearly stated in the recitals to make compliance easier for businesses and ensure a better enforcement.

Recording obligations for High-risk AI (art. 12)

Recording obligations are important and give developers the possibility to retrace their steps. They also allow to establish a relationship of trust with end-users. Recording obligations should, however, contain information that also represents added value for users and that can be recorded in an uncomplicated manner. **In our view, the following information - among others - could be made available in the sense of recording obligations and with a benefit for end users and developers:**

- Artificial Intelligence Architecture
- Resources used
- Problem statement and solution approach
- Computer-implementable instructions
- Responsible use of AI & associated data/processes e.g. re:
    - Carbon footprint of resources vs. benefits.
    - No discrimination in AI use to harm or oppress one group
    - No AI exploitation of humans and animals
    - No detection of diseases through user behaviour
- Data compliance with GDPR
- Transparent documentation of data
- Verification and minimisation of bias (language, gender, etc.) to the best of our ability

Finally, we believe that the duration of the record-keeping obligation should be aligned with the GDPR. The GDPR is the blueprint for all further digital and data-related legislative proposals. Therefore, the duration of the data retention obligation should also be adapted and not go beyond existing obligations. Storing data that no longer has any use can lead to confusion and additional effort without adding any value.

Responsibilities of providers and users

The responsibilities in the AI Act allocated to different economic operators should be clear and transparent to ensure legal certainty. Any kind of confusion will create an additional burden for developers, business users and end-users.

More specifically, the AI Act requires providers of high-risk AI software to put in place a quality management system ensuring compliance with future EU rules. Importers and distributors will be required to verify that high-risk AI software is compliant, provide evidence to competent authorities upon request, and recall non-compliant software. Users will have to monitor high-risk AI software for evident anomalies or irregularities. Users marketing a high-risk AI software under their name or trademark, modifying the intended purpose or making substantial changes will have to take over providers' responsibilities.

This point needs further clarification. The term 'substantial change' is too vague and can be interpreted in different ways. This needs to be clarified, as it determines whether a new conformity assessment is required. In the legislation, qualitative concepts are introduced that offer insufficient guidance and can result in unnecessarily high administrative burden for large and small businesses as they do not provide the required clarity. **The mere implementation of a standardised service should never be considered a substantial change that could lead to the allocation of liability being transferred from the provider to the user.** In addition, more clarity is needed on when a system is "put into use" with specific guidelines.

Furthermore, the **term 'user' in the AI Act is very unclear**, and can have different meanings depending on the context (B2B / B2C). Who will be defined as the user for example when there is both a business user deploying the AI system and an end consumer using the technology? This might lead to confusion when implemented in practice as the obligations according to the economic operator are very different. **The definitions of user and provider in the AI proposal and the revision of the Product Liability Directive should be the coherent.**

We believe that policymakers need to learn from past experience in implementing EU legislation and the difficulties that businesses had or have to face (e.g. in the GDPR the concept of joint controllership) and to provide clarity on the very different responsibilities. Unless one entity is responsible for all aspects of the system, different groups in the chain of development, deployment, and use will have limited visibility and ability to meet all of the AI Act requirements. For example, developers will not be able to attest to use case related requirements if they do not have full control and visibility into all intended use cases/settings. Users of the AI may have limited insights into the algorithm and data sets used by the developer. **We need to make sure that the responsibilities are allocated to the actor who in factual sense has the ability to meet such obligation due to its control/influence over the matter at hand.**

Feasible clear and manageable obligations

Practical feasibility of the AI Act is very important. Obligations imposed on providers, producers, importers, distributors and users of AI systems should be should be high level and proportionate, but also easy in the implementation, focus on the concrete risks and practical. Many details should also be driven by industry-specific regulators (e.g. medical device regulatory bodies should be responsible for establishing AI medical device requirements), or by broader standards bodies. Otherwise, these obligations will fail to be efficient and fit for purpose and could potentially harm EU innovation and growth. In particular:

- Certain requirements for the high-risk AI applications are problematic and not phrased in an appropriate way. For instance, **ensuring that training data is "complete" and "free of any errors" is an unrealistic standard** and should be reframed as ensuring "best efforts" or abiding by "industry standards".
- Certain requirements are also quite vague, such as the notion that AI systems must be developed in a way that **ensures their operation is sufficiently transparent to "enable users to interpret the system's output and use it appropriately**."
- Many requirements also **attempt to control actual development of the system rather than place safeguards around its use**, which will limit ability to develop and innovate.
- **Obligations should be objective driven and specifically address the risk of the use case**. Where appropriate, they should also seek to avoid regulating input/development of systems, as this will significantly hamper companies' abilities to innovate and iterate, and instead focus on output, and how it used to make decisions.
- Ensuring that industry experts are consulted on the technical feasibility of the new obligations introduced as well as during any kind of future planned amendments of the list of high-risk systems. This could best be done by **giving stakeholder experts but also AI developers and data scientists a permanent role in the preparation process of the European AI Board (EAIB),** for example in an expert group that advises the EAIB.

Compliance costs

The proposed legislation outlines a complex compliance framework which will create important administrative burden and costs for all companies. **Micro and small business exemptions will be important in this respect.** The costs of meeting the obligations for high-risk systems are now estimated by the European Commission at € 10,000 for the development phase and between € 5,000 and €8,000 per year for meeting user obligations. In our view, this estimate is very low. The expected costs will create a barrier in particular for SMEs. This would impede growth and innovation in the EU and risks the migration of talent to other regions.

We believe that these obligations need to be designed to ensure that they can actually be met and that businesses are not confronted with unclear and/or unfeasible obligations.

Access to the source code, algorithms and data sets

The AI Act grants regulators "*full access*" to businesses' data sets and to an AI system's source code. While there may be precedent for this practice in certain limited circumstances, this creates very broad regulatory access without necessary safeguards protecting intellectual property, trade secrets, and personal information.

Adequate protection of IP is of great importance to stimulating innovation and give incentives to relevant actors to invest in the creation of valuable data sets. What is essential is that in the event of incidents, it is possible to find out in retrospect how an AI system has reached a decision or other outcome and it is not necessary to give access to sensitive and confidential information as the source code. In any event, a formal request for such valuable information should not go beyond what is necessary and very clearly defined to minimize the data exposed. Competent authorities should be allowed to keep this information no longer than necessary for the underlying investigation. There is a risk in this provision of businesses developing and deploying AI applications will avoid selling across the single market, which would undermine competition and consumer choice.

We believe that there is a need to strike the right balance between transparency and safeguarding trade secrets (such as the source code).

Harmonised standards

Another potential problem arising from the fact that the proposal refers to harmonised standards that do not yet exist. **Corresponding standards must be worked out and specified quickly, based wherever possible on existing standards.** The Commission should seek to request and speedily validate drafted standardisations for the AI Act before its official publication, and ensure the participation of all interested stakeholders in the development of these standards (specifically stimulating the participation of SMEs).

Enforcement

Efficient and cooperative enforcement is necessary to ensure a level playing field across the EU. Supervisors need to have the relevant expertise and sufficient resources in order to adequately perform their duties. This is necessary for legal certainty and to reduce the complexity of the (concurrent) regulations. Experience with other regulation shows that it is essential for supervisors to understand each other's perspectives and to reach a harmonized, coherent supervision in all Member States. Already today businesses in the EU face unclear and even conflicting requirements from different regulators. If a new supervisor is introduced, we risk creating a more complicated landscape. **It would be best to move towards a system in which all stakeholders reinforce each other to achieve the common goals of trust in AI and stimulating growth and innovation.**

Furthermore, we observe a general tendency by EU legislators to **set high turnover-based fines on businesses in case of non-compliance** - up to 6 % of their total worldwide annual turnover for the preceding financial year in the case of the AI Act. We believe that fines should always be effective, proportionate and dissuasive. High fines are unlikely to be of help to businesses that already strive to be compliant, which can nevertheless make mistakes. Instead of focusing on fines as the default, enforcement authorities should seek in the first instance to support businesses in their effort to be compliant.

We suggest that penalties be aligned with the GDPR, and a lower maximum penalty of 4% worldwide turnover to better align with existing legislation.

Regulatory Sandboxes

Regulatory sandboxes are an important instrument to ensure that the AI Act can be timely adopted where necessary to remain future proof. As set out in the proposal, Member States' competent authorities or the European Data Protection Supervisor (EDPS) can develop sandboxes, but they have no obligation to do so. Therefore, it is likely that no such sandboxes will be ready before the entry into force of the Regulation. **This risks leading, not to more innovation, but instead to delays and potential fragmentation in their implementation.**

We also consider it a precondition that the experimental nature of e.g. test and experiment facilities, regulated sandboxes and digital innovation hubs is properly safeguarded. The current proposal places such high compliance requirements on AI systems in the sandbox phase that we seriously question whether this not undermine their practical usefulness. Distinction should be made between compliance sandboxes which can aid SMEs in adhering to the complex obligations of the Regulation and Regulatory sandboxes which provide for a controlled environment. In addition further elaboration should be made to assess which experiments can be undertaken to detect technical, organizational, and legal obstacles as well as possible (high) risks and which measures can be taken to mitigate such risks. Finally, it is necessary to provide an option also for users not only providers to participate in the sandboxes and ensure that all relevant supervisors are involved in a guidance role.

EuroCommerce strongly supports the creation of voluntary regulatory sandboxes under the AI Act in order to promote the development, testing and validation of innovative AI systems. The framework must be flexible and future proof and leave room to test whether the legal framework still fits in with new developments and adapt when necessary. Additionally, the AI Board should have extended powers to oversee how sandboxes are managed and avoid national fragmentation.

Digital Skills

We believe that in order succeed, the AI Act framework needs to be combined with important investment in skills, digital education, and research. We strongly encourage the European Commission to support investment in various digital skills in particular for SMEs and in cooperation with education providers to secure digital literacy across the EU, so that everyone can flourish in an AI-powered future. **Without the right skills, the EU cannot compete with third countries, nor unlock European-based innovation needed for the future.**

Digital education will be paramount in training the AI experts of tomorrow and supporting the competitiveness of the European economy. **We support the suggestions put forward by the European Commission to invest in already existing and create new AI research centres** (*'lighthouse centre of research and innovation for AI in Europe'*) to promote a balanced centralised approach.

Guidelines for developers

Since the new rules are primarily written for lawyers, **we would welcome it if the Commission could present an application-oriented guideline after the conclusion of the legislative process, in which the provisions are "translated" in a practical and easy-to-understand manner for AI developers**, e.g. with corresponding checklists and step-by-step instructions. The guidelines could help developers answer questions such as when an AI application poses a high risk or how to ensure that data sets do not contain bias.

Contact:
Savvina Papadaki - +32 2 738 06 41 -papadaki@eurocommerce.eu

Transparency Register ID: 84973761187-60