Position Paper
on the European Commission Proposal for a European Artificial Intelligence Act

Brussels, 20 December 2021

The Confederation of European Security Services (CoESS) recommends in this paper important amendments to the European Commission's Proposal for a Regulation laying down harmonised rules for Artificial Intelligence (EU AI Act) - stressing that the proposal must provide legal certainty and take into account practical implications of its provisions on security and AI-enabled services.

CoESS supports a legal framework that guarantees an ethical and human-centric use of Artificial Intelligence (AI) in Europe and efficient uptake of AI solutions, notably by the services industry.

In cooperation with law enforcement, the security industry will be at the forefront of integrating AI solutions in human-led services at airports, but also in remote monitoring and access control in both public and private spaces. In our view, the integration of AI in security solutions could allow in certain use-cases for a significant increase in performance of security processes, translating in a better protection of European citizens, Critical Infrastructures and the economy against increasingly complex threats to public security.

To strengthen this legal framework for AI, CoESS recommends amendments along the following lines:

1. **We stress the importance of legal certainty and the need for practical and unambigious applicability criteria, definitions, obligations, roles and responsibilities in the EU AI Act.** To this end, we recommend a number of amendments in Article 3.
2. **We highlight that restrictions of the use of "real-time" remote biometric identification systems must not leave room for interpretation; reflect operational realities and requirements in public security; and set important safeguards against the technology's misuse.** Exemptions of Article 5.1.d should therefore only apply for law enforcement authorities and entities acting on their behalf. Mandatory qualification requirements for those operating "real-time" biometric identification systems should be introduced. At the same time, the proposal must allow for such systems to be deployed in Critical Infrastructure.
3. **We underline that adequate and realistic human oversight provisions are key for legal certainty, safe uptake of AI products and services by users, and an ethical and human-centric use.** We therefore recommend a number of clarifications in Article 14 that reflect realities in security processes, i.e. at airports, Critical Infrastructure Protection, remote surveillance and access control.

1. Definition of user

CoESS is convinced that legal certainty of the definition of "users" in Article 3 is the basis for water-proof compliance of users with provisions of the EU AI Act (namely Articles 14 and 29 – see pages 14 and 15 of this paper). In consequence, this is also key for efficient auditing and compliance assessments by national competent authorities.

We therefore stress that it is necessary to clarify the term "user using an AI system under its authority". This likewise requires clear identification of frontend and backend operations of an AI system. Proposals for both such amendments are made in this paper.

Practical example: Remote monitoring is an important business segment of security companies. Here, security officers are in frontend operations remotely monitoring the output of a number of video surveillance cameras in diverse locations for both private and public clients. In these services, it is often the case that security companies only process the data of cameras, without owning them or without further authority, knowledge and/or control of the concrete remote monitoring and surveillance equipment being used. They may often not know whether the equipment includes AI components. In these cases, they should not be able to be held liable for a malfunctioning of the AI system. It is in the clients' responsibility, who has full authority over the system, to ensure compliance with provisions of the EU AI Act – either by own processes or contract management.

Article 3 - Definitions

(4) 'user' means any 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.

New: (4a) 'user using an AI system under its authority' means any natural or legal person, public authority, agency or other body that fulfils the following criteria:

- ***a) is nominated and/or held accountable for the ethical and legal compliance of the system's frontend operation and human oversight as per Article 14,***
- ***b) controls the frontend operations of an AI system, related risks as well as the input of information into the AI system, either alone or jointly with others,***
- ***c) has full knowledge of and exercises defined controls over the intended purpose, reasonably forseeable misuse and AI components of a system based on provided instructions of use.***

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

New: (4b) 'frontend operation' means the visible use, deployment and operation of an AI system under human oversight as per Article 14, which interprets and acts on data output, and interacts with the data subject.

New: (4c) 'backend operation' means the technical operation of an AI system, including its settings and data input, data management and processing, digital maintenance and software updates, providing data output and enabling frontend operations.

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**

2. Qualification of users as providers

CoESS welcomes that the definitions of "placing on the market" and "putting into service" in Articles 3.9 and 3.11 correspond largely to the EU Machinery Directive 2006/42. To create legal certainty on when users qualify as providers, we believe that coherence should be further fostered in Article 28. As per Directive 2006/42[1], the person placing machinery on the market in the EU may be able to arrange for the "original manufacturer" to fulfil the obligations according to the Directive, and have the item CE marked. If that is not the case, the person placing the machinery on the market or putting it into service in the EU must fulfil these obligations him/herself. Article 28 should therefore clarify that users 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 rovisions of Article 28.1.b-c apply. For legal clarity, we recommend to add a respective provision to Article 28.1.a.

Practical example: security companies may in the future place on the market or put into service existing high-risk AI solutions under their own trademark. In this case, they should only be considered as providers, if the original provider did not already pass a compliance assessment.

Article 28 Obligations of distributors, importers, users or any other third-party

1. Any distributor, importer, user or other third-party shall be considered a provider for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:

(a) they place on the market or put into service a high-risk AI system under their name or trademark and the original provider has not fulfilled its obligations as such;

[1] European Commission (2019): Guide to application of the Machinery Directive 2006/42/EC. Available here.

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**

3. Definition of safety component

The definition of "safety component of a product or system" is at the heart of the definition of high-risk AI as per Article 6. AI components can often also have a security function, which must be seen separately from safety. The definition as it stands is therefore not inclusive of security components. Therefore, we recommend an amendment as per the text below in order to rule out any legal uncertainty on what AI systems are covered by the definition of high-risk AI in Article 6.

Article 3 - Definitions
(14) 'safety component of a product or system' means a component of a product or of a system which fulfils a safety and/or security function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property;

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. Definition of significant modification

The definition of "significant modification" is key for the definition of high-risk AI, and which AI systems need to comply with provisions of the future EU AI Act, as per Article 83.2.

As per the current proposal, its definition in Article 3.23 would also include changes and modifications that are due to a self-learning feature of the AI system of which operators may not be aware. CoESS understands that the European Commission will address liability matters related to self-learning AI in a future legal or non-legal initiative. CoESS therefore recommends that the future EU AI Act should only cover modifications that are due to human intervention and control, in order to provide legal clarity. We add that the term of "significant changes" in Article 83.2 is confusing and should be aligned with Article 3.23.

Practical examples: The European Commission "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics" (COM(2020)64) rightly states that "Autonomy can affect the safety of the product, because it may alter a product's characteristics substantially, including its safety features. It is a question under what conditions self-learning features prolong liability of the producer and to what extent should the producer have foreseen certain changes". As CoESS expects this aspect to be addressed by a future legal or non-legal initiative on liability rules, the definition of "substantial modification" should only covers those that are undertaken by an operator.

Article 3 - Definitions

(23) 'substantial modification' means a ~~change~~ modification undertaken by an operator to the AI system following its placing on the market or putting into service which affects the compliance of the AI system with the requirements set out in Title III, Chapter 2 of this Regulation or results in a modification to the intended purpose for which the AI system has been assessed;

Article 83.2 - Definitions

This Regulation shall apply to the high-risk AI systems, other than the ones referred to in paragraph 1, that have been placed on the market or put into service before [date of application of this Regulation referred to in Article 85(2)], only if, from that date, those systems are subject to significant ~~changes~~ modifications in their design or intended purpose.

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

5. Use of "real-time" remote biometric identification systems in Critical Infrastructure

CoESS understands from Recitals 23 and 24 that the EU AI Act is without prejudice to Regulation (EU) 2016/679[2] (GDPR), and Directive (EU) 2016/680[3] (LED). Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification must continue to comply with GDPR and LED, but that Article 5 must be seen as *lex specialis* to both.

CoESS notes that:

- GDPR allows for the processing of biometric data based on the data subject's explicit content or based on substantial public interest as per Article 9.
- LED allows for the processing of biometric data, including automated individual decision-making, for law enforcement purposes by competent authorities pursuant to Articles 1, 10 and 11.

We however miss a clarification of the interplay between the EU AI Act's Article 5, GDPR and LED, which creates, in our understanding, legal uncertainty and unnecessary "one-size-fits-all" restrictions on the use of "real-time" remote biometric identification systems – independent of the specific use-case and respectively related risks of "mass surveillance". Notably, Article 5 prohibits the use of "real-time" remote biometric identification systems in one very specific case, where their use would be possible under provisions of GDPR and LED, and of high benefit for public security: Critical Infrastructure Protection (CIP). CoESS strongly recommends to close this legal gap through respective amendments in Article 5. Fundamental rights implications of using these technologies vary considerably depending on the purpose, scope and context of the deployment. CoESS warns of the negative consequences of limiting law enforcement authorities' use of such state-of-the-art technology for CIP at times of increasingly complex threat scenarios to public security and the need

[2] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[3] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data.

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**

for enhanced resilience of Critical Infrastructure - as confirmed by the recent European Commission proposal for a Directive on the Resilience of Critical Entities.

Practical example: to reflect current trends and developments in public security and related threats, CoESS believes that law enforcement authorities must have the possibility to deploy "real-time" remote biometric identification systems in certain Critical Infrastructures – under provisions of Article 9 of GDPR and Articles 10 and 11 of LED, based on a thorough impact assessment of EU Member States. The current definition of "publicly accessible spaces" would prohibit such use-cases, comprising law enforcement authorities of a crucial protection tool for infrastructures that are essential for the functioning of our societies and economies. Article 5.1.d.ii should therefore explicitly allow for the use of "real-time" remote biometric identification systems in Critical Infrastructure.

Article 3 - Definitions

(NEW) 'critical infrastructure' means an asset, system or part thereof which is necessary for the delivery of a service that is essential for the maintenance of vital societal functions or economic activities within the meaning of Article 2(4) and (5) of Directive ……/…… on the resilience of critical entities;

Article 5.1.d - Prohibited Artificial Intelligence Practices

(ii) the prevention of a specific and substantial ~~and imminent~~ threat to the critical infrastructure, life, health or physical safety of natural persons or or of a terrorist attack;

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**

6. Clarification that only law enforcement authorities can make use of Article 5

CoESS agrees that the legal proposal must make clear that only law enforcement authorities, as per Article 3.40, are allowed to use "real-time" remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, and not leave room for interpretation to this provision. Furthermore, we firmly believe that Member State authorities have a responsibility to ensure that only adequately qualified and licensed personnel of law enforcement authorities is allowed to operate "real-time" remote biometric identification systems[4].

Practical example: A lack of AI skills can be a significant barrier to the ethical and human-centric use of AI: the human oversight provisions as per Article 14 are very complex and expect from the human interface a very distinct knowledge of the functioning and associated risks of the AI system, as well as ongoing control over the operation. CoESS therefore calls on lawmakers to include a mandatory obligation for Member State authorities to put in place an adequate qualification and licensing regime for security officers using AI systems that are covered by Article 4. This not being the case, CoESS fears that the full respect of fundamental rights by this highly sensitive technology cannot be guaranteed, leading to a lack of trust of citizens in this technology which can be of high added value for public security.

Article 5 – Prohibited Artificial Intelligence Practices

1. *The following artificial intelligence practices shall be prohibited:*
   (…)
   (d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement by law enforcement authorities or on their behalf, unless and in as far as such use is strictly necessary for one of the following objectives:
   (…)

[4] In addition, the European Commission may want to establish a central body to facilitate European skills training for law enforcement authorities in EU Member States.

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

Article 5 – Prohibited Artificial Intelligence Practices

2. *The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:*

   (…)

   In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall

   (a) comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations;

   (b) guarantee compliance with the human oversight provisions set out in Article 14 through formal qualification and licensing frameworks, which Member State authorities shall put in place.

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**

7. Definition of (real-time) remote biometric identification, verification and authentication technologies

The legal proposal covers the deployment of ("real-time") remote biometric **identification** systems as per Article 5 and Article 6.2. However, it is not clear whether the notion "*identification*" also includes "*verification*" and "*authentication*". Notions of remote biometric **verification** and remote biometric **authentication** systems, which both come with very distinct use-cases and considerably lower risks than identification systems, are omitted in the proposal.

CoESS believes that this omission creates substantial legal uncertainty concerning the deployment of biometric **verification** and **authentication** systems, and recommends that ("real-time") remote biometric **verification** and **authentication** systems are excluded from the scope of Annex III. Both come with a very low risk, because they are used in consent with and/or on request of the natural person.

Also, all distinct biometric distinct systems must be adequately defined in Article 3.

Practical examples:

The purpose of remote biometric **verification** and **authentication** systems is very distinct to **identification** systems and are based on consent. Both hence come with a very different risk-level to fundamental rights of citizens and should be excluded from the scope of the legal proposal.

- For the purpose of **identification**, a comparison is made between an identified facial map and a database of identifying data to which a natural person may not have given consent – for example in use-cases related to the search of criminals and other specific persons of interest.
- For the purpose of **verification**, a comparison is made between an identified facial map and a database of identifying data to which a natural person has given consent – for example in use-cases related to access control to sensitive areas like Critical Infrastructure, other essential service infrastructures or government buildings.
- For the purpose of **authentication**, a natural person authenticates his/her own identity on own request – for example in personal access to mobile phones, computers, online banking.

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**

Article 3 - Definitions

New (36a) "Identification of/ identifying a natural person" means the process of establishing the identity of an individual among a group by comparing the data of the individual to identify to those of each individual in the group (one-to-many matching) and excludes the process of confirming if an individual is who she or he claims to be (authentication) or confirming if an individual has a privilege that he or she claims to have (verification) (one-to-one matching).

New (36b) 'remote biometric verification system' means an AI system for the purpose of verifying the identity of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database with prior consent of the natural person, and with prior knowledge of the user of the AI system whether the person will be present and can be identified".

New (36c) 'remote biometric authentication system' means an AI system for the purpose of authenticate the identity of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database on request of the natural person".

NEW (36d) "at a distance" means the process of identification, verification or authentication in physical distance, in direct interaction with the data subject or without.

New (37a) ''real-time' remote biometric verification system' means a remote biometric verification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention".

New (37b) ''real-time' remote biometric authentication system' means a remote biometric authentication system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention".

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**

Article 5 – Prohibited Artificial Intelligence Practices

New Article 5(5): prohibited artificial intelligence practices do not cover ("real-time") remote biometric verification and/or authorisation systems as defined in Art. (36b), (36c), (37a) and (37b).

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**

8. Adequacy of human oversight provisions in Articles 14 and 29

The human oversight provisions of Articles 14 and 29 do not reflect realities in security processes and lack precision for the concrete responsibilities of providers on the one hand (backend operators defining the features of the technology, providing data and essential backend support such as software updates), and users (as per updated definition on page 2 of this paper). Borders between provider-responsibility and user-responsibility are blurred. In addition to the previously recommended clear definition of "users using an AI system under its authority" (see page 2 of this paper), CoESS recommends further precise wording on human oversight provisions in Article 14. Users can only be expected to have human oversight over the AI system's frontend operations to the extent described in the instructions for use, and if security-by-design features allow for specific interventions.

Article 14 - Human oversight

4. The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances ***and instructions for use*** :

(a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its ***frontend*** operation ***and output***, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;

(b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;

(c) be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available ***as provided by instructions for use***;

(d) be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system ***to the extent described in the instructions for use;***

(e) be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure ***to the extent described in the instructions for use and by means of security-by-design features as per Article 14.3.1.***

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

Article 29 - Obligations of users of high-risk AI systems

1. Users of high-risk AI systems shall use such systems in accordance with the instructions of use accompanying the systems, pursuant to paragraphs 2 and 5.

2. The obligations in paragraph 1 are without prejudice to other user obligations under Union or national law and to the user's discretion in organising its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.

3. Without prejudice to paragraph 1, to the extent the user exercises control over the input data, that user shall ensure that input data is relevant in view of the intended purpose of the high-risk AI system.

4. Users shall monitor the ***frontend*** operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis. (…)

5. Users of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system, to the extent such logs are under their control. The logs shall be kept for a period that is appropriate in the light of the intended purpose of the highrisk AI system and applicable legal obligations under Union or national law. (…)

6. Users of high-risk AI systems shall use the information provided under Article 13 to comply with their obligation to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, where applicable.

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**

9. Clarification of human oversight on remote biometric identification technologies (Art. 14.5)

As per the legal proposal's Article 14.5, two natural persons are required to verify and confirm the outputs of the remote biometric identification system. CoESS recommends to change the wording of this provision to guarantee a valuable use of such technologies in security processes and provide legal certainty. In its current form, the proposal does not clarify whether the two natural persons verifying and confirming the outputs have to be physically present. In practical application in private security services, this provision creates legal uncertainty, also for auditing on compliance with provisions, and unnecessary room for interpretation with potentially highly negative impacts on security processes.

Also, we recommend that the wording is changed in a way that allows for temporary actions or decisions to be made on the basis of the identification if such temporary actions or decisions cannot be delayed due to safety and security reasons for the purpose of law enforcement.

Practical example: As it stands, the provisions are detached from realities in public security and would considerably slow-down the identification process if:

- a rapid decision is required for law enforcement purposes. The regulation should therefore allow for flexibility in temporary actions or decisions which cannot be delayed due to safety or security reasons for the purpose of law enforcement.

- a front-line officer is working in isolation and is the only person available to verify the output. The regulation should therefore make clear that two suitably qualified people can also verify the outputs from a remote location and the output should then be sent to who ever is acting on the front-line. Such clarification is also key for competent authorities responsible for auditing of user compliance with provisions set in Chapter 2 and 3 of the EU AI Act.

Article 14.5 - Human oversight

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons on-site or remotely, except for temporary actions or decisions which cannot be delayed due to safety or 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

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**