



Acting as the voice of the **security industry**

Confederation of European Security Services



# Charter

on the ethical and responsible use of **Artificial Intelligence** in the European private security services



11 October 2024

#### Copyright:

Unless stated to the contrary, all materials and information are copyrighted materials owned by CoESS (Confederation of European Security Services). All rights are reserved. Duplication or sale of all or any part of it is not permitted. Permission for any other use must be obtained from CoESS. Any unauthorised use of any materials may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes. To the fullest extent possible at law we (and all our sister, parent, subsidiary and member companies and organisations) exclude all liability for any loss or damage (including direct, indirect, economic or consequential loss or damage) suffered by you as a result of using the contents of this manual.

#### Disclaimer:

This Charter was developed by a dedicated Expert Group of CoESS for the European private security industry. It focuses on guidance for deployers of AI systems only.

This document shall provide security companies with a first understanding of the EU AI Act and important codes of conduct prior to and during the use of an AI system. The information provided in this Charter does not replace system and use case specific risk and regulatory assessments that should be conducted by the deployer to ensure compliance with the EU AI Act.

#### Design & graphics:

<https://blog.acapella.be/>

#### Photo credits:

© AdobeStock: 713733409: Milan, 913052673\*: suratin, 874669432\*: Andres Mejia, 588772865: NicoElNino, 846542130\*: ImageFlow, 802446835\*: ERIK, 728100169\*: Miumzlik, 355680792 and 516647240: .shock, 794014906\*: Natanong, 720464800\*: inthasone, 725689364\*: sandsun, 777449543\*: Bartek, 185898613: Kadmy, 732479109\*: ALL YOU NEED studio, 861484312\*: ALEXSTUDIO, 824935213: pressmaster, 326350464: PX Media

\* Generated with AI

© iStock: 2130201321: Suriya Phosri, 1472578503: Pakpoom Makpan, 1428421517: Galeanu Mihai, 1168365129: metamorworks

#### Special thanks to the active contributors to this Charter:

Carolina Garcia Cortés, Innovation Manager, Prosegur  
Cornelius Toussaint, CEO, Condor Group  
Daniel Sandberg, Director of Artificial Intelligence, Securitas Group  
Graham Evans, Technical Officer, BSIA  
Helena Eriksvik, Head of Global Legal Data & Privacy, Securitas Group  
Pauline Norstrom, CEO Anekanta®AI, and representative of BSIA  
Victoria Ferrera Lopez, Regulatory Affairs Group Senior Manager, Verisure  
Wim Bartsoen, Chief Digital Security Officer, Securitas Group

#### About CoESS:

The Confederation of European Security Services (CoESS) acts as the voice of the private security industry, covering 22 countries in Europe and representing 45,000 companies with 2 million security officers. Private security services provide a wide range of services, both for private and public clients, ranging from Critical Infrastructure to public spaces, supply chains and government facilities. CoESS is recognised by the European Commission as the European employers' organisation representative. We are actively involved in European Sectoral Social Dialogue and multiple EU Expert Groups – including SAGAS, SAGMAS, LANDSEC, the EU Operators Forum for the Protection of Public Spaces and the EU Ports Alliance.

**EU Transparency Register Number: 61991787780-18**

# Executive Summary

This Charter, developed in alignment with the EU Artificial Intelligence Act and the core values of CoESS, establishes a framework of **10 essential requirements** for the **responsible and ethical deployment of Artificial Intelligence (AI)** by European private security companies.



**RISK MANAGEMENT:** adopt appropriate and targeted risk management measures.



**DATA GOVERNANCE:** uphold diligent data governance, ensuring the use of trustworthy data and strict compliance with GDPR.



**HUMAN OVERSIGHT:** Equip staff with the necessary training and policies to meet human oversight requirements, proportionate to the specific AI use case.



**RESILIENCE MEASURES:** achieve robust physical and cyber protection for company assets, AI systems, and associated infrastructure.



**RECORD-KEEPING:** document the AI systems' operational performance.



**TRANSPARENCY AND EXPLAINABILITY:** set in place adequate transparency measures that guarantee compliance with GDPR and the EU AI Act, and aim for adequate levels of explainability.



**FUNDAMENTAL RIGHTS IMPACT ASSESSMENT:** Conduct assessments on the potential impact on fundamental rights, even if its not a legal obligation, but when there are plausible concerns about unlikely but possible rights impacts.



**DUE DILIGENCE:** follow due diligence policies when buying AI systems



**WORKERS' INVOLVEMENT:** foster awareness among workers on the use of AI in your company and set in place mechanisms for addressing concerns, particularly if using high-risk AI.



**ENGAGE WITH PUBLIC AUTHORITIES:** work actively with competent authorities to get additional guidance and to clarify legal uncertainties and compliance requirements.

# CONTENTS

<b>Executive Summary</b>	<b>3</b>
<b>Introduction</b>	<b>6</b>
<b>Chapter I: Definition of AI and use cases in the European private security services</b>	<b>8</b>
I. What is AI ? Striving for a definition	8
II. Cross-cutting criteria to differentiate between low-risk and high-risk AI	10
III. The EU AI Act and legal compliance: low-risk vs. high-risk AI	11
IV. Examples of possible low-risk and high-risk AI use cases	14
<b>Chapter II: Opportunities and risks of AI deployment in security services</b>	<b>18</b>
I. Opportunities	18
II. Risks	20



<b>Chapter III: Values and Requirements</b>	<b>25</b>
I. CoESS' transversal values for the ethical and responsible use of AI	25
II. First steps to ensure an ethical and responsible use of AI	26
III. Requirements for the ethical and responsible use of AI	27
<b>Chapter IV: Checklist</b>	<b>33</b>
<b>Annex: Repository of useful guidelines and standards</b>	<b>34</b>

# Introduction

The integration of Artificial Intelligence (AI) into security services is expected to play an important role in the ever-evolving transformation of the security industry.

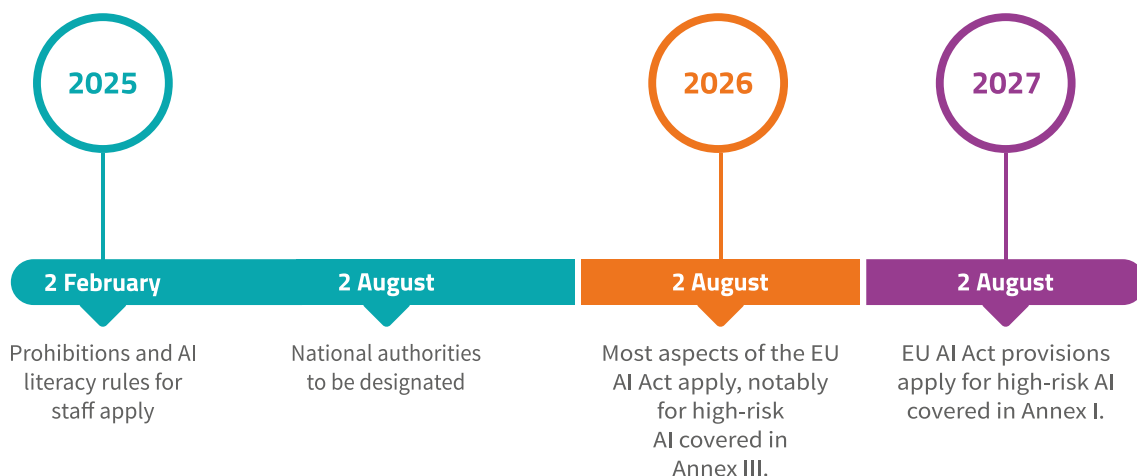
From data-enabled risk analysis to integrated video surveillance, AI systems can be deployed in many different use cases in the security services, bringing benefits to workers, customers, companies, and public security. Nevertheless, some use cases come with risks.

The European Union (EU) has therefore regulated the development and deployment of so-called “high-risk” AI in the EU AI Act. Security companies that operate in the EU and integrate AI systems into their services will have to start complying with most aspects of the Regulation as of 02 August 2026, but with some provisions applying as soon as 02 February 2025 (see timeline graphic).

It is important to help companies understand the impact of the EU AI Act on their business operations. Many companies may not even be aware if they use AI today in their services. But as of now, every security company, big and small, will have to know if they deploy an AI system and what to do. But there is more.

The Confederation of European Security Services (CoESS) and its members stand for human-centric innovation for the public good and a steadfast commitment to ethics, responsibility, and compliance.

## Timeline: Application of the EU AI Act





This Charter shall therefore not only help companies comply with the EU AI Act, but also integrate AI systems in a responsible and ethical way that goes beyond compliance. To this end, this Charter is structured in four chapters:

- **CHAPTER I** provides orientation for companies to help them identify AI systems and “high-risk” use cases in the security services, based on legal and other cross-cutting criteria.
- **CHAPTER II** offers an overview of opportunities and risks that are associated with the use of AI in the security services.
- **CHAPTER III** establishes requirements for AI deployers in the security industry that address pertinent risks, both according to the legal obligations of the EU AI Act and CoESS’ value set.
- **CHAPTER IV** sets out an easy-to-understand checklist for companies on the steps to take when planning to deploy an AI system today.

#### DISCLAIMER

This Charter was developed by a dedicated Expert Group of CoESS for the European private security industry. It focuses on guidance for deployers of AI systems only.

This document shall provide security companies with a first understanding of the EU AI Act and important codes of conduct prior to and during the use of an AI system. The information provided in this Charter does not replace system and use case specific risk and regulatory assessments that should be conducted by the deployer to ensure compliance with the EU AI Act.



# Chapter I: Definition of AI and use cases in the European private security services

## I. What is AI ?

### Striving for a definition

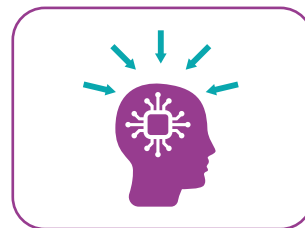
The first question every deployer will have to answer is: am I using AI? The legal definition of AI is, however, a complex exercise with different approaches around the globe. This Charter promotes compliance in particular with the EU AI Act, so we will refer in this document to the AI definition in EU law.

In the EU AI Act, the EU strongly aligns the legal definition of AI with the one of the Organisation for Economic Cooperation and Development (OECD). As per the EU AI Act's Article 3.1, an AI system is defined as:

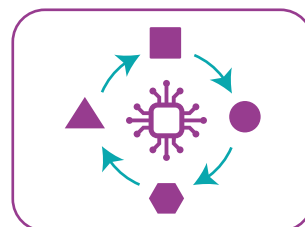
*"a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"*

This legal definition is quite complex. It is therefore helpful to have a look at the OECD AI Principles<sup>1</sup>, an intergovernmental Standard on AI, and explain its different aspects :

**AUTONOMY<sup>2</sup>:** an AI system can accomplish a task with a varying range of human involvement, from being partly to fully autonomous. This is both the core asset and risk associated with the use of AI. Depending on the output of the task and level of human oversight, even simple, fully autonomous systems can pose a substantial risk to fundamental rights.



**ADAPTIVENESS:** Another core asset, but also risk, of many AI systems is their ability to self-learn and to adapt or evolve. They evolve based on input from users i.e. after the design and deployment phase. AI therefore has an inherent risk that the system is processing data in a way that is often referred to as a "blackbox", reducing the explainability of the AI system's output.



<sup>1</sup> R. Stuart, K. Perset, M. Grobelnik (2023): Updates to the OECD's definition of an AI system explained. Available here: <https://oecd.ai/en/work/ai-system-definition-update>

<sup>2</sup> additional references available for the definition of autonomy in AI systems: EN ISO/IEC 22989 and Recital 12 of the EU AI Act [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf)

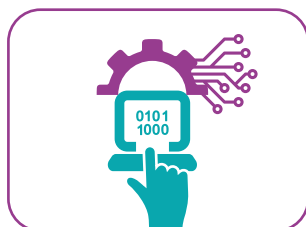




**OBJECTIVES:** an AI system can have different objectives. Explicit objectives are usually the result of the rules set by the developer (and possibly also deployer) – e.g. a drone autonomously transporting an object from A to B. But there are also AI systems, which have only implicit objectives, such as General Purpose AI based on Large Language Models (LLM).



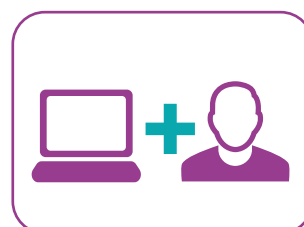
**INPUT:** AI systems are based on input, which is necessary for them to generate an output. Input can include sets of rules and algorithms defined by the developer, training data used by the developer to further evolve the AI system, additional instructions by the deployer, and data received by the environment, which may further contribute to the self-learning of the system.



**OUTPUT:** The developer (and potentially those who deploy the system) determines the intended functionalities of the AI system and the types of outputs it will generate - such as predictions, content, recommendations, or decisions. To reach an output, an AI system processes its input based on rules, instructions, and algorithms created by its developers and potentially refined by those who deploy it. High-risk applications typically involve outputs that have significant real-world impacts and operate with a high level of automation, leaving little human oversight.



**ENVIRONMENT:** Environments, which feed the AI systems with input, and are subject to its output, can be both physical (e.g. detection and verification of objects and natural persons) and virtual (e.g. in the analysis of business operations).



## II. Cross-cutting criteria to differentiate between low-risk and high-risk AI


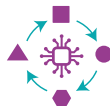




The different aspects that can explain the functioning of AI systems can also be used as interdependent, cross-cutting criteria, which may provide a very first orientation for deployers on:

- how to know whether a system is itself an AI product or an AI safety component of a product.
- how to distinguish between low-risk and high-risk AI systems and use cases.

However, every assessment of an AI system and use case is unique and, within the EU, subject to the definition of low-risk and high-risk AI in the EU AI Act.

Another, more extensive approach to define different criteria and characteristics of AI can be found in EN ISO/IEC Standard 23053:2022 (Framework for Artificial Intelligence Systems Using Machine Learning).

**“Every assessment of an AI system and use case is unique”**

<b>AUTONOMY</b>		IF the AI system produces autonomous outputs in a physical environment, it is likely to be classified as high-risk. The EU AI Act therefore makes human oversight mandatory for high-risk AI systems and use cases.
<b>ADAPTIVENESS</b>		IF the AI system's decision-making process is based on logical self-learning in a “blackbox” and evolves over time, it can lead to an increased lack of explainability and is more likely to be categorised as high-risk.
<b>OBJECTIVES</b>		IF the objectives of the AI system have an impact on natural persons or are implicit, it becomes more likely that the AI system and use case are categorised as high-risk.
<b>INPUT</b>		IF the input is based on personal data of natural persons then compliance with GDPR is key and the risk of being categorised as high-risk increases.
<b>OUTPUT</b>		IF the output of the AI system poses a risk of harm to the health, safety or fundamental rights of natural persons, including by materially influencing the outcome of a decision-making process, it is likely to be classified as high-risk.
<b>ENVIRONMENT</b>		IF the output affects an environment that includes a natural person, the likelihood that the AI system and use case are high-risk is higher.



### III. The EU AI Act and legal compliance: low-risk vs. high-risk AI

Different AI systems and use cases bring different risks. The EU AI Act follows a risk-based approach and regulates mostly high-risk AI systems and use cases. With this Chapter, we aim to provide deployers of AI systems in European private security services with an initial understanding of the approach taken by the EU AI Act. Please note that the European Commission's EU AI Office will develop guidelines for AI system definition, prohibitions and high-risk classification.

To start with: every deployer of AI systems in the EU has to comply with the EU AI Act.

That's however the only simple part. Because legal obligations for deployers of AI systems (see as of page 27) differ depending on the risk associated with the system and use case in question. The EU AI Act distinguishes between the following categories of AI systems and use cases:

1. LOW-RISK AI SYSTEMS AND USE CASES
2. PROHIBITED AI PRACTICES
3. HIGH-RISK AI SYSTEMS AND USE CASES



Low-risk are generally those AI systems and use cases which do not fall in the 'prohibited' and 'high-risk' categories. The EU AI Act further clarifies that an AI system is also generally classified as low-risk if it is intended to:

- perform a narrow procedural task or mere preparatory task of high-risk AI use cases;
- improve the result of a previously completed human activity;
- not replace or influence the previously completed human assessment, without proper human review.

Within the low-risk category, the EU AI Act further distinguishes between systems with minimal risk, without legal obligations, and certain AI systems with a transparency risk, which have to comply with certain transparency obligations<sup>3</sup>.

**“Every deployer of AI systems in the EU has to comply with the EU AI Act”**



<sup>3</sup> AI systems that interact with natural persons, but would qualify as low-risk (such as LLM and chatbots), have to comply with certain transparency obligations which are set out Article 50 of the EU AI Act. For example, the concerned natural person must be informed that it is interacting with an AI system. All AI systems that are neither prohibited nor qualify as “high-risk” (see page 13) or systems with a transparency risk are considered to be of minimal risk. Their deployers do not have to comply with extensive legal obligations of the EU AI Act, but they are encouraged to apply voluntary codes of conduct – to be developed by EU bodies, Member States, or representative bodies.

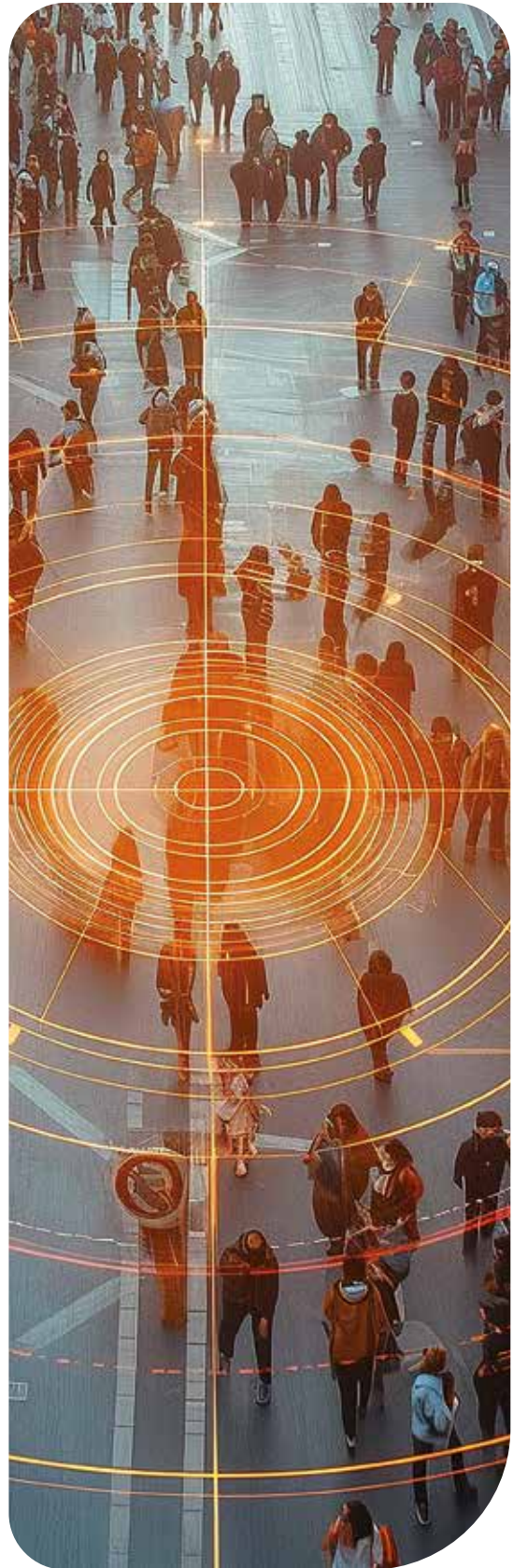
## 2. Prohibited AI practices



The EU AI Act defines in its Article 5 those AI systems and use cases, which bring an unacceptable risk to the fundamental rights of European citizens. These are therefore prohibited and can neither be marketed nor used in the EU as of 02 February 2025. These include:

- *Profiling to assess or predict the risk of a person committing a crime;*
- *Creation of facial recognition databases through automated image searches on CCTV or the internet;*
- *Social scoring leading to unfavourable treatment of natural persons;*
- *Biometric categorisation of unlawfully acquired datasets;*
- *Real-time remote biometric identification in public spaces, such as use of Facial Recognition Technology (FRT), with important exemptions in the area of law enforcement<sup>4</sup>;*
- *Emotion recognition at the workplace or educational institutions (except use for medical and safety reasons).*

The EU AI Office will publish further guidelines on AI system definition and prohibitions.



<sup>4</sup>Exemptions exist for the use of real-time remote biometric identification systems in publicly accessible spaces by law enforcement authorities or on their behalf. These are systems that automatically identify a natural person without its consent. Member States can fully or partially allow the use of such technologies in public spaces, within limits outlined in the EU AI Act (such as judicial authorisations), if they are used for the targeted search of a victim of abduction or a person that is suspected of having committed a criminal offence (as defined in Annex II of the EU AI Act), as well as for the prevention of a specific, substantial and imminent threat to the life or physical safety of citizens, such as a terrorist attack. Member States can however also set in place more restrictive rules. Regulation can hence differ from one EU Member State to another.



### 3. High-risk AI



**This is the most important category, because the EU AI Act defines rules for the deployment of high-risk AI systems.**

## “The EU AI Act defines rules for the deployment of high-risk AI systems”

Once the deployer has determined whether an AI system is at use, it is important to assess whether it classifies as high-risk as per the EU AI Act’s definition in Article 6:

1. the AI system is itself a product or a safety component of a product which is (1) covered by pre-existing legislation listed in Annex I of the EU AI Act and (2) required to go through a third-party assessment.

*Examples: As per Annex I, this concerns AI-enabled drones covered by Regulation 2018/1139, AI systems used in Aviation Security equipment covered by Regulation 300/2008, as well as AI-enabled wireless devices subject to Directive 2014/53<sup>5</sup>.*

2. and/or it is deployed in high-risk sectors as defined in Annex III of the EU AI Act.

*Examples include AI systems that are intended to be used:*

- ♦ *for biometric identification and emotion recognition, and which do not fall in the scope of prohibited practices. This includes biometric identification systems, which identify a natural person with a time delay (not in real-time) and without their active involvement through the comparison of a person’s biometric data with the biometric data contained in a reference database (see page 16)<sup>6</sup>. Biometric*

*verification and authentication systems (e.g. as part of access control or to unlock a mobile device – as described as of page 15) are not high-risk AI.*

- ♦ *as safety components in the management and operation of critical infrastructure.*
- ♦ *to evaluate a person’s access to (vocational) education and training.*
- ♦ *in employment and workers management, such as for recruitment purposes or for decision-making related to working conditions, task allocation, performance evaluation and contractual relationships.*
- ♦ *to evaluate and classify emergency calls.*
- ♦ *for risk assessments, such as evaluations of law enforcement authorities or on their behalf to assess the risk of a natural person to become a victim of criminal offence.*

## “Deployers, but also developers and distributors of high-risk AI systems, will have to comply with the different provisions of the EU AI Act as of 02 August 2026”

These provisions are further outlined in Chapter III of this Charter as of page 27.

But how to know for sure whether an AI system is high-risk or falls into a respectively regulated use case?

It is the responsibility of an AI system provider to document the assessment whether an AI system is high-risk or not before the system is placed on the market or put into service.

But it also depends on the use case. High-risk products and use cases are defined for deployers in the EU AI Act in Article 6 and Annexes I & III, but the Regulation is complex.

The European Commission will therefore develop guidance on the implementation of high-risk classification. Meanwhile, our cross-cutting criteria can provide deployers with a first orientation.

<sup>5</sup> The EU AI Office is expected to publish further guidelines on the interplay between the EU AI Act’s high-risk definition and existing product-related legislation.

<sup>6</sup> The EU AI Office is expected to publish further guidelines on AI system definition, prohibitions and high-risk classification.



## IV. Examples of possible low-risk and high-risk AI use cases

### DISCLAIMER

This document shall provide security companies with a first understanding of possible low-risk and high-risk systems and use cases. The information provided in this Charter does not replace system and use case specific risk assessments that should be conducted by the deployer to ensure compliance with the EU AI Act.

### Low-risk AI use cases



Many AI use cases in security services can be expected not to qualify as high-risk. Keeping the EU AI Act and our cross-cutting criteria in mind, the following use cases in security services can be expected to rather fall into the low-risk category:

#### 1. Risk analysis



By scraping through huge amounts of non-personal data from existing security infrastructure, such as video cameras, AI systems can provide clients with concrete intelligence about their

security measures and recommendations for improvement. When deploying such AI applications, security companies can provide very rapidly concrete, data-based intelligence and predictive analysis on trends and patterns such as:

- Historical patterns of visitor flows and movement.
- Peak times / days / months of visitors and criminal offences in the facility or neighbourhood.

- Respective vulnerability assessments of a facility, based on current security plans in place.

Such risk analysis can drive informed decision-making and help make security services more effective. Security companies can provide recommendations to offer a targeted package of solutions, such as staffing and deployment of specific technologies.

#### 2. Analysis of business operations



AI applications can also analyse the efficiency of internal business operations, based on data such as:

- Peak usage periods of certain business services.
- Facility management, for example energy-efficiency levels of buildings, products and car fleets.
- Visitor tracking.
- Data on occupational health and safety incidents.
- Impact of services provided for marketing purposes.

Internal business operations, and hence services offered to clients, can be adapted to be more cost-efficient, ecological and safer. Service impact assessments can be used for marketing purposes.

#### 3. Crowd management



AI-enabled CCTV can be used to track the number of people present at an event, automatically identify locations with a high density of visitors, analyse movement patterns of a crowd, as well

as bottlenecks that can create risks to the safety and security of visitors. Staff on the ground can then take respective measures – e.g. in access control or directing crowd movement.

These systems can be highly useful at mass events, such as football games or festivals, and are valuable to guide first responders and emergency aid during an incident. However, the deployment of such systems is likely to



qualify as high-risk use cases if they start including personal data in their analysis and output (for example, if the system starts collecting biometric data and combines it with non-personal data to produce certain outputs, e.g. biometric identification or categorisation).

#### 4. Biometric verification



Biometric verification systems are very distinct from biometric identification systems:

- Verification systems confirm that a specific person is who they claim to be by comparing biometric data of that individual to previously provided biometric data (Question: Is it you?).
- Identification systems identify an unknown person without their consent (Question: who is it? See page 16).

The EU AI Act's Annex III therefore classifies biometric identification systems as "high-risk", and not verification systems. Biometric verification can present a substantial enhancement of effectiveness and efficiency of access control, particularly at sensitive facilities such as Critical Infrastructure.

#### 5. Other use cases for AI-enabled analytics of non-personal data



The list of possible use cases of AI-enabled data analytics could be continued endlessly. Particularly as part of video surveillance services, the potential to provide more effective, accurate and quicker services is tremendous:

- **Alarm triage:** AI-enabled video cameras can be used to help triage real from false alarms in monitoring and alarm receiving centres (MARC). For instance, a camera may distinguish, based on shape and movement patterns, whether a reindeer just entered a facility's surveilled perimeter, or a human being. The system can hence vet the alarm, determine whether it is likely false, and provide a

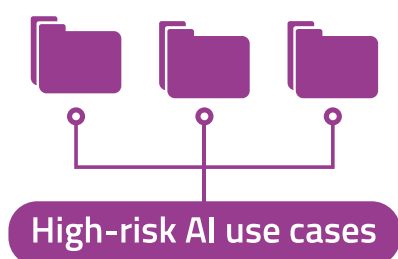
respective recommendation to the security officer in the MARC. This can reduce the time to respond to actual incidents, and improve both business operation efficiency and the level of protection provided to a client.

- **Object analysis:** similar to the alarm triage, AI systems can quickly analyse and classify certain detected objects. For example, they can analyse whether a certain vehicle is allowed to be in a restricted zone (e.g. based on a database/whitelist of "approved" license plates). In a more critical case, an AI-enabled drone detection system may quickly analyse whether a drone carries a potentially hazardous payload and analyse its speed and probable time of impact. Such intelligence can tremendously improve response time and decision-making in counter-drone measures.
- **Behaviour detection:** CCTV can be empowered by AI applications to identify suspicious behaviours, which are associated with criminal offences – e.g. movement patterns and other activities. AI systems can then provide a respective alarm, to be evaluated by security personnel on the ground or in a MARC before taking preventive action. Such use cases enhance security measures and enable rapid responses in case of critical situations.

The use of AI in video surveillance systems can however quickly fall in the category of high-risk depending on the data that is used, the level of human oversight / autonomy, and the output that is provided by the system.







High-risk AI use cases can provide substantial value in security services, but must guarantee compliance with the EU AI Act and this Charter.

The EU AI Act lays down many product categories and use cases, which automatically qualify as high-risk. Based on this legal definition (see page 13), which can also be mirrored against our cross-cutting criteria, the following use cases in security services can be expected to fall into the high-risk category:

### 1. Biometric identification



The EU AI Act clearly identifies biometric identification technologies as either largely prohibited (real-time identification in public spaces) or high-risk AI (post-remote identification)

systems. FRT systems are a typical biometric identification technology. For the purpose of identification, FRT systems make a comparison between an identified facial map of a natural person and a database of biometric data to which the natural person may not have given consent (in contrast with biometric verification or authentication system, which are based on data subject consent and are used in access control or when opening your mobile phone).

Deploying biometric identification systems in public spaces can bring substantial value for the search of terrorists and other specific persons of interest, and are hence of great benefit to law enforcement authorities and public security. They can, however, also come with substantial risks to EU citizens' fundamental rights – particularly because they can be used without the data subject's explicit consent.

Looking at our cross-cutting criteria, they provide autonomous recommendations that are developed in

a “black-box” based on the comparison with biometric data. The input is based on personal data, possibly without the data subject's consent. Their objectives are explicit, but their output can have legal consequences for natural persons. This makes the human oversight of this technology, which addresses all these risks, particularly important.

Real-time biometric identification deployments are therefore to a big extent prohibited by the EU AI Act, and the use of a time-delayed identification has been made subject to additional safeguards in comparison with other high-risk AI<sup>7</sup>. For additional guidance, the British Security Industry Association (BSIA) has published an ethical and legal use guide for FRT available at <https://www.bsia.co.uk/>, which is highly useful for a deployment that does not only guarantee mere compliance with law, but also adheres to important ethical values<sup>8</sup>.

### 2. Emotion recognition



Emotion recognition systems identify emotions or intentions of a natural persons based on their biometric data. Such technologies function in a similar way to other

behaviour detection systems, but their use is based on the evaluation of biometric data of a natural person, who may not have given consent to its use. Their deployment can be more efficient than low-risk AI-enabled behaviour detection systems. But similar to biometric identification systems, they fulfil all cross-cutting high-risk AI criteria and are clearly identified in the EU AI Act as either prohibited (e.g. at the workplace and in educational institutions) or high-risk AI systems with enhanced transparency obligations.

### 3. Prohibited items detection in Aviation Security



A typical example for AI-enabled systems in aviation security are “Automated Prohibited Item Detection Systems” (APIDS). These systems automatically

identify prohibited items in aviation security based on images and data they have been fed with by the

<sup>7</sup> For example, no decision shall be taken based solely on the output of these systems, and the output shall always be reviewed by at least two adequately qualified and authorised natural persons, except if Member States believe this requirement to be disproportionate in law enforcement use cases.

<sup>8</sup> Further to the BSIA's Guide, a new British Standard (BS 9347) is to be released which guides the security industry user towards safe and trustworthy policies for verification and identification, throughout the supply chain for facial recognition technology.

## “High-risk AI use cases can provide substantial value in security services, but must guarantee compliance with the EU AI Act and this Charter”

developers. The deployment of AI-enabled aviation security equipment can significantly enhance security measures and operational effectiveness at airports – if coupled with adequate human oversight. But AI-enabled detection systems like APIDS can also pose substantial risks, particularly due to the environment they operate in: failing to detect a prohibited item in the aviation security environment can have substantial consequences for public security. The EU AI Act therefore classifies them automatically as high-risk<sup>9</sup>, which also appears logic if we apply our cross-cutting criteria.

### 4. AI-enabled drones



AI is today an essential safety component in unmanned vehicles – especially in the case of autonomous drones. AI algorithms enable drones to operate autonomously, reducing the need for human intervention. Drones can further include AI-enabled sensors and detection systems that provide real-time intelligence to a security officer or to the autonomously flying drone itself. AI-enabled drones can help remote security officers take informed decisions in real-time. Officers can monitor large areas with several drones at the same time, without having to pilot them all and thereby make surveillance tasks much more efficient. Also, the integration of AI systems can make drone operations safer, as they can help the drone adapt to changing flight conditions, such as entrance into no-fly zones and weather. But the enhanced level of autonomy and risks to the physical environment make it necessary to make the deployment of AI-enabled drones subject to specific rules. For example, a malfunctioning autonomous drone poses a risk both to the people on the ground as well as to vehicles in the air. The EU AI Act therefore categorises all AI systems as “high-risk” that are a safety component of a product or which are themselves a product subject to the EU Drone Regulation, and which are required to go through a third-party assessment<sup>10</sup>.

### 5. HR management



The use of so-called algorithmic management at the workplace can substantially support task allocation and recruitment – especially in companies with a high number of employees.

→ **Task allocation:** AI-enabled analysis of business operations can provide recommendations to management on worker allocation in different services and shifts. There's hence a big potential to optimise the organisation of work, which can contribute to productivity gains benefiting companies and workers. At the same time, AI systems cannot consider the work done by workers from a human performance perspective like a human manager can, taking into account soft skills and inter-personal relationships. Human oversight is therefore key.

→ **Recruitment:** If they are based on trustworthy data, AI-enabled analytics can help better match job profiles with prospective candidates – for the benefit of companies, job seekers and inclusive workplaces.

Such use cases and associated opportunities bring likewise risks and have a potential impact on the worker, both in terms of task allocation as well as opportunities on the job market. Particularly in recruitment, depending on the programming of the system, AI can also lead to a systemic discrimination of certain workers groups. Outputs of the AI system can impact future career prospects, livelihoods of these persons and workers' rights. The use of AI for HR management is therefore automatically categorised as high-risk AI when these systems are intended to be used for the recruitment or selection of natural persons, or for management decisions affecting the workers' contractual relationship and task allocation. Importantly, deployers of these AI-systems must ensure, as per the EU AI Act, information of affected workers and their representatives prior to its deployment.

<sup>9</sup> Like all AI systems which are part of products regulated by Regulation No 300/2008 on common rules in the field of civil aviation security and required to go through a third-party assessment. The EU AI Office is expected to publish further guidelines on the interplay between the EU AI Act's high-risk definition and existing product-related legislation.

<sup>10</sup> The EU AI Office is expected to publish further guidelines on the interplay between the EU AI Act's high-risk definition and existing product-related legislation.

# Chapter II: Opportunities and risks of AI deployment in security services

Our use case examples show that the deployment of AI can bring many benefits to public security and European citizens. **The integration of AI into security services transforms security concepts, improves operational resilience of companies, makes security workers' missions safer, and leads to more effective security services.** But while AI technology holds great potential to empower security actors to better identify and counter criminal activity, its deployment also requires diligent risk assessments. This Chapter looks into the most important opportunities that AI-enabled services can bring to European citizens, businesses and workers, but also into main risk drivers and undesired outcomes.

**“When integrating AI into services, it shall bring added value by ensuring complementarity and synergy of people and technologies”**

## I. Opportunities

### 1. Higher security performance through synergy with human-centric services

**The integration of AI in security solutions is not an end in itself. When integrating AI into services, it shall bring added value by ensuring complementarity and synergy of people and technologies** – providing security workers with a “sixth sense” and translating it into an unprecedented level of security.

#### 1.1. Data-enabled identification, triage, and mitigation of security risks in real time

**New capabilities for detection, triage and response time to suspicious movements, intrusions or anomalies stand out as a fundamental advantage of integrating AI in security services:**

- ◆ Object-analysis and prohibited item detection systems based on AI can quickly analyse and classify detected objects or hazards.
- ◆ Behaviour detection and emotion recognition systems (optic, acoustic) can help identify unusual behaviours and speed up intervention for a better protection of public spaces and Critical Infrastructure.
- ◆ AI-enabled drones and C-UAS technology provide a highly valuable additional tool in the guarding and remote surveillance of Critical Infrastructure and public spaces, especially in large perimeters (e.g. train tracks, pipelines, offshore energy infrastructure, etc.).
- ◆ Remote biometric identification systems can bring substantial value for the targeted search of



terrorists, other specific persons of interest and vulnerable people.

- ♦ AI can help triage real from false alarm in MARCs and maintain consistent service quality levels.

All these use cases offer useful intelligence in real time that can provide security officers with an additional “sense”, improve security measures through enhanced decision-making, and shorten response time in case of an incident. Security services become more sophisticated and reach a new level of “intelligence”.

### 1.2. Enhanced adaptiveness of security solutions

**AI renders security services more agile and can adapt services to clients’ needs in real time.**

AI-enabled risk analysis can drive informed decision-making and target security solutions to the specific needs of a client. They ultimately strengthen the resilience of a client’s facility, prevent future incidents through predictive analysis, and enhance safety of workers and security officers.

In crowd management, AI can provide security service providers with rapid intelligence in challenging environments and informed decision-making in real time. They make crowd management more effective, enable quick decisions and adaptiveness of security and safety measures, and substantially enhance event security.

### 1.3. Workers’ empowerment through automation

**AI empowers security workers with new insights and information thanks to the automation of tasks.**

Biometric verification systems support workers in authenticating people and enforcing access control, particularly at sensitive facilities such as Critical Infrastructure.

Automated drones can help remote security officers take informed decisions in real time. Officers can monitor large and/or multiple areas with drone swarms without having to pilot all. Operations safety is supported through AI-enabled consideration of external perimeters, such as weather conditions.

Alarm triage prevents security officers from repeatedly validating disturbing false alarms (e.g. in certain weather conditions such as snow fall) and helps them focus on their main tasks – avoiding information overload. Any kind of AI-enabled data analytics and optical/acoustic sensors can reduce burden in security workers’ standard tasks and support decision-making.

### 1.4. Enhanced data protection and cybersecurity

**AI can enhance data protection and cybersecurity** through supporting analysts in accelerated threat and data access anomaly detection – saving valuable response time. AI can substantially support cyber risk assessments and help detect phishing, malware, and other malicious activities.

## 2. Benefits to companies and workers

Benefits of AI in security services are not mutually exclusive: many use cases are not only an opportunity for public security and the protection of clients, but also for security companies and workers.



### 2.1. Better safety and protection of workers

**A key asset of the use of AI is an enhanced level of protection of security workers.** AI-enabled risk analysis can take into account occupational hazards of security workers. AI enables workers to increasingly detect and validate risks remotely. AI-enabled drones and robots do not only provide security officers with a better overview of potential risks, but prevent them from entering hazardous environments.

### 2.2. Promotion of inclusive workplaces

The OECD<sup>11</sup> underlines that **the use of algorithmic management at the workplace can help increase diversity, inclusion, equality, and non-discrimination.** Trustworthy data is thereby crucial. The use of AI at the workplace must be based on relevant and high-quality data to fight bias or discrimination in the workplace. Algorithmic management can then promote more objective assessments of job applications, performance evaluations and bring better opportunities for recognition and promotion for workers who have traditionally suffered from bias in the labour market.

### 2.3. New job opportunities

**The enhanced empowerment and protection of workers in AI-enabled services can make the security services profession more attractive.** In its research, OECD found out that in sectors such as manufacturing or finance, the reduction of workers' time spent on

repetitive tasks gave them a greater opportunity of spending time on more strategic tasks<sup>12</sup>. Furthermore, tasks related to AI-enabled services may attract new worker groups, which are currently underrepresented in the European security services, including women and young people.

### 2.4. Optimisation of business operations and competitiveness

**Data-driven business operation optimisation can enhance operational resilience, help maintain quality in service, and allow intelligence-driven investments** - increasing competitiveness in the industry. AI can support operational processes to become more cost-efficient, ecological and safer with benefits for workers, security companies and clients, e.g. by better crew scheduling or patrol route planning.

## II. Risks

**Alongside these opportunities, it is important to recognise that the deployment of AI can entail risks.** Striking a balance between leveraging AI's potential and mitigating its risks requires careful consideration of ethical, legal, societal, and security-related implications of the deployment in question.

This Chapter gives a short overview of important categories of risks that are associated with the use of AI in security services.

<sup>11</sup> OECD (2023), *OECD Employment Outlook 2023: Artificial Intelligence and the Labour Market*, OECD Publishing, Paris, <https://doi.org/10.1787/08785bba-en>.

<sup>12</sup> OECD (2023), *OECD Employment Outlook 2023: Artificial Intelligence and the Labour Market*, OECD Publishing, Paris, <https://doi.org/10.1787/08785bba-en>.





## Risk drivers

When we talk about risks related to the deployment of AI, the public discourse often focuses on the possible negative impact of its use. We should however first focus on the risk drivers.

For deployers, there exist five main risk drivers, which reinforce each other and should be addressed holistically before and during the deployment of AI:

### 1. Lack of diligent risk management processes

AI is not any kind of technology. The absence of a diligent, use case specific risk management process during the life-cycle of an AI system's use can lead to non-compliance with relevant law (such as the EU AI Act or GDPR), and unexpected risks to the health, safety or fundamental rights of citizens and security staff.

### 2. Use of untrustworthy and biased data sets

Using untrustworthy data in AI deployments can lead to amplified biases in AI decisions, unreliable outputs and fundamental rights risks. It undermines explainability, accountability and trust in AI systems, potentially resulting in substantial reputational risks for deployers.

### 3. Lack of human oversight

Human oversight is central to the deployment of AI in security services. A lack thereof can be a consequence of understaffing or staff that isn't adequately trained or managed to effectively operate the system in the specific use case. Inadequate human oversight can lead to a loss of explainability of the AI system's functioning and output. Staff can over-rely on the system's output such as false positives or negatives. A lack of human oversight does not only limit, misguide and/or undermine human autonomy, but is a significant driver of risks to the health, safety and fundamental rights of citizens.

### 4. Lack of resilience

AI systems and their algorithms shall be resilient against physical manipulation and cyberattacks. Otherwise, their functioning and outputs can be influenced and disabled – leading to substantial risks, particularly in security service use cases.

### 5. Lack of AI governance

A dedicated AI governance policy should assign the accountable officer and set out a clear chain of processes and responsibilities – with the ultimate responsibility and accountability for good or misuse of AI to sit with the Board or governing body of the deployer. Without such a policy, there is a risk that those legally accountable may claim 'plausible deniability' and that management levels in the deployers' company took action without Board involvement.

## Risk categories

These risk drivers can translate in manifold, use case specific, material and immaterial risks. We summarise them here in different categories.

### 1. Risks to fundamental rights of citizens

**In the public debate, the general use of AI raises fears that fundamental rights may be disrespected** due to:

- ♦ a loss of human autonomy and explainability of AI systems;
- ♦ mistrust against different use cases and their intended purposes / objectives;

- ♦ concerns about data privacy and data sets used for the input of the AI system;
- ♦ infringement of important fundamental rights due to the system's output.

Violations of fundamental rights can be material or immaterial, including physical, psychological, societal, or economic harm. Risks associated with the use of AI for law enforcement purposes often include fears of mass surveillance and intrusive surveillance; breaches of data privacy; discriminatory security practices; and accountability in case of a system's malfunctioning and related consequences<sup>13</sup>. Safeguards against these risks are addressed in the EU AI Act and crucial for companies' ethical and legal use of AI in the security services (see Chapter III).

<sup>13</sup>[https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_EN.html)

## 2. Risks to workers' rights and occupational health and safety

**The use of AI can also present risks for workers.** This particularly concerns risks associated with algorithmic worker management tools<sup>14 15</sup> and include:

- ♦ Discrimination of workers due to the use of biased datasets in the deployment of algorithmic worker management systems during recruitment processes, contract renewals, task allocation, and access to training.
- ♦ Perception of a high-stress work environment including of a more intense work pace, increased complexity of tasks and information flows, and the feeling of constant monitoring, surveillance and evaluations.
- ♦ Reduction of human interaction with colleagues and supervisors if workers are asked to increasingly work in isolation.

The EU AI Act and other European legislation sets in place safeguards against these risks.

## 3. Reputational risks for companies

**Trust is central to the work of security services and to the use of AI.** The EU has published in 2019 Ethics Guidelines on the trustworthy use of AI, highlighting that each deployment must be legally sound, ethical, and robust in order to build trust<sup>16</sup>. Data from 2023 however confirms that public trust in the technology is still low<sup>17</sup>.

In Europe, public and media interest in AI has been high in the past years, also due to several incidents (see page 23). Often the spotlight falls on organisations that get things wrong. If a company lacks transparency about its use of AI, deploys inadequately skilled staff for AI oversight, and badly manages risks, leading to incidents, it can quickly be singled out as unethical and uncaring towards workers, customers, and citizens. As with any new technology, a single incident may be used

to generalise the potential risk and jeopardise or slow down its further development.

## 4. Security risks

**The use of AI in security services inherently holds security risks, especially if risk drivers are not adequately addressed.** Inadequate human oversight, as well as a lack in physical and cyber resilience of the system, can lead to important malfunctioning of the system with repercussions on public security:

- ♦ Inadequately qualified staff may not be aware of false negatives with important consequences, e.g. in airport security.
- ♦ Malicious actors may manipulate an AI system, both physically and by means of cyberattacks, to introduce a malfunction of the system and prepare a criminal action<sup>18</sup>.
- ♦ Inaccuracy and bias of training models as well as complexity of systems can lead to incorrect claims and outputs of the AI system (hallucinations<sup>19</sup>), leading to undesirable consequences and undermining trust in the system<sup>20</sup>.
- ♦ AI provides malicious actors with new tools and can be used for deep fakes<sup>21</sup> and cyberattacks<sup>22</sup>. They could further hack data in the AI system, such as biometric data, to undertake socially engineered cyberattacks and circumvent security protocols.

## 5. Secondary effects

**The use of AI systems can have secondary effects, which are easy to overlook prior to their deployment without proper risk management procedures.** For example, the use of smart GPS systems can significantly improve traffic flow in a city but may likewise lead to an increased and undesired use of minor roads in residential areas. The same goes for data-enabled security risk analysis. While it can significantly enhance protection and security of a certain premise, it could likewise have an impact on rents and insurance premiums in certain neighbourhoods.

<sup>14</sup> Baiocco, S., Fernández-Macías, E., Rani, U. and Pesole, A., *The Algorithmic Management of work and its implications in different contexts*, Seville: European Commission, 2022, JRC129749

<sup>15</sup> OECD (2023), *OECD Employment Outlook 2023: Artificial Intelligence and the Labour Market*, OECD Publishing, Paris, <https://doi.org/10.1787/08785bba-en>.

<sup>16</sup> <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

<sup>17</sup> [https://kpmg.com/xx/en/home/insights/2023/09/trust-in-artificial-intelligence.html#:~:text=AI%20trust%20and%20acceptance,depend%20on%20the%20AI%20application.&text=Three%20in%20five%20\(61%20percent,wary%20about%20trusting%20AI%20systems.&text=67%20percent%20report%20low%20to%20moderate%20acceptance%20of%20AI](https://kpmg.com/xx/en/home/insights/2023/09/trust-in-artificial-intelligence.html#:~:text=AI%20trust%20and%20acceptance,depend%20on%20the%20AI%20application.&text=Three%20in%20five%20(61%20percent,wary%20about%20trusting%20AI%20systems.&text=67%20percent%20report%20low%20to%20moderate%20acceptance%20of%20AI).

<sup>18</sup> <https://csrc.nist.gov/pubs/ai/100/2/e2023/final>.

<sup>19</sup> AI hallucinations define a situation where an AI system creates nonsensical, bizarre and inaccurate output. This may occur due to imperfect system modelling, complex interactions in deep learning systems, or if the system perceives patterns or objects that are either non-existent or imperceptible to a human.

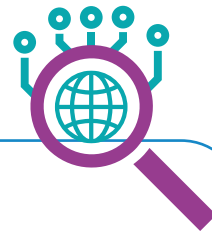
<sup>20</sup> <https://www.economist.com/science-and-technology/2024/02/28/ai-models-make-stuff-up-how-can-hallucinations-be-controlled>

<sup>21</sup> [https://www.dhs.gov/sites/default/files/publications/increasing\\_threats\\_of\\_deepfake\\_identities\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf)

<sup>22</sup> <https://www.wired.com/story/here-come-the-ai-worms/>.



## HOW WE CAN LEARN FROM PAST INCIDENTS AND EXISTING RISKS



### Clearview AI

In 2020, the New York Times<sup>23</sup> disclosed that Clearview AI, a US-based facial recognition software firm, amassed more than 3 billion facial images from social media, including additional data such as individuals' names, and stored them in a database. Access to the database was sold to law enforcement agencies, which allowed them to instantly identify an individual through a photo. Data Protection Agencies (DPA) raised important ethical and GDPR-related concerns about this business model, with DPAs in France and Germany instructing the company to cease its business activities and erase all personal data<sup>24</sup>.



### Childcare benefits scandal in the Netherlands

From 2013 to 2019, Dutch tax authorities utilized a self-learning algorithm to develop risk profiles aimed at detecting childcare benefits fraud. Acting upon the system's recommendations, authorities penalized families even on mere suspicion of fraud. Consequently, tens of thousands of families, often from lower-income backgrounds or ethnic minorities, were plunged into poverty due to substantial debts owed to the tax authority. The Dutch DPA outlined several breaches of the EU data protection regulations and imposed a fine of €3.7 million fine on the tax authority<sup>25</sup>.



### Physical intervention or cyberattacks manipulating behaviour of AI systems

Computer scientists from the US National Institute for Standards and Technology warn that AI systems can malfunction if an adversary finds a physical or cyber way to manipulate its decision making<sup>26</sup>. Autonomous vehicles learn from street images where and how to drive, while chatbots analyse conversation records to predict responses. However, training data can be poisoned by corrupted data. Malicious actors can conduct a cyberattack on AI systems to access sensitive information in order to misuse it. Input to the system can be physically altered to confuse or manipulate the system.



### The UK Post Office Scandal

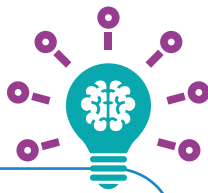
The UK Post Office's IT system, Horizon, erroneously accused hundreds of post office operators of financial discrepancies between 2000 and 2014, which had not been caused by human negligence but faults in the IT software. Over 900 employees were convicted of theft, fraud and false accounting – leading to innocent individuals facing false accusations and prosecutions. Numerous postmasters had reported issues with the software to management, and even the software provider was aware of bugs. Nevertheless, concerns were not heard by the UK Post Office. Although the Horizon software was not an IT system, this particular incident showcases the importance of human oversight, qualitative data and system algorithms, AI governance policies and risk management processes.

<sup>23</sup> <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

<sup>24</sup> <https://www.law.kuleuven.be/citip/blog/clearview-ai-illegally-collecting-and-selling-our-faces-in-total-impunity-part-ii/>

<sup>25</sup> <https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/#:~:text=In%202019%20it%20was%20revealed,on%20the%20system's%20risk%20indicators.>

<sup>26</sup> <https://csrc.nist.gov/pubs/ai/100/2/e2023/final>



**“Trust is central to the work of security services and to the use of AI”**

### WHAT WE CAN LEARN

These examples show how quickly the use of AI can derail into concrete risks. It is therefore important to address risk drivers holistically from the start:

- 1.** Risk management processes throughout the life cycle of an AI system’s use are key to identify and address use case specific risks and ensure compliance. For the use of FRT, the BSIA published a helpful “Guide to the ethical and legal use of Automated Facial Recognition”<sup>27</sup>.
- 2.** The use of AI systems that are based on trustworthy data and algorithms is critical to trustworthy output and ruling out fundamental rights violations.
- 3.** Qualitative human oversight with adequately skilled staff is key to ensure that a human can always evaluate the AI system’s recommendation and take a final, independent, decision.
- 4.** High levels of physical protection and cyber resilience through the AI system’s life cycle are crucial to protect citizens, users, and clients from the malfunctioning of an AI system.
- 5.** Clear reporting lines, processes and responsibilities as part of an AI governance policy are crucial for deployers to take action in case of malfunctioning or misuse of an AI system.



<sup>27</sup>[https://www.bsia.co.uk/zappfiles/bsia-front/public-guides/form\\_347\\_automated\\_facial%20recognition\\_a\\_guide\\_to\\_ethical\\_and\\_legal\\_use-compressed.pdf](https://www.bsia.co.uk/zappfiles/bsia-front/public-guides/form_347_automated_facial%20recognition_a_guide_to_ethical_and_legal_use-compressed.pdf)



## CoESS' MISSION

25

fundamental rights and principles related to non-discrimination, transparency and privacy. For CoESS, the human-centric deployment of AI also means that AI shall become a public good and serve European citizens in every dimension.

**4. Transparency and explainability:** the deployment of AI shall be transparent to the stakeholders concerned, as appropriate to its use case. The explainability of the functioning and output of AI systems is crucial, not only for the ethical and responsible use of AI, but also public understanding and trust.

**5. Data privacy:** data governance along the deployment's value chain shall ensure the protection of European citizens' data privacy rights enshrined in the EU Charter of Fundamental rights and GDPR.

**6. Physical and cyber resilience and safety:** AI systems and their use in security services shall be safe, resilient and secure to prevent, withstand and overcome incidents. Systems shall work in a repeatable and predictable way, and a consistent level of quality services shall be ensured throughout the AI systems deployment. Unintentional material and immaterial harm to workers and affected stakeholders shall be minimised and prevented.

**7. Accountability:** the entire value chain of the development and deployment of AI systems shall be accountable, according to their roles and legal requirements, for the proper functioning of AI systems.

**8. Sustainability:** the deployment of AI shall holistically contribute to the United Nations' Sustainable Development Goals, promoting inclusive growth, (ecologically) sustainable development and well-being. It shall be ensured that AI solutions are sustainable and environmentally friendly – duly considering operations' impact on the environment.

**“The deployment of AI should follow a value-based code of conduct”**

## II. First steps to ensure an ethical and responsible use of AI

The core purpose of this Charter is to provide deployers of AI systems in the security services with guidance on legal and voluntary requirements for the ethical and responsible use of AI which address the risks identified in Chapter II, based on CoESS' transversal value-set. Before deciding upon deploying an AI system and setting in place adequate measures to guarantee its responsible and ethical use, the deployer should take three preparatory steps in a multi-stakeholder approach<sup>32</sup>:

### Step 1: Identify the AI system

As a first step, the deployer should identify whether they are planning to actually use an AI system before purchasing it. Although AI systems should be labelled as such by the provider. This may not always be the case especially for systems that are marketed before enforcement of the EU AI Act. The deployer should therefore consider examining with the provider, internally and/or externally, the underlying technology that is applied in a certain use case. Based on the EU AI Act's "AI Definition" (see page 8), it likely qualifies as an AI system if it incorporates machine learning algorithms or deep learning models to produce outputs such as predictions, content, recommendations and decisions based on data input. A review of our cross-cutting criteria (see page 10) can help.

### Step 2: Assess applicable legal requirements and evaluate whether the AI system and the use case qualify as low-risk or high-risk as per the EU AI Act

Before each use, the deployer shall define the purpose and intended outcome of the AI systems' use and conduct an assessment to understand if the AI system and use case qualify as low- or high-risk. This assessment is crucial to comply with the EU AI Act and to use the AI responsibly and ethically. It should start with the following questions:

<sup>32</sup> CoESS recommends to assess and implement these requirements in a multi-stakeholder approach, including (among others) the responsible project managers, regulatory affairs managers and compliance experts, technical AI experts, data protection officers, HR, security experts both in physical and cybersecurity, as well as business unit managers of the service segment concerned. Such teams should be diverse, also to detect potential biases throughout the operations of an AI system. AI policies and codes of conduct must be a company board priority.



### Step 3: Assess the added value of deploying the AI system

Before using the AI system, the deployer should evaluate if the integration of AI in the specific use case adds any value, and identify its specific purpose and intended outcome. Next, the deployer should evaluate potential advantages, disadvantages and unintended outcomes of integrating AI into the service in question, assessing these against the overarching goal of improving its quality and effectiveness. This assessment should consider factors such as field-effectiveness, impact on working conditions and decision-making, qualification of workers and the need for upskilling, as well as cost-effectiveness.

## III. Requirements for the ethical and responsible use of AI

### DISCLAIMER

This document shall provide security companies with a first understanding of the EU AI Act and important codes of conduct prior to and during the use of an AI system. The information provided in this Charter does not replace system and use case specific risk and regulatory assessments that should be conducted by the deployer to ensure compliance with the EU AI Act

#### 1. Is the AI system or use case prohibited as per the EU AI Act (see page 12)?

**2. Does my company qualify only as a deployer or also provider of the AI system?** If the deployer adds their name on the AI system or makes modifications to the system or its intended use, then they would be qualified as an AI system provider<sup>33</sup> as per the EU AI Act, making them subject to additional legal obligations in the case of high-risk AI systems.

**3. Does the AI system or use case qualify as high-risk?** Our cross-cutting criteria can help to make a first assessment. To have legal certainty, the deployer should check:

- Whether the AI system in question is CE marked and registered in an official, publicly available EU database (available by 02 August 2026).
- Whether the use case falls into any of the high-risk categories defined in Annex III of the EU AI Act (see page 13).

**4. Are different AI systems combined in one use case** (e.g. installation of crowd management systems on an AI-enabled drone) and, if so, what is the impact on the low-risk vs. high-risk categorisation of the use case?

**5. If the AI system or use case does not qualify as high-risk, does the system in the use case interact with natural persons** and therefore does it bear transparency risks (see page 12)?

AI actors are accountable for the proper functioning of AI systems, based on their roles, the context, and consistent with the state of art. To ensure compliance with our value-set, the EU AI Act and other relevant legislation, this Charter recommends that deployers set out an AI governance policy that assigns legal responsibility and accountability for the good or misuse of AI to the Board or governing body of the deployer. Furthermore, the deployer shall develop in a multi-stakeholder approach<sup>34</sup> an internal code of conduct which sets in place the following measures:

<sup>33</sup> If the deployer adds their name or trademark on an AI system, makes a substantial modification to it or changes the intended purpose of the AI system (in comparison to the providers' instructions of use), the deployer may furthermore classify as a provider of a high-risk AI system as per the EU AI Act's Article 25, and hence comply with a much larger range of legal obligations that outlined in this Charter.

<sup>34</sup> CoESS recommends to assess and implement these requirements in a multi-stakeholder approach, including (among others) the responsible project managers, regulatory affairs managers and compliance experts, technical AI experts, data protection officers, HR, security experts both in physical and cybersecurity, as well as business unit managers of the service segment concerned. Such teams should be diverse, also to detect potential biases throughout the operations of an AI system. AI policies and codes of conduct must be a company board priority.





## RISK MANAGEMENT

Risk management systems are a legal obligation for high-risk AI as per EU AI Act, Art. 9

**Risks associated with the deployment of an AI system shall be adequately managed throughout its entire lifecycle and according to its intended purpose and context of use.** To this end, the deployer shall establish a risk management system to:

- ensure compliance with relevant law, including GDPR and the EU AI Act.
- identify and analyse known, reasonably foreseeable, and other possible risks that the AI system can pose to health, safety or fundamental rights of EU citizens and workers, as well as the security of clients when it is used according to its intended purpose, but also under conditions of reasonably foreseeable misuse;
- adopt appropriate and targeted, technically and physically feasible risk management measures designed to minimise the identified risks to a reasonably acceptable level;
- establish fall-back procedures and other adequate mitigation and control measures addressing risks that cannot be eliminated.

These measures shall consider all requirements listed in this Charter and adequately address the risk drivers and risk categories identified in Chapter II. Many international Standards<sup>35</sup> and Guidelines<sup>36</sup> exist to help operators conduct risk management processes.



## DATA GOVERNANCE

Data governance is a legal obligation for high-risk AI as per EU AI Act, Art. 10 & 26

**Deployers shall set in place diligent data handling practices:**

- Data governance must guarantee full compliance with GDPR.

- Adequate cyber and physical security of datasets, including personal data and sensitive data, must be ensured – including of relevant datacentres.
- The deployment of AI in security services must be based on trustworthy, robust, and qualitative data. To this end, due diligence policies and procedures in selecting AI systems shall ensure that providers have trained, validated and tested the AI system with input data that meets certain quality criteria and excludes potential bias, compliant with the EU AI Act. To the extent that the deployer exercises control over the input data, they shall ensure that it is relevant in view of the intended purpose of the high-risk AI system.

Data governance shall further ensure traceability of data processing, explainability of the AI system's output, auditability and accountability.



## HUMAN OVERSIGHT

Many measures related to human oversight are a legal obligation for deployers of high-risk AI systems as per the EU AI Act, Art. 4, 14 and 26

**Adequate human oversight of any AI system is central to the fulfilment of the values set out in this Charter.**

The EU AI Act therefore also rightly foresees in its Article 4 that already as of 02 February 2025, deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff. For the European security services, CoESS underlines that responsible staff must be enabled to fulfil the requirements set out in this Charter, **appropriate and proportionate to the specific use case.**



<sup>35</sup> Such as ISO/IEC 23894 "Artificial Intelligence – Guidance on Risk Management" and ISO/IEC 42001 "Artificial Intelligence Management System".

<sup>36</sup> These include the EU Self-Assessment List for Trustworthy AI, available at: <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>; the UK Portfolio of AI assurance techniques, including the Anekanta AI Risk Intelligence System for biometric and high-risk AI, available at <https://www.gov.uk/ai-assurance-techniques>; and the US National Institute of Standards and Technology AI Risk Management Framework, available at <https://www.nist.gov/itl/ai-risk-management-framework>



Deployers shall take appropriate technical and organisational measures to ensure they use AI systems in accordance with the instructions for use accompanying the systems.

The deployer shall further ensure that staff overseeing AI systems is empowered through adequate training, qualification, technical and operational measures, including delegation of authority, to:

- comprehend instructions for use, the intended purpose and use case of an AI system, and conclusions drawn from risk management;
- understand the relevant capacities and limitations of the AI system;
- be aware of the level of accuracy, robustness and cybersecurity of the AI system – including any known and foreseeable circumstances that may have an impact on accuracy, robustness and cybersecurity;
- know conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights of affected persons due to the system's output;
- be able to explain the intended purpose of data collection to affected persons and to provide information on how the AI's output was reached;
- be aware of changes to the AI system which may impact its performance<sup>37</sup>;
- be able to duly monitor the AI system's operation, including the detection and management of anomalies, dysfunctions and unexpected performance;

- remain aware of the possible tendency of automatically relying or over-relying on the output produced by an AI system;
- correctly interpret the high-risk AI system's output and take autonomous decisions;
- decide, in any particular situation, not to use the AI system or to otherwise disregard, override or reverse its output;
- intervene in the operation of the AI system and set in place relevant fall back procedures and other adequate mitigation and control measures in case of an incident;
- inform the provider and relevant public authorities in case of an incident.

In the case of high-risk AI deployments, the EU AI Act's Article 14 requires diligent policies, processes and policies of the deployer to ensure legal compliance. Special human oversight provisions exist for biometric identification use cases<sup>38</sup>.

Deployers shall strongly take into account the potential need to upskill workers prior to the deployment of AI. The security industry should work closely with public authorities to prepare for the integration of AI systems into services and, if needed, adapt training frameworks that reflect requirements for AI literacy, skills, qualification, and licensing requirements. Social Dialogue can play an important role to lead this process and to ensure the responsible use of AI in the workplace, for the benefit of occupational health, safety and job quality.

**“Social Dialogue can play an important role to ensure the responsible use of AI in the workplace.”**

<sup>37</sup> People trained in human oversight can also reduce the risk of biased decisions arising from previously unbiased AI systems that became biased during their use. As appropriate in the use case, workers should be trained to align the AI deployment with human-centred values throughout the operation.

<sup>38</sup> In the case of biometric identification use cases, the EU AI Act Article 14.5 prescribes that no action or decision is taken by the deployer on the basis of system's output unless it has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority. Exemptions from this provision exist for use cases that fulfil law enforcement purposes.





## RESILIENCE

Measures related to AI system accuracy, robustness and cybersecurity are a legal obligation for deployers of high-risk AI as per the EU AI Act, Art. 15

**In line with the EU AI Act and other relevant legislation, the AI system provider has the responsibility to design and develop their products in a way that appropriately ensures its accuracy, resilience and cybersecurity.**

Deployers shall, however, also take the necessary technical, operational and organisational measures to respond to pertinent physical and cybersecurity risks, in line with a previous risk assessment, intended purpose and use case environment. AI systems shall be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately, repeatably and predictably, and do not pose unreasonable safety risk. It is therefore important that physical and cyber risks be addressed in a holistic way<sup>39</sup>.

- Physical manipulation of AI systems can lead to erroneous outputs and respectively significant security and safety risks. Physical protection measures can include access control and access monitoring to physical AI hardware, infrastructure and data storage; maintenance of optimal environmental conditions for the AI systems' functioning; and implementation of secure procedures for AI system disposal. Staff should be properly trained to implement these measures. A special focus should be further given to data centre security and resilience.

- Cyberattacks on the AI system during its operation can “poison” the training data set or models or present important data privacy and protection risks. Standards<sup>40</sup> and guidelines<sup>41</sup> exist in the field of cyber resilience, which can be useful for deployers of AI systems.

Especially in the security services sector, **exemplary physical and cyber resilience of the AI system is crucial to avoid incidents and put the reputation of the deployer at risk.** To overcome incidents and ensure business continuity, deployers shall set in place fall-back procedure and contingency plans. Security officers may have to replace the AI system's operation in the respective use case. Data can be stored across geographically dispersed locations to minimize the impact of localized physical disruptions and cyber-attacks.



## RECORD-KEEPING

Record-keeping is a legal obligation for high-risk AI as per EU AI Act, Art. 12 & 26

**Automatic record-keeping is, as per the EU AI Act, a mandatory technical feature of high-risk AI systems and deployers, as far it is under the latter's control.** It is important for deployers to ensure the respect of values related to traceability, explainability, and accountability. In proportion to the intended purpose of the system, the documentation of AI systems' operational performance ensures that the deployer can trace, explain and justify how decisions are made. Importantly, accountability demands clear records to establish who is responsible for AI operations (and potential modifications to it), ensuring transparency and (voluntary) compliance with regulatory requirements.

The EU AI Act foresees a record-keeping period of at least six months when high-risk AI systems are deployed and sets additional obligations when deploying remote biometric identification systems.

<sup>39</sup> See for further information the White Paper of CoESS and the International Security Ligne on “Cyber-Physical Security and Critical Infrastructure”, available at <https://www.coess.eu/>.

<sup>40</sup> ISO Standard “ISO/IEC CD 27090 Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems” addresses AI system cybersecurity risks.

<sup>41</sup> Such as the EU Joint Research Centres “Guiding Principles to address cybersecurity requirements for high-risk AI systems”, available at <https://op.europa.eu/en/publication-detail/-/publication/7d0a4007-51dd-11ee-9220-01aa75ed71a1/language-en>. CoESS and Euralarm have published more general Cybersecurity Guidelines for the Security Industry, available at <https://www.coess.eu/>.



## TRANSPARENCY AND EXPLAINABILITY

Diverse transparency measures are a legal obligation for high-risk and limited-risk AI as per EU AI Act, Art. 13, 26, 49, 50 and 71

**Compliance with GDPR is a key aspect of the ethical and responsible use of AI.** But there is more: AI deployers shall commit to transparency, explainability and responsible disclosure regarding AI systems.

- **Transparency towards persons that are exposed to the AI system:** humans must always be aware that they are interacting with an AI system and/or are subject to its output in a way that is lawful and in proportion to the specific use case. Transparency information should be meaningful, appropriate to the context, consistent with the state of the art, and be accessible for people with disabilities. Affected persons must be enabled to understand and, if necessary, challenge, the output and related decisions. Worker representatives must be informed about the deployment of AI systems in workers' management. As appropriate to the use case and AI system, the deployer should set in place transparent and accessible complaint mechanisms that respect specific rights and remedies for individuals unlawfully impacted by AI systems.
- **Transparency towards the greater public:** when using high-risk AI systems on behalf of public authorities, the deployer must register it in a European publicly accessible database<sup>42</sup> as per Art. 49 and 71 of the EU AI Act. To increase transparency and public trust in the use of AI in security services and, if deemed adequate and safe in the specific use case, deployers may voluntarily register any high-risk AI deployment, also if they are not deploying it on behalf of a public authority.
- **Transparency towards authorities:** Deployers should make AI documentation available for inspection by competent authorities to ensure compliance with legal requirements. Deployers of post-remote biometric identification systems must submit annual reports to relevant market surveillance and data protection authorities.

- **Explainability:** It is further important that deployers are in the position to explain the intended purpose of data collection to affected persons and to provide clear and simple information on how the AI's decisions were reached in proportion to the use case and with respect to intellectual property, privacy and security. To this end, deployers should, if needed, request the developer to provide model cards or otherwise human readable guidance on how the AI system makes decisions.

**Deployers should further promote understanding among the public and policymakers on the use of AI in security services.** This can be achieved by promoting this Charter.



## FUNDAMENTAL RIGHTS IMPACT ASSESSMENT

Fundamental Rights Impact Assessments are a legal obligation for deployers of high-risk AI as per the EU AI Act, Art. 27

**In addition to the legally mandatory data protection impact assessment as per the GDPR, Article 25, deployers of high-risk AI who are public authorities or who provide services on behalf of public authorities must conduct a Fundamental Rights Impact Assessment** as per Article 27 of the EU AI Act before using a high-risk AI system for the first time. Such an assessment must cover:

- a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose;
- a description of the period of time within which, and the frequency with which, the high-risk AI system is intended to be used;
- the categories of persons likely to be affected by its use in the specific context;
- the specific risks of harm likely to impact affected persons;
- a description of human oversight measures in line with instructions for use;

<sup>42</sup> This EU database is regulated as per Article 71 of the EU AI Act. Information to be entered by deployers of AI systems is listed in Annex VIII. The database shall be established and managed by the European Commission in the course of xxx.

- risk management measures, incl. internal governance and complaint mechanisms.

Deployers of high-risk AI systems who provide services on behalf of public authorities must notify their national authorities about this assessment and shall repeat the assessment if they consider that any of these elements are not up to date during use. Deployers who do not deploy high-risk AI systems on behalf of public authorities should also consider doing such an assessment if they have reasons to believe that their use case may come with unlikely, but possible, fundamental rights impacts. The EU AI Office may develop guidelines to help deployers fulfil their legal obligations.

As appropriate to each use case, deployers may consult affected stakeholder groups on such Fundamental Rights Impact Assessments.



## DUE DILIGENCE

**Deployers of AI systems should follow due diligence policies when buying AI systems:**

- verify that the AI system is trained on high-quality, diverse, and representative datasets.
- confirm the AI system's conformity with important cybersecurity requirements, at least those set out in relevant law such as the EU AI Act and the EU Cyber Resilience Act.
- use only AI systems that are transparent in their decision-making processes and include adequate instructions for use<sup>43</sup> which allow, among others, an easy understanding of the system's intended purposes and necessary human oversight measures; the level of accuracy, including its metrics, robustness and cybersecurity; as well as foreseeable circumstances and misuses that can lead to fundamental rights risks.

Providers of high-risk AI system must register their products in the EU Database referred to in the EU AI Act's Article 71. Deployers shall use only high-risk systems that are duly registered.



## INVOLVE WORKERS IN THE INTEGRATION OF AI INTO SERVICES

**In addition to legal obligations to inform workers about the use of AI at the workplace, the employer should actively involve security officers in the deployment of AI systems into services.**

This could include awareness raising activities, including seminars, webcasts and other information material, to provide transparency on which AI systems are used and on why and how they are intended to be used. As part of human oversight measures, and appropriate to each use case, workers must receive an adequate understanding of what can and cannot be expected from the system in order not to overwhelm workers and avoid complacency. Benefits of AI risk analysis should reach each employee, e.g. through the sharing of statistics and recommendations with regards to operational health and safety.

Deployers can establish dedicated contact points where workers can raise ethical concerns over the functioning and use of certain AI systems, protected as per relevant labour law and possibly via an ethics or internal review committee.



## IN CASE OF DOUBT: REACH OUT TO COMPETENT AUTHORITIES

**Internal codes of conduct and AI policies should foresee that deployers work actively with competent authorities in case of doubts about legal certainty and requirements set out in this Charter.** Also, if the employer has reason to consider that the use of the AI systems may present any material or immaterial risk to affected persons, they should inform the system providers and relevant market surveillance authority, and suspend the deployment of the system. In case of an incident with a high-risk AI system, competent authorities must be informed.

**“This Charter recommends that deployers set out an AI governance policy”**

<sup>43</sup>For high-risk AI system compliant with the EU AI Act provisions in Article 13.



## Chapter IV: Checklist

The EU AI Act will become applicable in a stepped approach, with most provisions applying as of 02 August 2026. Much of the implementation of, and compliance with, the EU AI Act depends however on Guidelines to be published by the European Commission's EU AI Office, Standards to be developed by CEN/CENELEC, the enforcement framework to be set up by national authorities.

But if you are already deploying AI systems in your services, or are planning to do so, there are ways to be on top of that wave and use this Charter to set in place AI governance frameworks that guarantee ethical and responsible use of AI in your services.

Here's a checklist that can help you:

- #1** Set up an internal AI governance & leadership team, processes and responsibilities in a multi-stakeholder approach. 
- #2** Identify the possible AI systems in question as well as their intended use and purpose in your service offering. 
- #3** Get an understanding of the legal frameworks and standards applicable to your use case and confirm compliance deadlines. 
- #4** Assess the possible risk profile of your AI system and use case, respective legal obligations and the added value of deploying the AI system in the specific use case. 
- #5** Engage with your national authorities and / or legal experts and confirm your internal assessment. 
- #6** Get inspired by this Charter and build an internal code of conduct. 
- #7** Purchase your AI system in a due diligence approach and upskill your AI leadership team. 
- #8** Conduct a risk assessment and set in place a risk management process for each individual use case. 
- #9** Prepare adequate measures for each individual use case according to the values and requirements set out in this Charter AND THE EU AI ACT, and upskill your workforce respectively if needed. 
- #10** Continuously review your AI governance, monitor the regulatory environment and incident involving high-risk AI, and engage with the EU AI Office, regulatory bodies in your country, Standardisation bodies, industry associations and the AI community to stay informed about the latest trends, guidelines, standards and legal developments. 

# Annex: Repository of useful guidelines and standards

## → Legal text of the EU AI Act:

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

## → EU Guidance

- ♦ Follow the EU AI Office:  
<https://digital-strategy.ec.europa.eu/en/policies/ai-office>
- ♦ Follow the EU AI Pact:  
<https://digital-strategy.ec.europa.eu/en/policies/ai-pact>
- ♦ Follow the European AI Alliance:  
<https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance>
- ♦ EU Guidelines on Trustworthy AI:  
<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
- ♦ EU Joint Research Centre “Guiding Principles to address cybersecurity requirements for high-risk AI systems”:  
<https://op.europa.eu/en/publication-detail/-/publication/7d0a4007-51dd-11ee-9220-01aa75ed71a1/language-en>
- ♦ EU Self-Assessment List for Trustworthy AI :  
<https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>

## → International Guidance

- ♦ OECD’s definition of an AI system:  
<https://oecd.ai/en/wonk/ai-system-definition-update>
- ♦ International Association of Privacy Professionals (IAPP) AI Resource Center:  
<https://iapp.org/>
- ♦ UK Portfolio of AI assurance techniques:  
<https://www.gov.uk/ai-assurance-techniques>
- ♦ US National Institute of Standards and Technology AI Risk Management Framework:  
<https://www.nist.gov/itl/ai-risk-management-framework>

## → Security Industry Guidance

- ♦ British Security Industry Association (BSIA): Automated Facial Recognition – A guide to ethical and legal use:  
<https://www.bsia.co.uk/>
- ♦ CoESS & Euralarm Cybersecurity Guidelines for the Security Industry:  
<https://www.coess.eu>





#### → **European Standards**

Follow the CEN-CENELEC Joint Technical Committee 21 “Artificial Intelligence”:

<https://www.cenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/>

#### → **International Standards**

- ◆ ISO/IEC 5339:2024 “Information technology — Artificial intelligence — Guidance for AI applications”:  
<https://www.iso.org/standard/81120.html>
- ◆ ISO/IEC TS 8200:2024 “Information technology — Artificial intelligence — Controllability of automated artificial intelligence systems”:  
<https://www.iso.org/standard/83012.html>
- ◆ ISO/IEC 22989:2022 “Information technology — Artificial intelligence — Artificial intelligence concepts and terminology”:  
<https://www.iso.org/standard/74296.html>
- ◆ ISO/IEC 23894 “Artificial Intelligence – Guidance on Risk Management”:  
<https://www.iso.org/standard/77304.html>
- ◆ ISO/IEC TR 24028:2020 “Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence”:  
<https://www.iso.org/standard/77608.html>
- ◆ ISO/IEC TR 24030:2024 “Information technology — Artificial intelligence — Use cases”:  
<https://www.iso.org/standard/84144.html>
- ◆ ISO/IEC TR 24368:2022 “Information technology — Artificial intelligence — Overview of ethical and societal concerns”:  
<https://www.iso.org/standard/78507.html>
- ◆ ISO/IEC TR 27563:2023 “Security and privacy in artificial intelligence use cases — Best practices”:  
<https://www.iso.org/standard/80396.html>
- ◆ ISO 30434:2023 “Human resource management — Workforce allocation”:  
<https://www.iso.org/standard/68711.html>
- ◆ ISO/IEC 38507:2022 “Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations”:  
<https://www.iso.org/standard/56641.html>
- ◆ ISO/IEC 42001 “Artificial Intelligence Management System”:  
<https://www.iso.org/standard/81230.html>



Acting as the voice of the **security industry**

Confederation of European Security Services

**Private security services in Europe** provide a wide range of essential services, both for **private** and **public clients**, ranging from **Critical Infrastructure facilities** to **public spaces** and **supply chains**.

**coess.eu**

**Confederation of European Security Services**

Avenue des Arts 56

B-1000 Brussels

Belgium