EUROSMART
The Voice of the Digital Security Industry

Feedback on the proposal for an AI Act

Eurosmart would like to thank the European Commission for the opportunity to provide feedback on the proposal for an Artificial Intelligence (AI) Act. Eurosmart has long been an advocate for trustworthy AI in line with EU values. Our association welcomes the proposed legislation, in particular the bridge to the Cybersecurity Act. We would like to give the following recommendations:

• Definition of AI systems

The current definition of an AI system is too narrow as it covers only software and not hardware. The definition should also consider the option whereby an AI system is fully implemented in hardware (e.g., AI on edge, in particular AI hardware specialised or generic purpose accelerators). Eurosmart would like to ask the European Commission what the reason is for only considering software.

In addition, Eurosmart questions the list of techniques mentioned in Annex I. Some software that is not usually in the scope of AI technologies could be considered AI with the definition proposed by the European Commission. In particular, the inclusion of "logic- and knowledge-based approaches" and "statistical approaches" is problematic as it makes it virtually impossible to distinguish AI software from traditional data analysis tools. Such a definition creates legal uncertainty for developers, providers and users of AI systems.

Eurosmart would like to propose an amended version of Annex I:

> *(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning,* ***potentially based on the approaches listed in (b):***
>
> ***(b)*** *Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;* ***including statistical approaches, Bayesian estimation, search and optimization methods.***
>
> ***(c) deleted***

For the definition in Article 3, Eurosmart recommends relying on the JRC technical report *AI Watch – Defining Artificial Intelligence*[1], in particular the common features in AI definitions:

[1] Samoili, S., López Cobo, M., Gómez, E., De Prato, G., Martínez-Plumed, F., and Delipetrev, B., *AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence*, EUR 30117 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-17045-7, doi:10.2760/382730, JRC118163.

-Perception of the environment, including the consideration of the real-world complexity

-Information processing: collecting and interpreting inputs (in form of data)

-Decision making (including reasoning and learning): taking actions, performance of tasks (including adaptation, reaction to changes in the environment) with certain level of autonomy

-Achievement of specific goals: this is considered as the ultimate reason of AI systems

The OECD definition seems suitable as it does not exclude purely hardware implementation and includes the notion of "varying levels of autonomy". The OECD definition reads as follows:

> *"AI system: An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy."*[2]

Eurosmart suggests using the OECD definition and adding the following sentence "AI systems are developed with one or more of the techniques and approaches listed in Annex I [as amended above]."

Moreover, Eurosmart recommends aligning the definitions across the different EU legislations. For instance, between the AI Act and the (revised) Product Liability Directive.

• Cybersecurity certification

Eurosmart welcomes the bridge to the Cybersecurity Act whereby AI systems that are already cybersecurity certified can benefit from a presumption of conformity with the cybersecurity requirements of the AI Act. However, this is only the case if the cybersecurity certificate or statement of conformity effectively covers those requirements. Therefore, it is important to have the adequate certification schemes for AI systems.

In Eurosmart's views, dedicated AI certification schemes are needed in the context of the Cybersecurity Act. Our association enjoins the Commission to send a request to ENISA to draft cybersecurity certification schemes for AI. This would facilitate the presumption of conformity through cybersecurity schemes, as the requirements from the AI Act would be fully taken into account in these dedicated schemes.

The schemes should -at least- cover the following aspects:

- Cybersecurity of data
- Cybersecurity of algorithms
- Cybersecurity relating to the usage of AI algorithms

Another crucial aspect to assess is access rights. AI systems have rights to access some kernel features, API or other components. It is essential to have a real view of this access and rights and have traceability. Therefore, the evaluation needs to cover not only algorithms, data, but also life cycle of AI systems and their dependence with other components and rights. In short, AI systems should not use more rights or components than needed.

In addition, schemes need to cover security of supply chains and cross-industry relations.

These schemes should rely on the AI toolbox ENISA advocates for[3]. Such toolbox should include concrete mitigation measures for AI threats -based on risk assessments. This includes mitigation against training attacks (data poisoning, backdoor attack) and against inference attacks (evasion

[2] OECD, Recommendations of the Council on Artificial Intelligence, adopted on 22 May 2019.
[3] ENISA, *AI Cybersecurity Challenges*, Threat Landscape for Artificial Intelligence, December 2020.

attack, model stealing and data extraction). The Group Report from ETSI ISG SAI can constitute a useful reference for this purpose[4].

These AI schemes also need to be adapted to the various AI contexts (cloud, edge etc.), each of them conveying specific cybersecurity risks.

For some security aspects, such as assessing whether data are genuine, Eurosmart thinks that the European Commission should set up a dedicated infrastructure. Data is indeed the most crucial asset in terms of value and liability. Thus, Eurosmart calls for the establishment of an AI Competence Centre.[5] This infrastructure would develop tools to assess the quality of data and other crucial aspects, such as biometric algorithms.

• Predictability

The assessment of the reliability of an AI system is at an infancy stage. The output from these systems may vary over time for the same training datasets. In this respect, assessing the reliability of an AI system is a challenge. Standards and technical specifications must be clear regarding the necessary threshold of predictability. It is important to fund research projects in this area through Horizon Europe and Digital Europe. Eurosmart supports the planned Testing and Experimentation Facilities (TEFs) to test and verify explainability and trustworthiness of AI systems.

• Standards

Standards are essential to prove compliance with the requirements. Harmonised standards will enable providers of AI systems to benefit from the presumption of conformity. Here again, a lot remains to be done. Eurosmart calls on the European Commission to issue a standardisation request to the European Standardisation Organisations (CEN-CENELEC and ETSI). Those two organisations already work on the topic but could benefit from a better guidance from the European Commission. For instance, ETSI ISG SAI and CEN-CENELEC JTC 21 already address AI. The European Commission should leverage their work.

The standardisation request could define some priority areas for standardisation. Among the priority areas, it is worth mentioning:

-ethics: there is currently a lack of standards that consider ethical aspects and values in product or process design. This includes standards to achieve privacy-by-design, standards on the design of the value system or criticality tests to assess the potential impacts of a system on society;

-security, including a standard for basic horizontal security for all AI systems and standards for secure data;

-certification, including the relationship between ethical requirement and technical requirements, associated test methodologies should be defined 'by-default' for each standard in the area of AI systems;

-data quality management for AI, potentially based on the work currently done in ISO/IEC JTC 1/SC 42;

-non-intended use: to mitigate risks standards should not only recognise the intended use but additionally the non-intended use as adversaries do not follow the intended use of a product. This approach includes the quality and contextualization of underlying data used to generate AI systems.

---

[4] ETSI, *Securing Artificial Intelligence; Mitigation Strategy Report*, ETSI GR SAI 005 V1.1.1, March 2021.
[5] Eurosmart, "Europe lacks a reference point for Artificial Intelligence", March 2021.

The German Standardisation Roadmap for Artificial Intelligence[6] can be a useful source of inspiration for standardisation at EU level. It could be used as a basis and further complemented to take into account the interests of all EU stakeholders.

In addition, Eurosmart would like to underline the need for a dedicated structure that could coordinate the work on standardisation at EU level. This should be one of the missions of the AI Competence Centre mentioned earlier.

• GDPR certification

There is currently no solution to GDPR-certify a device. Operational and technical requirements are missing for GDPR certification. This is a major issue for AI systems, for which data protection is particularly important. Eurosmart calls on the Commission and the EDBP to consider this problem. Specific requirements for AI and associated test methodologies are needed.

Furthermore, Eurosmart sees a risk of having diverging guidelines coming from the European AI Board and from the EDPB. National competent authorities for AI might indeed not always be in line with national data protection authorities. How does the Commission envisage harmonisation of guidelines, in particular with regards to data protection?

• Auditability of data

The question of access to data is crucial. Many entities usually wish to have access to the source code of a product but there are data that are very strategic for companies. It can be a problem if everything is open (open-source code), source code might be used for other purposes. This needs to be strictly regulated. Trusted third parties accredited Conformity Assessment Bodies (CABs) are able to assess data and algorithms in trusted environments.

• Data sharing

Eurosmart would like to stress the importance of data sharing across stakeholders. For instance, data sharing could be a way to avoid deep fake, as genuine data could be shared in a reliable way. In this context, the genuineness of data needs to be defined including criteria for data categorisation.

Therefore, Eurosmart strongly supports the current initiatives, such as the Common European Data Spaces, underpinned by the Gaia-X project. This can be used for applications such as cybersecurity. Eurosmart also welcomes the proposal for a European Data Governance Act.

Data sharing should take the ageing process of data into account if data is related to changes. To reduce related risks, the use of such data might be restricted to a certain duration of time. In this case, data might be labelled with an 'expiry date' with impact to AI systems which made use of such data.

• Risk-based approach

Eurosmart would like to mention the particular case of biometric identification systems, as mentioned in Annex III of the proposed Regulation. From Eurosmart's understanding, personal authentication systems (e.g. unlocking a smartphone with face recognition, paying with fingerprint) would not fall into this high-risk category. Eurosmart recommends such an interpretation as it is important to differentiate authentication systems for personal use from generalised identification systems. Both do

[6] DIN, DKE, *German Standardisation Roadmap for Artificial Intelligence*, November 2020.

not convey the same risks. In the first case (personal authentication systems) biometrics data are stored and processed locally on a device for personal use and under the end-user control. The end user could destroy the chip in order not to have any identification possible. This use case is far less risky than biometric identification for the public. Therefore, it should not fall within Annex III.

In any case, clarity is key. It should be easy for manufacturers to know whether their products fall within the high-risk category. This is why Eurosmart recommends drafting a guidance for classification of AI systems, depending on multiple criteria (device, context, impact, types of users, number of stakeholders involved, benefits of the use etc.). The guidance should make classification easier. It could also provide guidance on the sensitivity of certain AI systems to specific risks (for instance some systems are particularly sensitive to cyber-attacks).

Moreover, Eurosmart underlines that AI systems do not only bring risks but also benefits to society. There will be cases where the benefits to use AI will be higher than the risks. However, the AI Act does not consider the balance benefits-risks. The risk is always considered but not the benefit. Article 7 of the proposed AI Act (Amendments to Annex III) lists the factors to take into account when assessing whether an AI system deserves to be categorised as high-risk. There is no reference to the benefits of the use of the AI system. This balance risk-benefit might change the ultimate choice of classification that is made.

- ## Diverted/non-intended use of AI systems

The risk analysis mainly depends on the intended use of the AI system. Eurosmart would like to warn about products for which the initial intended use can be diverted to another use that falls into the high-risk or banned AI systems without a substantial modification. For instance, a live facial recognition for dogs in public areas could be used to track humans -as algorithms might work for both. Eurosmart enjoins the European Commission to consider this possible situation.

In some cases, AI may also be used in a way for which the system was not designed for without intention from the user. This would result in a non-intended use of the AI system.

- ## Real time biometric identification in publicly accessible spaces

The proposed AI Act bans the use of AI for real time biometric identification in publicly accessible spaces for law enforcement purposes. It does not prohibit real time biometric identification in publicly accessible in the case of companies. Eurosmart questions allowing for private companies a use case which is prohibited for public authorities. Eurosmart believes that this provision can be implemented differently depending on the Member State, hence leading to fragmentation.

- ## Competitiveness

The EU needs to have its own structure to certify algorithms (equivalent to the US NIST). This structure could be the AI Competence Centre mentioned above. This is a competitiveness issue because at the moment European companies need to send their algorithms to third countries (e.g. US). Currently, tenders in the world reference the NIST certification, therefore European providers need to comply with it.

Additionally, Eurosmart strongly encourages the Commission to put the emphasis on an AI trust mark so that users are confident that European-made systems are ethical and robust. This AI trust mark would offset the additional requirements placed on AI providers in the EU, compared to competitors on less regulated markets. This marketing strategy is essential to ensure that the AI Act becomes a competitive advantage for EU providers instead of becoming an obstacle to export.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **NXP Semiconductors**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sarapis**, **SGS**, **STMicroelectronics**, **Synopsys, Thales**, **Tiempo Secure, Trusted Objects, TrustCB, WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**), consulting companies (**Internet of Trust**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is a member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, GlobalPlatform, ISO, SIA, TCG, Trusted Connectivity Alliance and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Contact@eurosmart.com