Position Paper
The EU AI Act
Contribution to Trilogue Negotiations

Brussels, 24 August 2023

The Confederation of European Security Services (CoESS) congratulates the European Parliament and Council for the crucial improvements tabled to the European Commission proposal for an EU AI Act. With this position paper, CoESS highlights key proposals of both institutions, which we recommend should be kept in a final agreement or which we believe require further clarification or a more balanced approach that promotes innovation, security and legal certainty for companies integrating AI in their future services. These proposals reflect the recommendations of CoESS' position paper on the EU AI Act proposal from December 2021.

1. Enhanced legal certainty for businesses

CoESS highly welcomes several proposals of European Parliament and Council that aim to clarify definitions and enhance legal certainty in the text – namely:

- **Exclusion of biometric verification and authentication systems of the scope:** both European Parliament (Art. 3.1.33c, 3.1.36, Annex III) and Council (Recital 8) clearly exclude biometric verification and authentication systems, which merely aim to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises. These proposed amendments substantially enhance legal certainty for our businesses and we recommend to keep all these proposals, both in the Recitals, the General Provisions and the Annex.
- **User definion (Art. 3.4):** we believe that the European Parliament's proposal in amendment 172 to use the term "deployer" instead of "user" is more adequate and recommend to keep this proposal in the final agreement.
- **Definition of law enforcement authorities (Art. 3.40):** we welcome that both the European Parliament Report and General Approach in European Council reflect realities in the internal security framework of Member States in Art. 3.40, and include those entities that conduct activities on behalf of law enforcement in the definition. These proposed amendments enhance legal certainty for our businesses and we recommend to keep these changes.

We, however, underline that the European Parliament Report, in contrast to the General Approach in Council, still comes short to **creating legal certainty in Article 28 on when a user/deployer qualifies as a provider**. If the Article is kept, Article 28.1.a should clarify that users/deployers shall only be treated as providers, and hence comply with respective provisions, if they place on the market or put

into service for the first time a high-risk AI system under their name or trademark for which the original provider has not already passed a compliance assessment, or if provisions of Article 28.1.b-c apply.

2. AI literacy: effective safeguards for the guarantee of human-centric AI and qualitative human oversight

CoESS highly welcomes that, in Articles 14 and 29, both the European Parliament Report and the General Approach of the European Council strengthen **appropriateness and proportionality** in the provisions on human oversight, and underline the importance that **users/deployers must ensure to only deploy adequately qualified, competent and trained personnel** for overseeing high-risk AI.

We are convinced that the deployment of adequately skilled personnel is the basis and key for the guarantee of human-centric AI, and hence trust in the technology and compliance with the future Regulation. We therefore favour the **amendments 214, 314 and 401** of the European Parliament in Articles 4, 14 and 29, because they put a more ambitious emphasis on AI literacy and the importance of qualitative human oversight based on adequately skilled personnel.

3. Reflections on the EU AI Act's implications for public security

CoESS is further convinced that, to the extent that the technology will be allowed to be deployed in the EU by law enforcement authorities, additional mandatory human oversight provisions on remote biometric identification systems would help build trust in the technology. In our original position, we have called for Member States to set in place **formal qualification and mandatory licensing frameworks** to guarantee compliance with Article 14 when such sensitive technologies are deployed for very specific purposes in extra-ordinary circumstances.

In line with CoESS' previous position paper, we also welcome the clarification made by European Council in **Article 14.5** to demand mandatory verification by two separate natural persons of the remote biometric identification result before any action is taken, except for the purpose of law enforcement, in cases where Union or national law considers the application of this requirement to be disproportionate. We believe that such possible exemptions are necessary for cases when temporary actions or decisions cannot be delayed due to safety and security reasons for the purpose of law enforcement.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

4. Balancing adequacy and added value when introducing new administrative burden for deployers of high-risk AI

Notably the European Parliament Report introduces new obligations for deployers of high-risk AI which we believe should in each case be based on what is absolutely necessary to enhance transparency on the deployment of high-risk AI.

1. CoESS takes note that both the European Parliament and Council aim to extend the obligations for public authorities, or those acting on their behalf, to **register the deployment of high-risk AI systems in a publicly available database**, referred to in Article 60, as per Article 51 and Annex VIII. If the legislator plans to extend the transparency register respectively, we believe that a balance should be struck between justified and valuable transparency obligations and the need to keep sensitive operational information confidential as follows:
    - In addition to what the Council's General Approach foresees, this could include a description of the intended use of the system, arrangements for human oversight, as well as a summary of the fundamental rights impact assessment and the data protection impact assessment – as proposed by the European Parliament's amendment 770 in Annex VIII.
    - Other provisions, however, which are proposed by the European Parliament's amendment 770 could lead to security risks and should be dropped. Obligations, as per point 4a, for law enforcement authorities and those acting on their behalf, like security services, to disclose publicly geographical and temporal scope of application can be leveraged for criminal purposes and create vulnerabilities in the protection of public spaces and Critical Infrastructure. Furthermore, provisions to disclose categories and nature of data being processed (point 4b) can lead to similar risks and create legal uncertainty due to a lack of a clear definition of these terms. We add that point 4d is not clearly defined in the amendment.
2. The European Parliament Report also introduces the new obligation for deployers of high-risk AI systems to conduct a **Fundamental Rights Impact Assessment** (FRIA) as per Amendment 413 in Article 29a. CoESS supports this new provisions, as long as it presents a natural extension of the Data Protection Impact Assessment (DPIA) under Article 35 of Regulation 2016/679 or Article 27 of Directive 2016/680. However, we strongly recommend to consider the following limitations of this provision:
    - The amendment would oblige deployers of high-risk AI to consult a vast range of stakeholders prior to the system's use as per Article 29a, paragraph 4. CoESS believes that this requirement would add a considerable administrative burden on deployers

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

of high-risk AI and hamper the uptake of AI technology with limited added value due to the already far-reaching FRIA and DPIA provisions. We therefore recommend to strictly align this provision with Articles 35 and 36 of Regulation 2016/679 – hence to notify and consult the national supervisory authority only.

- The amendment introduces in Article 29a, paragraph 5 the obligation for public authorities and undertakings referred to in Article 51(1a) (b) to publish a summary of the FRIA as part of their registration to the publicly accessible database pursuant to Articles 51 and 60. For the security reasons outlined in point 4.1 of this paper, we strongly recommend to reconsider provisions proposed by the amendment which can lead to risks in public security (e.g. avoid publication the intended geographic and temporal scope of the system's use).

About CoESS

CoESS acts as the voice of the private security industry, covering 23 countries in Europe and representing 2 million security officers as well as over 45,000 companies. The private security services provide a wide range of services, both for private and public clients, ranging from Critical Infrastructure facilities to public spaces, supply chains and government facilities. CoESS is recognised by the European Commission as the only European employers' organisation representative of the private security services. Representing a labour-intensive sector, CoESS is actively involved in European Sectoral Social Dialogue and multiple EU Expert Groups – including SAGAS, SAGMAS, LANDSEC, RAILSEC and the EU Operators Forum for the Protection of Public Spaces.

EU Transparency Register Number: 61991787780-18

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**