European Commission

# CERIS Workshop on Artificial Intelligence in Security Research

**WI-FI Network**: BAO100wifi
**Password**: welcomebao100

Brussels | 23th March 2023

# Welcome address

Marta Cygan, Director HOME, F2, DG HOME, European Commission

Brussels | 23th March 2023

# Panel 1: Proposed AI Act and its implications for law enforcement

**Moderator:** Martin Übelhör, DG HOME F2
Yordanka Ivanova, DG CNCT A2
Daniel Camara, La gendarmerie nationale FR
Donatella Casaburo, ALIGNER project
Saskia Bayerl, AP4AI project
Laurens Hernalsteen, CEN CENELEC
Stéphane Duguin, The CyberPeace Institute

Brussels | 23th March 2023

SHAPING EUROPE'S DIGITAL FUTURE

# The proposed AI Act and its relevance for law enforcement

Yordanka Ivanova,
Legal and policy officer
European Commission , DG CNECT A2

# Proposal for a Regulation on AI

## A single EU law for AI in the 27 EU Member States

- Two main objectives: address **risks to safety and fundamental rights** and **create a EU single market for AI**
- “Classic” internal market harmonized rules for the **placing on the market, putting into service and use of** AI
- **Horizontal in scope**: public and private sector
  - Excluded: military, research
- Without prejudice and complementary to existing EU law (e.g. data protection, criminal procedural law)

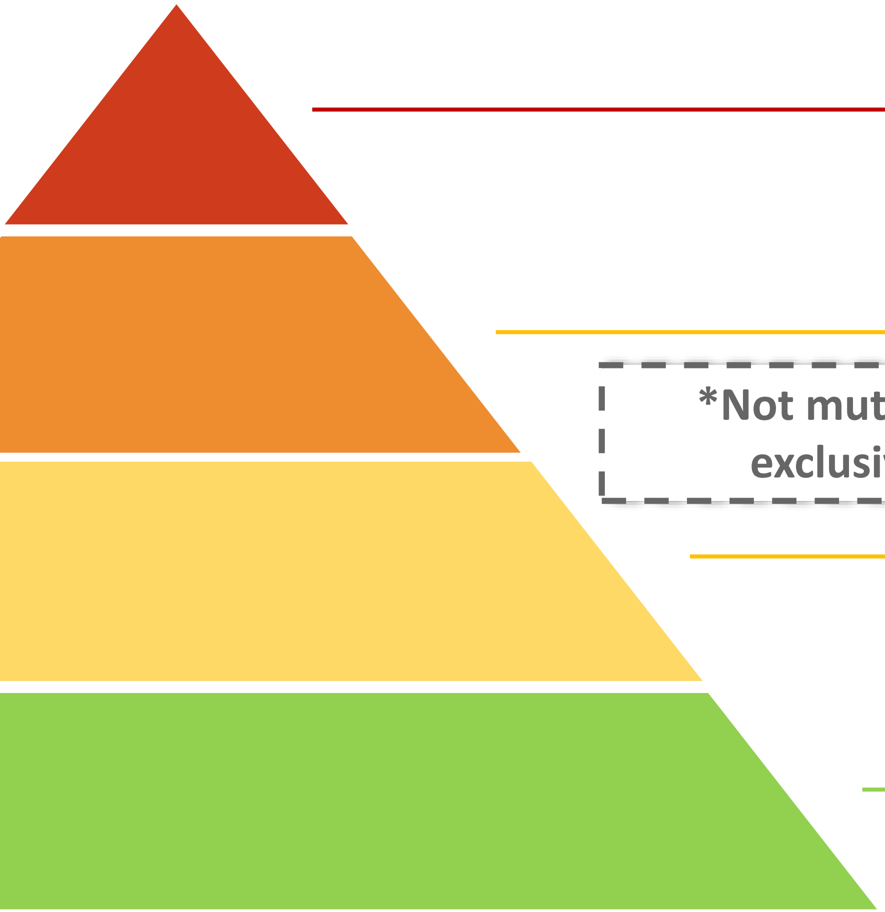
## Innovation-friendly and risk-based legislation

- Provide **legal certainty** to operators and stimulate **trust** in the market
- No overregulation: designed to intervene only where strictly needed following a risk-based approach

## Creates a level playing field for EU and non-EU players

- Applicable independent of origin of producer or user

# A risk-based approach to regulation



*Not mutually exclusive

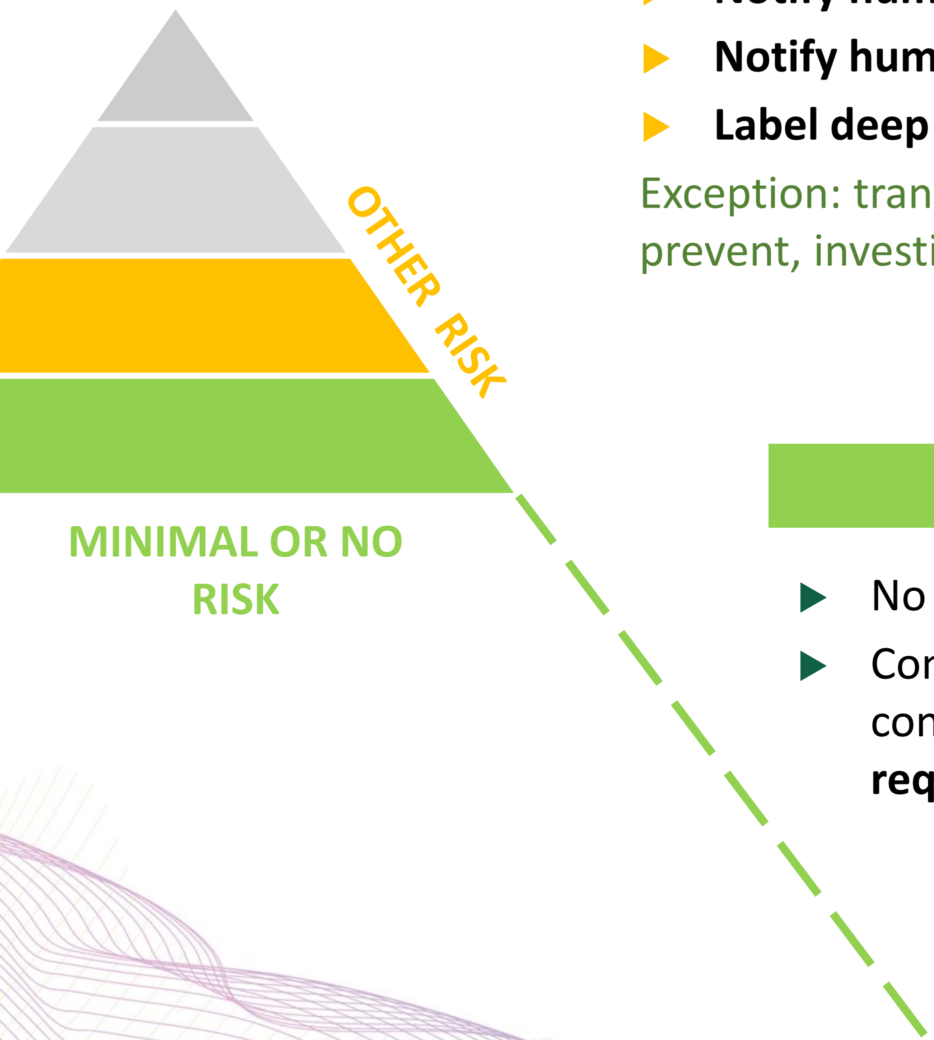
**Unacceptable risk**
e.g. social scoring — **Prohibited**

**High risk**
e.g. recruitment, medical devices, law enforcement — **Permitted** subject to compliance with AI requirements and ex-ante conformity assessment

**AI with specific transparency obligations**
(e.g. Chat bots, deep fakes) — **Permitted** but subject to information/transparency Obligations

**Minimal or no risk** — **Permitted** with no restrictions

# Most AI systems will not be high-risk (Titles IV, IX)



## New transparency obligations for certain AI systems (Art. 52)

- **Notify humans** that they are **interacting with an AI system**
- **Notify humans** that **emotional recognition or biometric categorisation systems**
- **Label deep fakes**

Exception: transparency obligations do not apply when authorised by law to detect, prevent, investigate and prosecute criminal offences

## Possible voluntary codes of conduct for AI (Art. 69)

- No mandatory obligations
- Commission and AI Board to encourage drawing up of codes of conduct intended to foster the **voluntary application of requirements to low-risk AI systems**

# High-risk Artificial Intelligence Systems (Title III, Annexes II and III)

Certain applications in the following fields:

## 1 AI SAFETY COMPONENTS OF REGULATED PRODUCTS

(e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation

## 2 CERTAIN (STAND-ALONE) AI SYSTEMS IN THE FOLLOWING FIELDS

- ✓ Biometric identification and categorisation of natural persons
- ✓ Management and operation of critical infrastructure
- ✓ Education and vocational training
- ✓ Employment and workers management, access to self-employment
- ✓ Access to and enjoyment of essential private services and public services and benefits
- ✓ Law enforcement
- ✓ Migration, asylum and border control management
- ✓ Administration of justice and democratic processes

**NB!** Not all use cases in the law enforcement sector are high-risk, but only a few explicitly listed in Annex III. The Commission can amend the list to keep it future-proof, following a common methodology and impact assessment.

# Annex III, 6 - Law enforcement

*Art. 3(40) AIA: defined as in the Law Enforcement Directive*

The following AI systems **intended to be used by ‘*law enforcement authorities*’:**

a) for making **individual risk assessments of natural persons** in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences

b) **polygraphs** and similar tools or to detect the **emotional state** of a natural

c) for detection of **deep fakes**

d) for **evaluation of the reliability of evidence** in the course of investigation or prosecution of criminal offences

e) **predicting the occurrence or reoccurrence of an actual or potential criminal offence** based on i) profiling of natural persons or ii) assessing personality traits and characteristics or past criminal behaviour of natural persons or groups

f) for **profiling of natural persons in the course of detection, investigation or prosecution** of criminal offences

g) for **crime analytics** regarding natural persons, allowing law enforcement authorities to search **complex related and unrelated large data sets** available in different data sources or in different data formats in order **to identify unknown patterns or discover hidden relationships in the data**

# Annex III, 7 - Migration, asylum and border control management

The following AI systems **intended to be used by ‘competent public authorities’:**

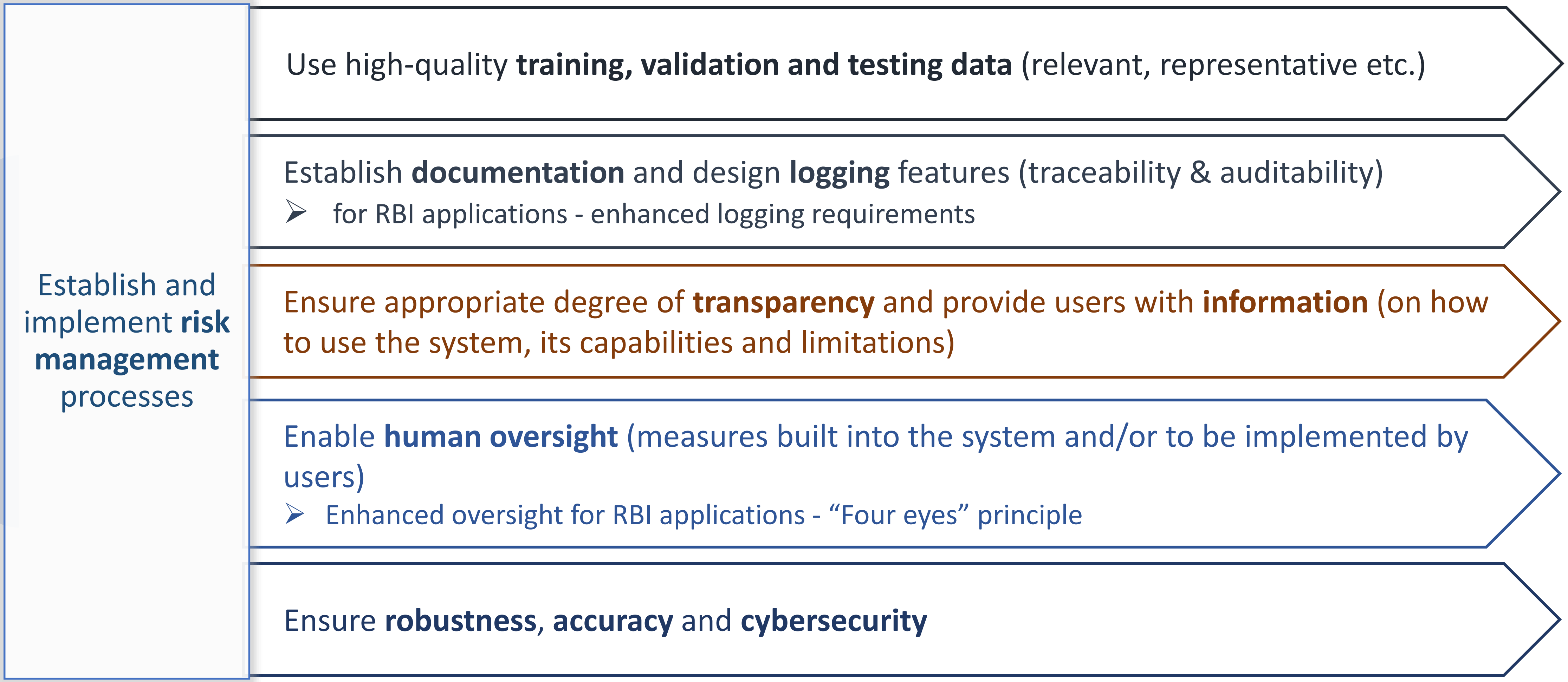
a) **polygraphs** and similar tools or to **detect the emotional state** of a natural person

b) to **assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person** who intends to enter or has entered into the territory of a Member State

c) for the **verification of the authenticity of travel documents and supporting documentation of natural persons** and detect non-authentic documents by checking their security features

d) for the **examination of applications for asylum, visa and residence permits and associated complaints** with regard to the eligibility of the natural persons applying for a status.

# Requirements for high-risk AI (Title III, chapter 2)



Establish and implement **risk management** processes

Use high-quality **training, validation and testing data** (relevant, representative etc.)

Establish **documentation** and design **logging** features (traceability & auditability)

- ➢ for RBI applications - enhanced logging requirements

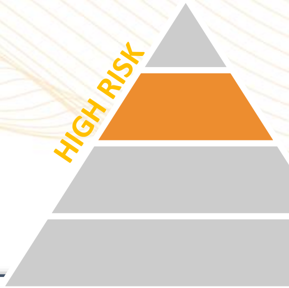
Ensure appropriate degree of **transparency** and provide users with **information** (on how to use the system, its capabilities and limitations)

Enable **human oversight** (measures built into the system and/or to be implemented by users)

- ➢ Enhanced oversight for RBI applications - “Four eyes” principle

Ensure **robustness**, **accuracy** and **cybersecurity**

# Obligations of operators of high risk AI systems



**Provider obligations**
**(incl. Tech providers or LEAs developing in-house)**

- Undergo **conformity assessment** to check compliance with the requirements (**self-assessment** for Annex III except for RBI) - time-limited derogation possible for public security - art. 47
- Implement **quality management** system in its organisation
- Draw-up and keep up-to-date **technical documentation**
- **Register** stand-alone high risk AI system in public EU database (no disclosure of instructions of use not to jeopardize security/investigation)
- Conduct **post-market monitoring** and take **corrective action**
- **Report serious incidents and malfunction** that infringe fundamental rights
- **Collaborate** with market surveillance authorities (enhanced confidentiality and security safeguards for LEAs)

**User obligations**
**(in-house AI or bought off the shelf)**

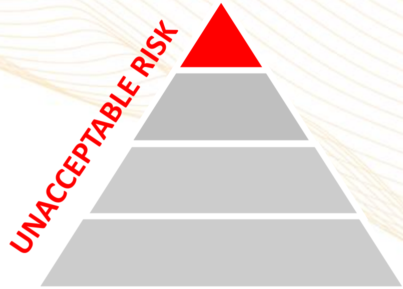
- Ensure **human oversight** and operate AI system in accordance with the **instructions of use**
- **Monitor** operation for possible risks
- **Inform the provider or distributor about any serious incident** or any malfunctioning
- Use the information given by the provider for the **data protection impact assessment** (where applicable)

⚠ **Existing legal obligations** for users continue to apply (e.g. LED, criminal procedural law – see also recital 31)

# Why does it matter for law enforcement authorities?

- *Opaque, unpredictable and biased AI systems seriously affecting fundamental rights **can be challenged in court and proclaimed illegal** (e.g. CJEU PNR judgement)*
- *Being 'high-risk' does not mean use is prohibited: on the contrary the AI Act requirements aim to address exactly those challenges and provide **a product certification scheme for trustworthy AI***
- ***Public trust and oversight** important for society to accept AI use in highly sensitive areas like law enforcement*
- *Good quality, secure and reliable AI systems also **important for LEAs to do effectively their daily job***
- *Tech providers will bear the main burden for compliance, but if LEAs developing in-house **EU harmonised standards will help demonstrate compliance***
- ***Regulatory sandboxes** to provide safe environment for innovation and experimentation with bespoke advice and tailored application of the act by the competent supervisory authorities (Articles 53 and 54)*

# AI practices that contradict EU values are prohibited (Title II, Article 5)



✗ **Subliminal manipulation** resulting in physical/ psychological harm

✗ **General purpose social scoring by public authorities**

✗ **Exploitation of children or mentally disabled persons** resulting in physical/psychological harm

✗ **Real-time remote biometric identification for** law enforcement purposes in publicly accessible spaces (with exceptions)

# Remote biometric identification (RBI)
# (Title II, Art. 5, Title III - Art. 6, Annex 3 (1)(a)

**Prohibited <u>use</u> of real-time RBI systems for law enforcement purposes in publicly accessible spaces (Art. 5)**

**Exceptions permitted for :**

- Search for victims of crime
- Threat to life or physical integrity or of terrorism
- Serious crime (EU Arrest Warrant)

**Ex-ante authorisation** needed by judicial authority or independent administrative body subject to strict safeguards and conditions
**National law** needed to allow the exceptions

**<u>Putting on the market</u> of RBI systems (real-time and post, public and private uses in any place - Annex III, point 1 a)**

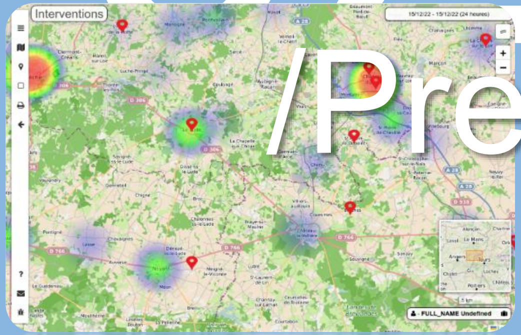
- **Requirements for high-risk systems**
- **Ex ante third party conformity assessment** by market surveillance authority
- Enhanced logging requirements
- "Four eyes" principle for human oversight

# Thank you

European Commission

# 01 /Needs

# 02 /Present



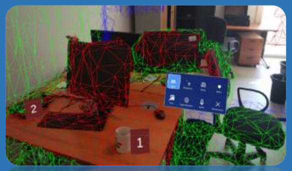
# 03 /Future

CENTRE FORENSIQUE D'INTELLIGENCE ARTIFICIELLE
CFIA
PÔLE JUDICIAIRE DE LA GENDARMERIE NATIONALE

# 01 /Needs

> “Before, It was hard to find clues; today is hard to discriminate what is important and what is not! Too much data is available!!!”

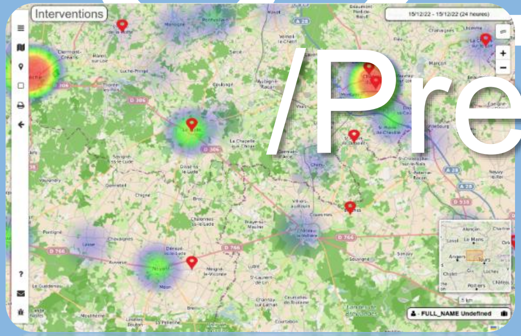
- Big data treatment
- Transcription
- Translation
- Large criminal networks analysis
- Safe communication methods
- Encription/Decription
- Preventive maintenance
- Human resources optimization
- .....



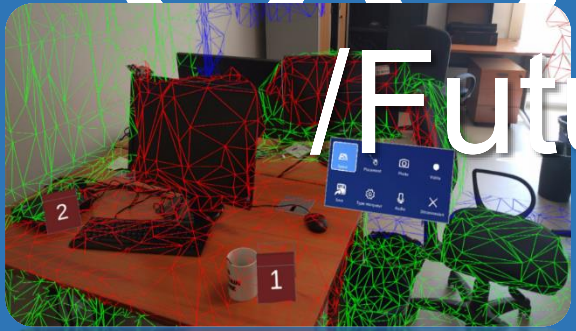
CENTRE FORENSIQUE D'INTELLIGENCE ARTIFICIELLE
CFIA
POLE JUDICIAIRE DE LA GENDARMERIE NATIONALE

## 01 /Needs

## 02 /Present



## 03 /Future



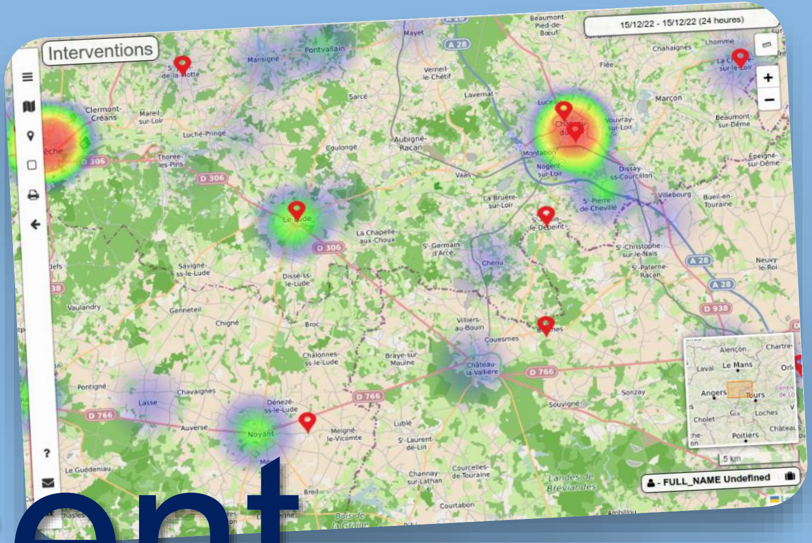
CENTRE FORENSIQUE D'INTELLIGENCE ARTIFICIELLE

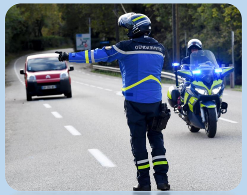
CFIA

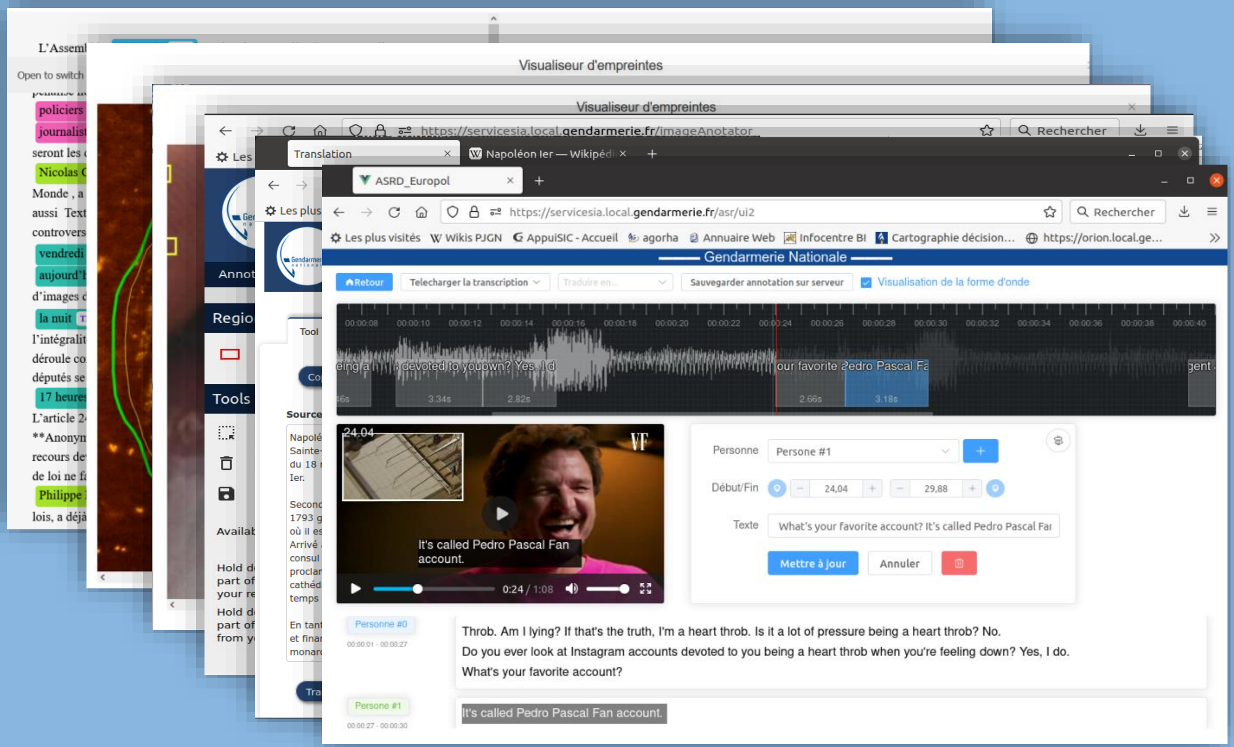
POLE JUDICIAIRE DE LA GENDARMERIE NATIONALE

# 02

# /Present






Visualiseur d'empreintes
https://servicesia.local.gendarmerie.fr/imageAnotator
Translation
Napoléon Ier — Wikipédi
ASRD_Europol
https://servicesia.local.gendarmerie.fr/asr/ui2
Gendarmerie Nationale
Retour
Telecharger la transcription
Traduire en...
Sauvegarder annotation sur serveur
Visualisation de la forme d'onde
Tools
Regio

Personne: Persone #1

Début/Fin: 24,04 – 29,88

Texte: What's your favorite account? It's called Pedro Pascal Fa

Mettre à jour | Annuler

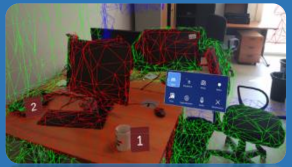
It's called Pedro Pascal Fan account.

Personne #0 (00:00:01 - 00:00:27)

Throb. Am I lying? If that's the truth, I'm a heart throb. Is it a lot of pressure being a heart throb? No. Do you ever look at Instagram accounts devoted to you being a heart throb when you're feeling down? Yes, I do. What's your favorite account?

Persone #1 (00:00:27 - 00:00:30)

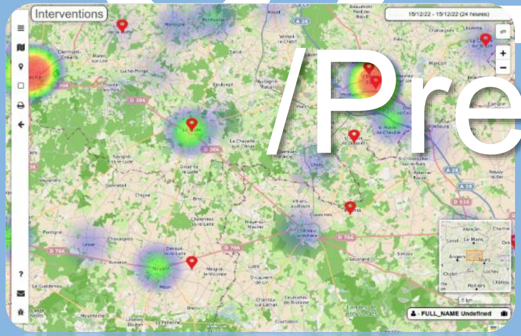
It's called Pedro Pascal Fan account.



CENTRE FORENSIQUE D'INTELLIGENCE ARTIFICIELLE
CFIA
PÔLE JUDICIAIRE DE LA GENDARMERIE NATIONALE

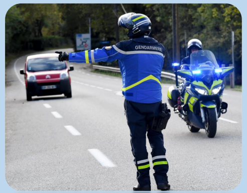
# 01 /Needs

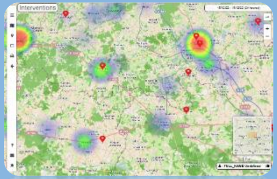
# 02 /Present



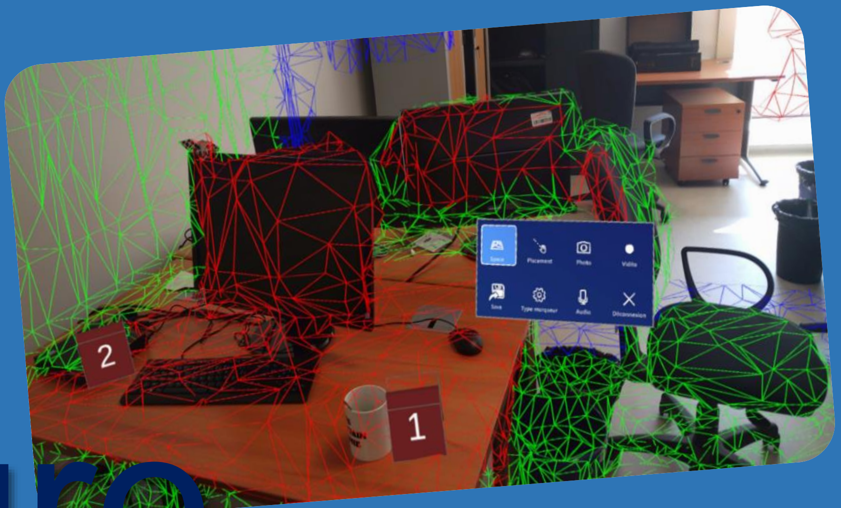
# 03 /Future

CENTRE FORENSIQUE D'INTELLIGENCE ARTIFICIELLE
CFIA
POLE JUDICIAIRE DE LA GENDARMERIE NATIONALE





# 03 /Future



- Virtual Environments (AR/VR)?
  - Crime scene representation/understanding
- Large Language Models?
  - Virtual Investigator assistants!
- Quantum Computing?
- What is CERTAIN
  - THE NEED TO FOLLOW AND KEEP UPDATED WITH TECHNOLOGICAL ADVANCES

CENTRE FORENSIQUE D'INTELLIGENCE ARTIFICIELLE
CFIA
POLE JUDICIAIRE DE LA GENDARMERIE NATIONALE

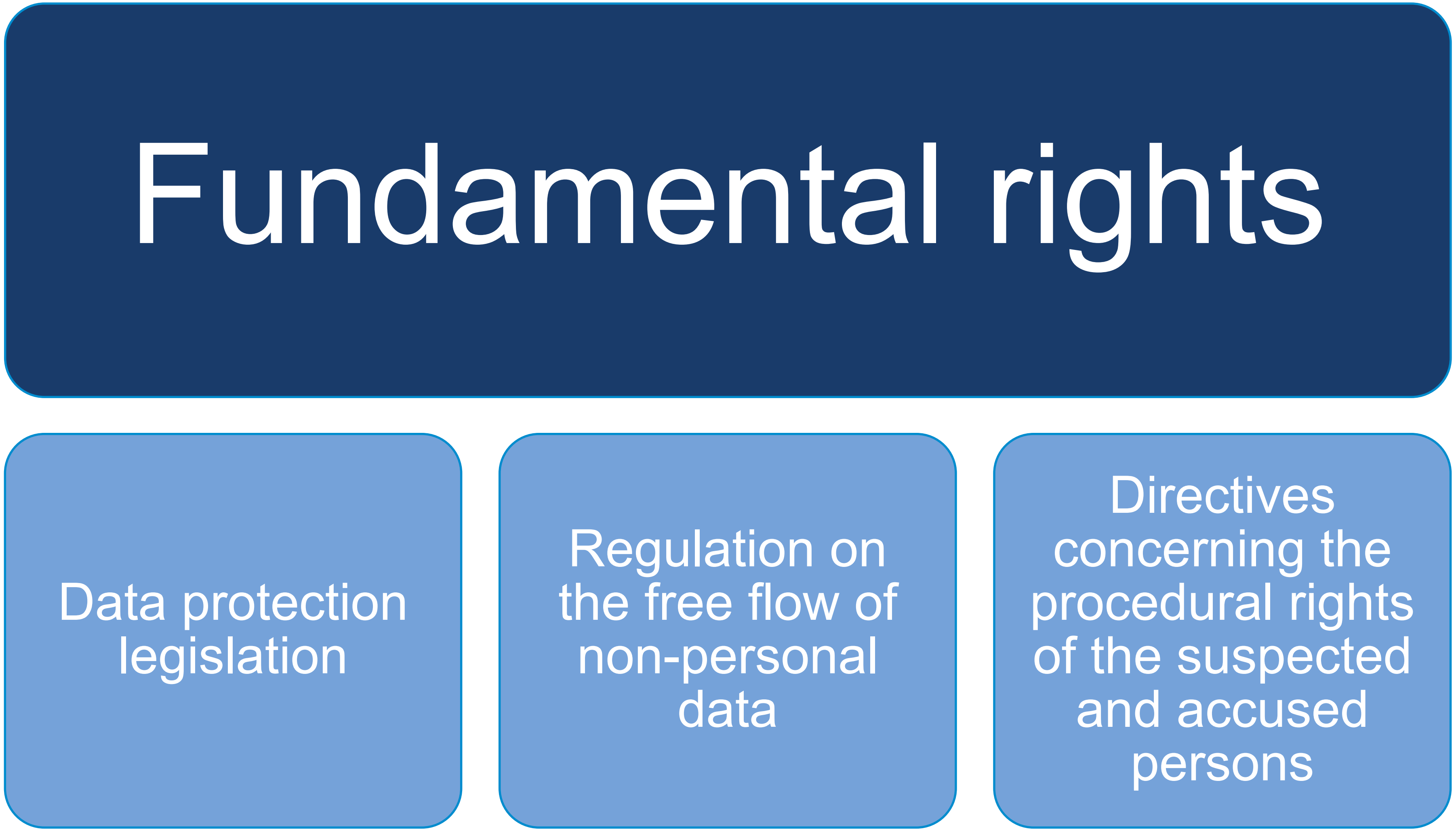
ALIGNER

# The legal framework for law enforcement AI

Donatella Casaburo, KU Leuven Centre for IT and IP Law (CiTiP)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101020574 .

# The EU legal framework



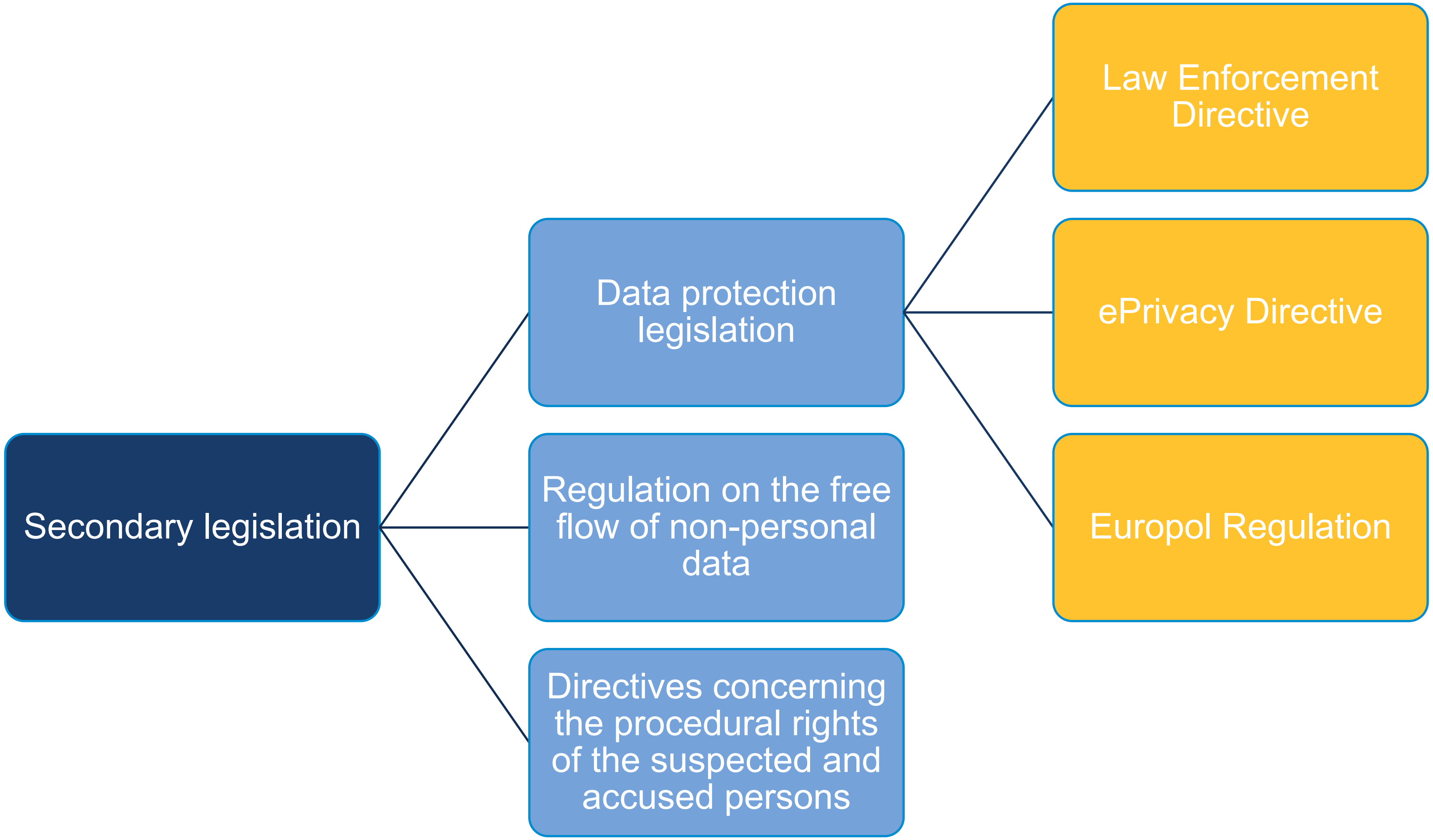
Fundamental rights

Data protection legislation

Regulation on the free flow of non-personal data

Directives concerning the procedural rights of the suspected and accused persons

# Secondary legislation



Secondary legislation

Data protection legislation

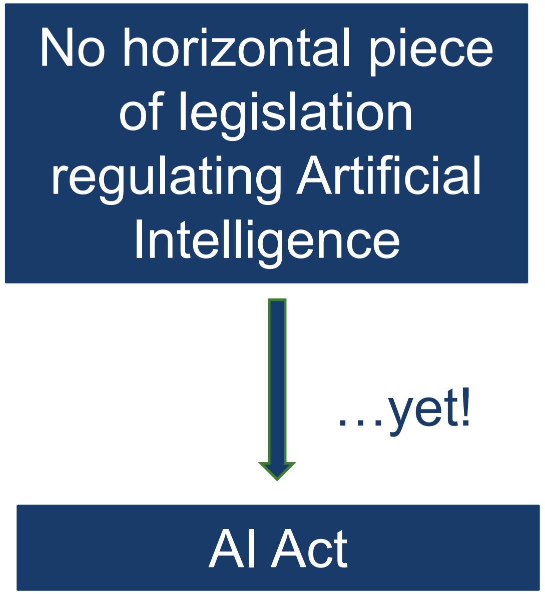
Regulation on the free flow of non-personal data

Directives concerning the procedural rights of the suspected and accused persons

Law Enforcement Directive

ePrivacy Directive

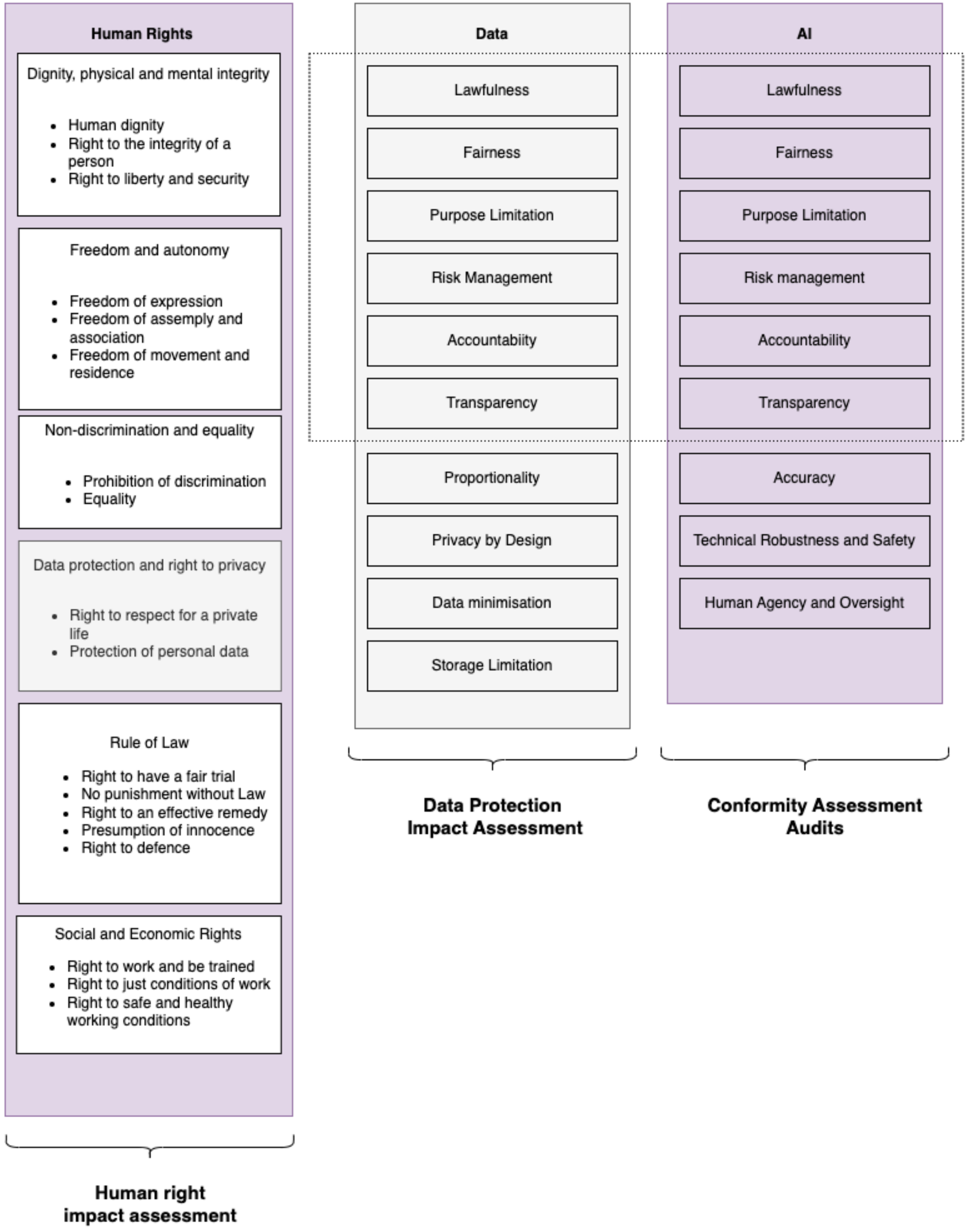
Europol Regulation



No horizontal piece of legislation regulating Artificial Intelligence

…yet!

AI Act



**Human Rights**

Dignity, physical and mental integrity

- Human dignity
- Right to the integrity of a person
- Right to liberty and security

Freedom and autonomy

- Freedom of expression
- Freedom of assemply and association
- Freedom of movement and residence

Non-discrimination and equality

- Prohibition of discrimination
- Equality

Data protection and right to privacy

- Right to respect for a private life
- Protection of personal data

Rule of Law

- Right to have a fair trial
- No punishment without Law
- Right to an effective remedy
- Presumption of innocence
- Right to defence

Social and Economic Rights

- Right to work and be trained
- Right to just conditions of work
- Right to safe and healthy working conditions

**Human right impact assessment**

**Data**

Lawfulness

Fairness

Purpose Limitation

Risk Management

Accountabiity

Transparency

Proportionality

Privacy by Design

Data minimisation

Storage Limitation

**Data Protection Impact Assessment**

**AI**

Lawfulness

Fairness

Purpose Limitation

Risk management

Accountability

Transparency

Accuracy

Technical Robustness and Safety

Human Agency and Oversight

**Conformity Assessment Audits**

# Legal Taxonomy

popAI developed a three high-level classes legal taxonomy:

The three levels to three broad functions of the laws reviewed: the protection of human rights, the protection of data (title: Data), and the protection of individuals from AI-related risks.

This classification aims to simplify the categorization of regulations that apply to AI in order to enable to

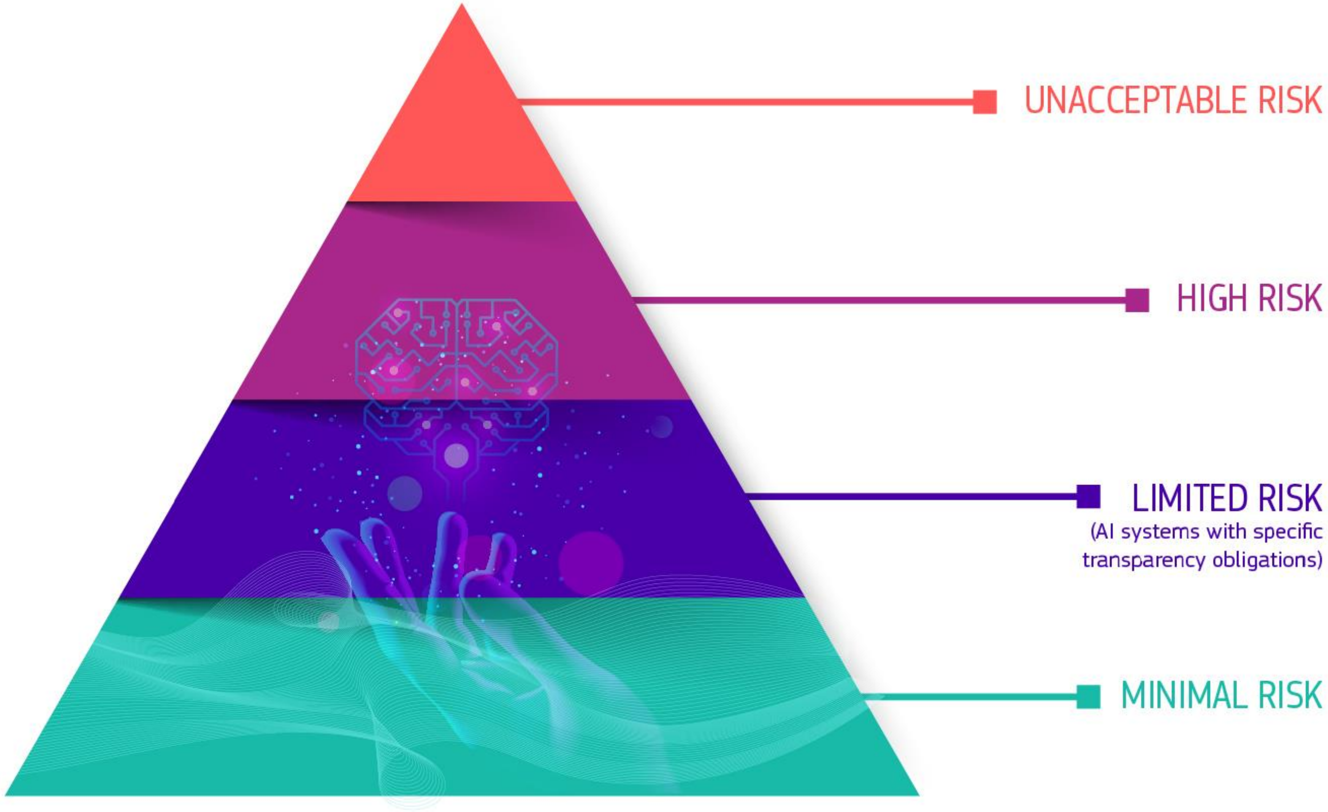
1) better compare how regulations address social concerns,

2) identify areas and intersection of areas that are currently not covered by binding and non- binding instruments and

3) promote a unified approach that merges human rights, data and AI related concerns.

# The AI Act: risk-based approach

Four categories of AI systems



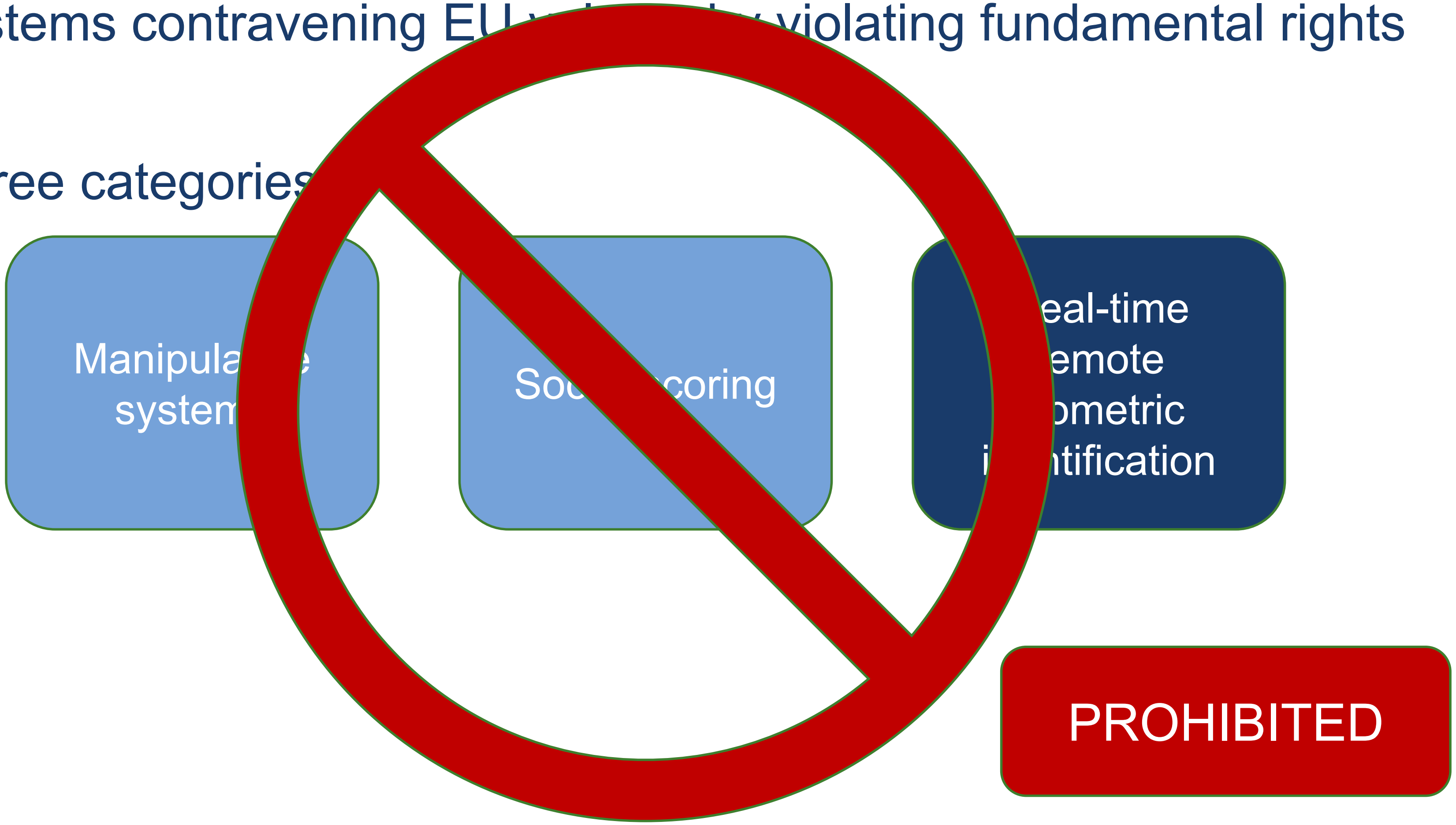
ALIGNER

Source: European Commission, ‘Regulatory Framework Proposal on Artificial Intelligence’ (Shaping Europe’s Digital Future)

# First category: Unacceptable risks

AI systems contravening EU v... violating fundamental rights

Three categories



Manipula e
system

Soc coring

eal-time
emote
ometric
i ntification

PROHIBITED

# ‘Real-time’ remote biometric identification

‘Real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement

**Identification system** = AI system designed with the purpose of identifying  natural persons at a distance, by matching their biometric data with those contained in a reference database

**Real-time** = The identification process, from the moment of the collection of data to that of the identification in itself, has to occur in real time, or without any significant delay

**Publicly accessible spaces** = Physical place accessible to the public

**Law enforcement purposes** = Prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties

# ‘Real-time’ remote biometric identification

‘Real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement

- The prohibition applies to AI systems placed on the market
  - ⇒ EU vendors can sell the identification systems to third countries
- The prohibition applies to AI ‘real-time’ identification
  - ⇒ ‘post’ identifications systems are not prohibited but considered as high-risk
- The prohibition does not apply to actors using remote biometric identification for non-law enforcement purposes
  - ⇒ ‘Real-time’ remote biometric identification systems used for other purposes (e.g., crowd control or public health) are only subject to the GDPR

Source: Michael Veale and Frederik Zuiderveen Borgesius, ‘Demystifying the Draft EU Artificial Intelligence Act’

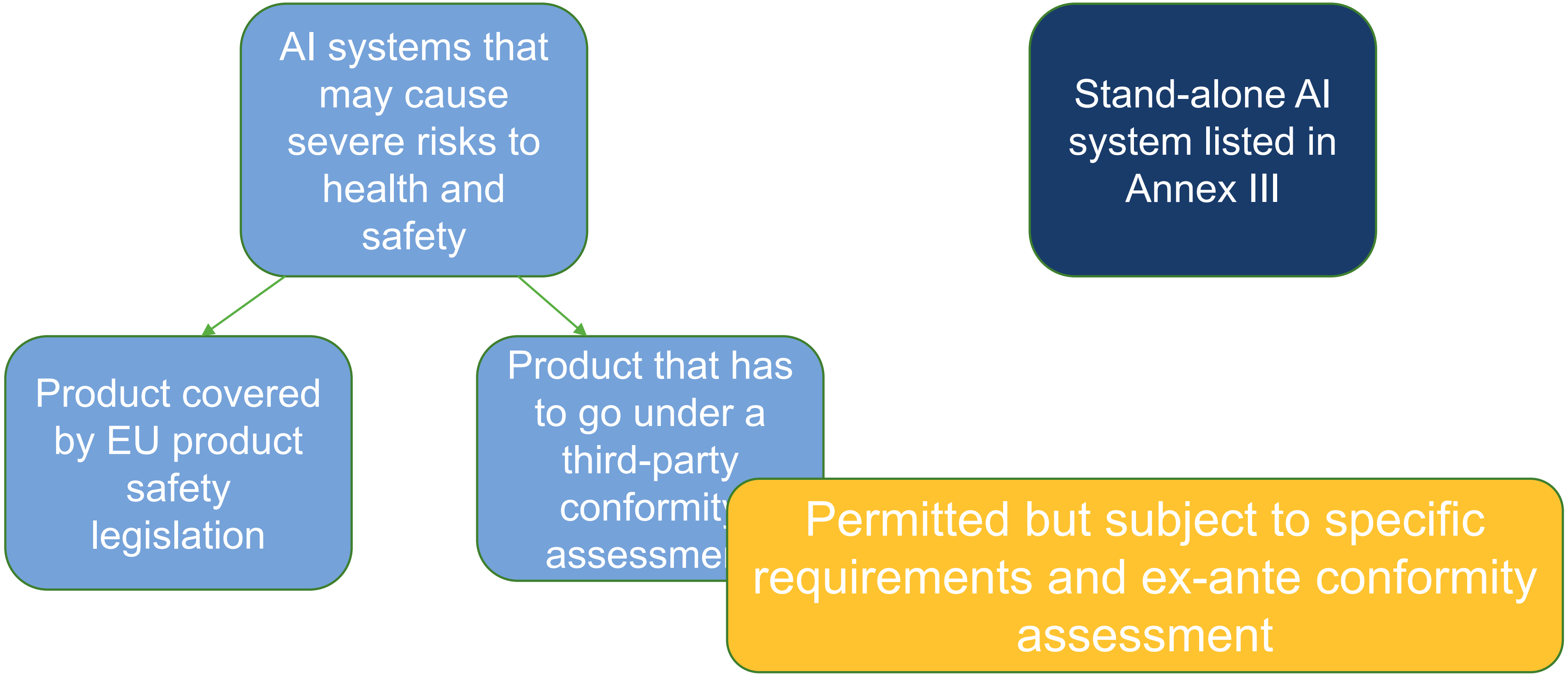
# ‘Real-time’ remote biometric identification - Exemptions

Participation in a criminal organization; terrorism; trafficking in human beings; sexual exploitation of children and child pornography; illicit trafficking in narcotic drugs and psychotropic substances; illicit trafficking in weapons, munitions and explosives; corruption; fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests; laundering of the proceeds of crime; counterfeiting currency, including of the euro; computer-related crime; environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties; facilitation of unauthorized entry and residence; murder, grievous bodily injury; illicit trade in human organs and tissue; kidnapping, illegal restraint and hostage-taking; racism and xenophobia; organized or armed robbery; illicit trafficking in cultural goods, including antiques and works of art; swindling; racketeering and extortion; counterfeiting and piracy of products; forgery of administrative documents and trafficking therein; forgery of means of payment; illicit trafficking in hormonal substances and other growth promoters; illicit trafficking in nuclear or radioactive materials; trafficking in stolen vehicles; rape; arson; crimes within the jurisdiction of the International Criminal Court; unlawful seizure of aircraft/ships; sabotage.

# Second category: High-risk

AI systems that pose significant risks to the health and safety or fundamental rights of persons

Two categories



AI systems that may cause severe risks to health and safety

Product covered by EU product safety legislation

Product that has to go under a third-party conformity assessme

Stand-alone AI system listed in Annex III

Permitted but subject to specific requirements and ex-ante conformity assessment

# Annex III

Eight categories, the most relevant of which are

(1) **Biometric identification** and categorization of natural persons, including ‘real-time’ and ‘post’ remote biometric identification

(2) **Law enforcement**, including predictive policing tools, polygraphs or similar instruments, tools to detect deep fakes, systems used to evaluate the reliability of criminal evidence and, in general, profiling tools and systems used for crime analytics using large datasets to identify unknown patterns

(3) Migration, asylum and **border control** management

(4) **Administration of justice** and democratic processes

# Thank you for your attention!

Donatella Casaburo
donatella.casaburo@kuleuven.be
KU Leuven Centre for IT & IP Law (CiTiP) - imec
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium
http://www.law.kuleuven.be/citip

www.aligner-h2020.eu

The sole responsibility for the content of this publication lies with the authors. It does not necessarily represent the opinion of the European Union. Neither the REA nor the European Commission are responsible for any use that may be made of the information contained therein.

I would never trust them. If the PEGASUS surveillance software could be used at state level with impunity and without consequence against non-terrorist individuals, there would be nothing to stop the police from doing the same.

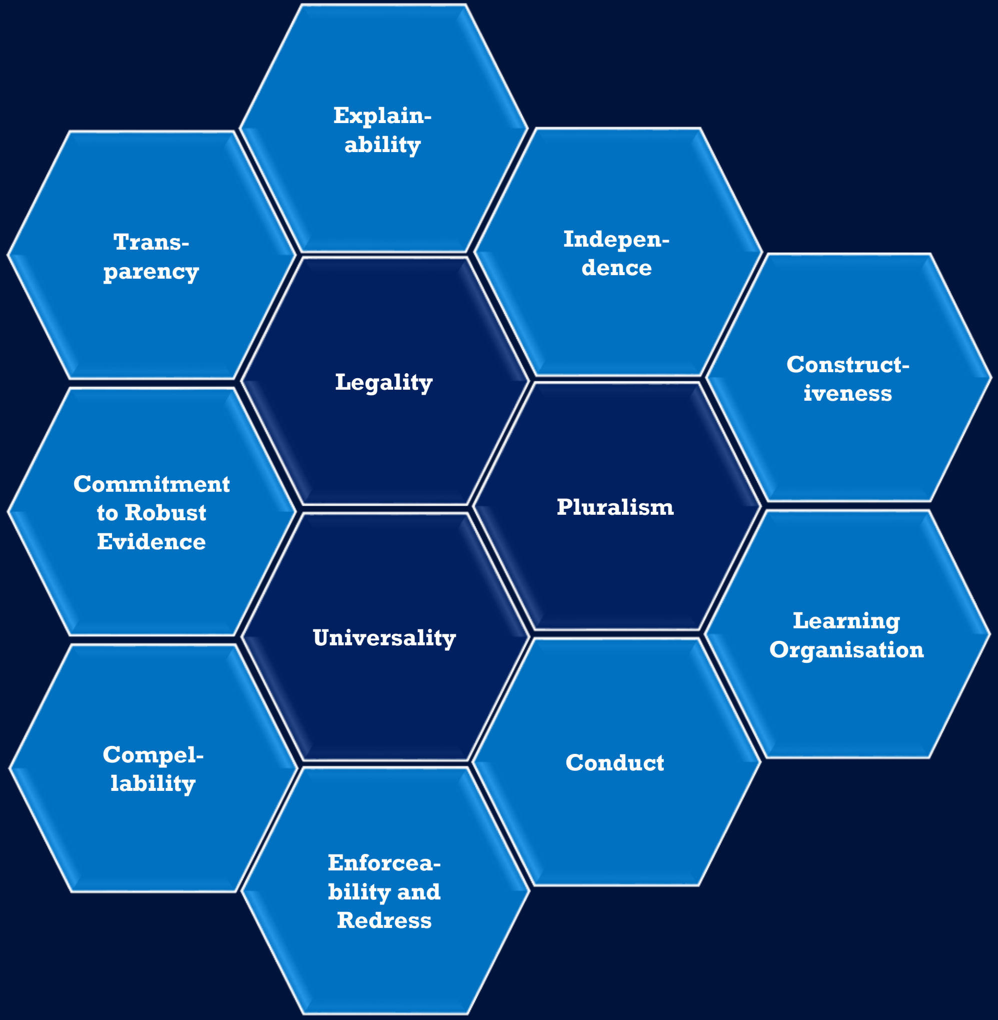
Then if they develop an AI that monitors police AI use and immediately flags abuses to a large public audience, maybe then I'd be 50% confident it would be used legally.

*AP4AI Citizen Consultation*

AP4AI

# ACCOUNTABILITY PRINCIPLES FOR AI

1. **Legality** - AI use is entirely in line with the law
2. **Universality** - every aspect of AI use without exception can be monitored and assessed
3. **Pluralism** - every group involved in and affected by AI use, without exception, has a voice in monitoring and assessing police use of AI
4. **Transparency** - all information to assess AI use and to enforce consequences is easily and fully accessible to groups that judge police use of AI
5. **Independence** - the people and groups that monitor police and enforce consequences are totally independent from police and organisations that design AI systems
6. **Commitment to Robust Evidence** - police are committed to providing evidence that is so robust that their AI use can be judged with confidence
7. **Enforceability and Redress** - it is possible to compel police to comply with all requests to improve their AI practices
8. **Compellability** - it is possible to compel police to provide access to all necessary information, systems or individuals to judge their use of AI
9. **Explainability** - all AI practices, systems and decisions can be fully explained to the public and oversight bodies
10. **Constructiveness** - police and groups that assess police use of AI always have a constructive attitude in their negotiations with each other
11. **Conduct** - all police uses of AI strictly follow professional standards
12. **Learning Organisation** - police are continually willing to change their current AI practices based on new knowledge and insights



A. **AI system and tools**

B. **Data**

C. **Laws and regulations**

D. **Oversight and redress process**

E. **Accountability evidence**

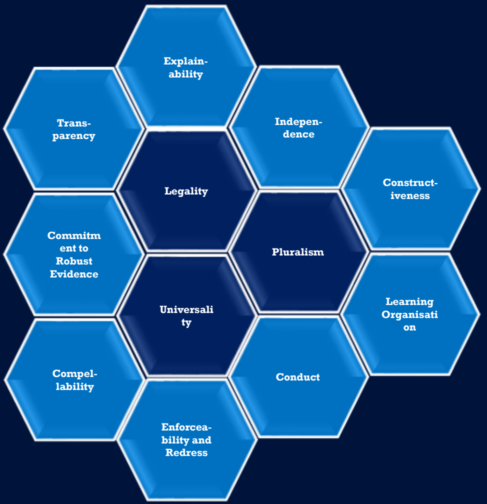
F. **Risk assessment and management**

G. **Stakeholders**

H. **Awareness and learning**

AP4AI

# ACCOUNTABILITY PRINCIPLES FOR AI



Explainability

Transparency

Independence

Legality

Constructiveness

Commitment to Robust Evidence

Pluralism

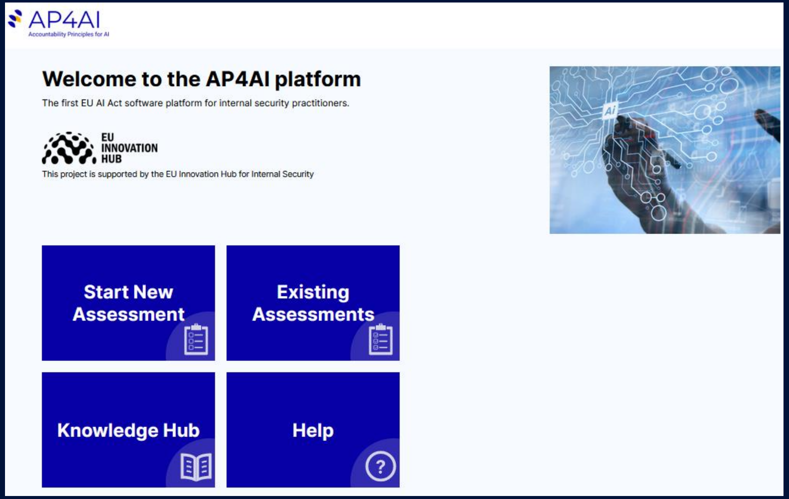
Universality

Learning Organisation

Compellability

Conduct

Enforceability and Redress



AP4AI
Accountability Principles for AI

## Welcome to the AP4AI platform

The first EU AI Act software platform for internal security practitioners.

EU INNOVATION HUB

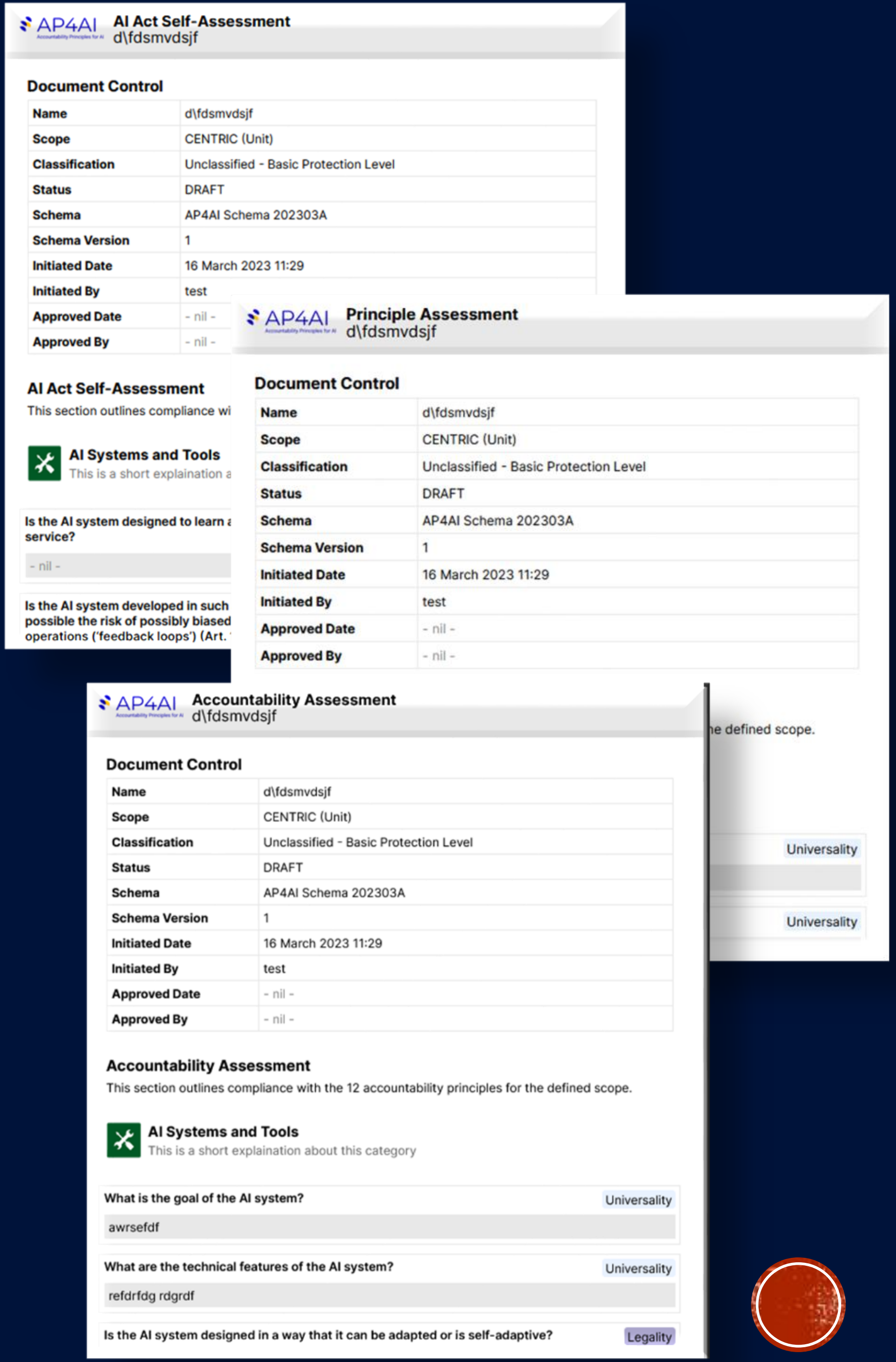
This project is supported by the EU Innovation Hub for Internal Security

Start New Assessment

Existing Assessments

Knowledge Hub

Help



AP4AI **AI Act Self-Assessment**
d\fdsmvdsjf

**Document Control**

| | |
|---|---|
| **Name** | d\fdsmvdsjf |
| **Scope** | CENTRIC (Unit) |
| **Classification** | Unclassified - Basic Protection Level |
| **Status** | DRAFT |
| **Schema** | AP4AI Schema 202303A |
| **Schema Version** | 1 |
| **Initiated Date** | 16 March 2023 11:29 |
| **Initiated By** | test |
| **Approved Date** | - nil - |
| **Approved By** | - nil - |

**AI Act Self-Assessment**

This section outlines compliance wi

**AI Systems and Tools**

This is a short explaination a

**Is the AI system designed to learn a service?**

- nil -

**Is the AI system developed in such possible the risk of possibly biased operations ('feedback loops') (Art. '**

AP4AI **Principle Assessment**
d\fdsmvdsjf

**Document Control**

| | |
|---|---|
| **Name** | d\fdsmvdsjf |
| **Scope** | CENTRIC (Unit) |
| **Classification** | Unclassified - Basic Protection Level |
| **Status** | DRAFT |
| **Schema** | AP4AI Schema 202303A |
| **Schema Version** | 1 |
| **Initiated Date** | 16 March 2023 11:29 |
| **Initiated By** | test |
| **Approved Date** | - nil - |
| **Approved By** | - nil - |

e defined scope.

Universality

Universality

AP4AI **Accountability Assessment**
d\fdsmvdsjf

**Document Control**

| | |
|---|---|
| **Name** | d\fdsmvdsjf |
| **Scope** | CENTRIC (Unit) |
| **Classification** | Unclassified - Basic Protection Level |
| **Status** | DRAFT |
| **Schema** | AP4AI Schema 202303A |
| **Schema Version** | 1 |
| **Initiated Date** | 16 March 2023 11:29 |
| **Initiated By** | test |
| **Approved Date** | - nil - |
| **Approved By** | - nil - |

**Accountability Assessment**

This section outlines compliance with the 12 accountability principles for the defined scope.

**AI Systems and Tools**

This is a short explaination about this category

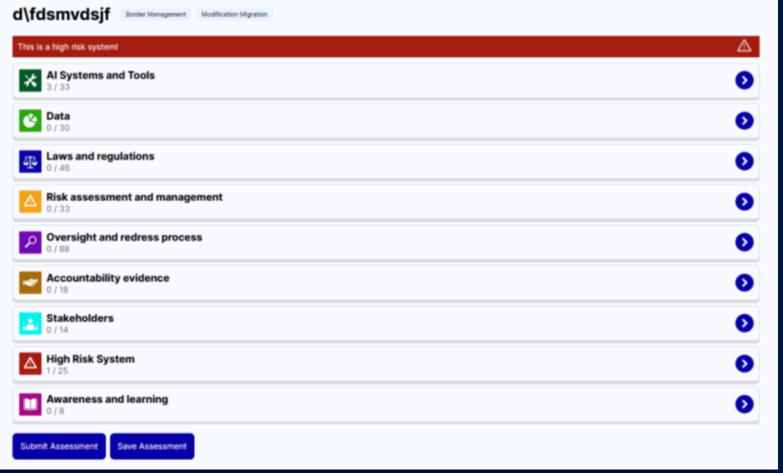
**What is the goal of the AI system?** Universality

awrsefdf

**What are the technical features of the AI system?** Universality

refdrfdg rdgrdf

**Is the AI system designed in a way that it can be adapted or is self-adaptive?** Legality

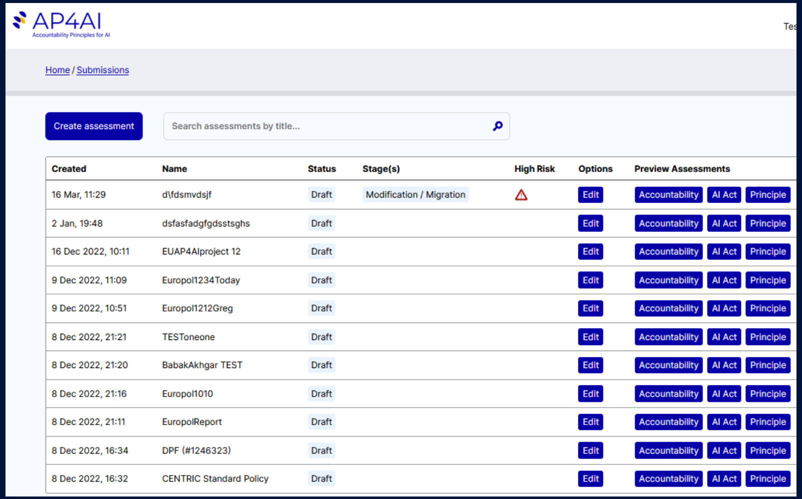


**d\fdsmvdsjf** Border Management Modification Migration

This is a high risk system! ⚠

- **AI Systems and Tools** 3 / 33
- **Data** 0 / 30
- **Laws and regulations** 0 / 46
- **Risk assessment and management** 0 / 33
- **Oversight and redress process** 0 / 88
- **Accountability evidence** 0 / 18
- **Stakeholders** 0 / 14
- **High Risk System** 1 / 25
- **Awareness and learning** 0 / 8

Submit Assessment Save Assessment



AP4AI
Accountability Principles for AI

Tes

Home / Submissions

Create assessment

Search assessments by title...

| Created | Name | Status | Stage(s) | High Risk | Options | Preview Assessments |
|---|---|---|---|---|---|---|
| 16 Mar, 11:29 | d\fdsmvdsjf | Draft | Modification / Migration | ⚠ | Edit | Accountability AI Act Principle |
| 2 Jan, 19:48 | dsfasfadgfgdsstsghs | Draft | | | Edit | Accountability AI Act Principle |
| 16 Dec 2022, 10:11 | EUAP4AIproject 12 | Draft | | | Edit | Accountability AI Act Principle |
| 9 Dec 2022, 11:09 | Europol1234Today | Draft | | | Edit | Accountability AI Act Principle |
| 9 Dec 2022, 10:51 | Europol1212Greg | Draft | | | Edit | Accountability AI Act Principle |
| 8 Dec 2022, 21:21 | TESToneone | Draft | | | Edit | Accountability AI Act Principle |
| 8 Dec 2022, 21:20 | BabakAkhgar TEST | Draft | | | Edit | Accountability AI Act Principle |
| 8 Dec 2022, 21:16 | Europol1010 | Draft | | | Edit | Accountability AI Act Principle |
| 8 Dec 2022, 21:11 | EuropolReport | Draft | | | Edit | Accountability AI Act Principle |
| 8 Dec 2022, 16:34 | DPF (#1246323) | Draft | | | Edit | Accountability AI Act Principle |
| 8 Dec 2022, 16:32 | CENTRIC Standard Policy | Draft | | | Edit | Accountability AI Act Principle |

EUROPOL

INNOVATION LAB

CENTRIC

Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

AP4AI

Accountability Principles for AI

## More information:

| | |
|---|---|
| • Website: | www.ap4ai.eu |
| • Twitter: | @AP4AI_project |
| • Email: | CENTRIC@shu.ac.uk |
| | Innovation-lab@europol.europe.eu |

EU INNOVATION HUB

cen CENELEC

European Standardization Organizations

# Harmonized European standards in support of the AI Act

Laurens Hernalsteen – lhernalsteen@cencenelec.eu

# The European Standardization System

- ▶ International
- ▶ Regional (European)
- ▶ National

Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic

Denmark
Estonia
Finland
France
Germany

Greece
Hungary
Iceland
Ireland
Italy

Latvia
Lithuania
Luxembourg
Malta
Netherlands
Norway

Poland
Portugal
Republic of North Macedonia
Romania
Serbia
Slovakia

Slovenia
Spain
Sweden
Switzerland
Turkey
United Kingdom

**43** National Standardization Organizations

from **34** countries

# Areas of work

## CEN SECTORS

- CONSTRUCTION
- CHEMICALS
- CONSUMER
- FOOD AND AGRICULTURE
- HEALTHCARE
- HOUSEHOLD APPLIANCES AND HVAC
- SERVICES
- TRANSPORT AND PACKAGING
- EUROPEAN LABELS
- DEFENCE AND SECURITY
- DIGITAL SOCIETY
- ENERGY AND UTILITIES
- MECHANICAL AND MACHINES
- MINING AND METALS
- OCCUPATIONAL HEALTH AND SAFETY

## CEN-CENELEC TOPICS

- ACCESSIBILITY
- ARTIFICIAL INTELLIGENCE
- ECODESIGN, ENERGY LABELLING AND MATERIAL EFFICIENCY
- PERSONAL PROTECTIVE EQUIPMENT
- PUBLIC PROCUREMENT
- QUANTUM TECHNOLOGIES
- ENERGY EFFICIENCY AND MANAGEMENT
- ENVIRONMENT AND SUSTAINABILITY
- ORGAN ON CHIP
- SMART GRIDS AND METERS

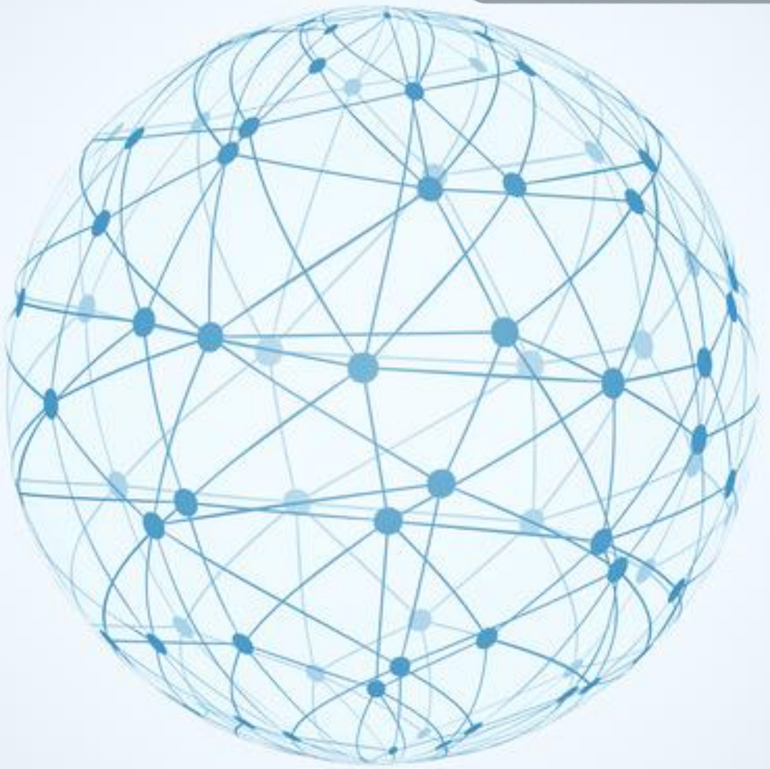
## CENELEC SECTORS

- ACCUMULATORS, PRIMARY CELLS AND PRIMARY BATTERIES
- DEFENCE AND SECURITY
- DIGITAL SOCIETY
- ELECTRIC MOTORS AND TRANSFORMERS
- ELECTROTECHNOLOGY GENERAL
- ENERGY AND UTILITIES
- HEALTHCARE
- HOUSEHOLD APPLIANCES AND HVAC
- LOW VOLTAGE ELECTRICAL EQUIPMENT AND INSTALLATIONS
- MECHANICAL AND MACHINES
- OCCUPATIONAL HEALTH AND SAFETY
- TRANSPORT AND PACKAGING
- ELECTRIC EQUIPMENT AND APPARATUS
- ELECTRONIC, ELECTROMECHANICAL AND ELECTROTECHNICAL SUPPLIES
- INSULATED WIRE AND CABLE
- LIGHTING EQUIPMENT AND ELECTRIC LAMPS

# CEN and CENELEC Community

More than **200.000** technical experts are connected in the CEN and CENELEC network

from industry, incl. SMEs, European associations, public administrations, academia, societal organizations, etc.



# Why am I talking about standards?

- The European Commission can ask the European Standardization Organizations to develop **harmonized European standards** in support of EU legislation

- Manufacturers that implement these standards benefit from a **presumption of conformity** with the legislation

- European Standards are automatically transposed into national standards in CEN and CENELEC members' countries and **conflicting national standards are withdrawn**

- In April, the European Commission will formally request CEN & CENELEC to develop such standards

# The upcoming standardization Request

**CEN & CENELEC Joint Technical Committee 21 "Artificial Intelligence"** is ready to take on this challenge

Extensive stakeholder participation of many stakeholders:

28 CEN & CENELEC member countries

ANEC, SBS, ETUC, the Commission, ENISA, …

Liaisons with many Technical Committees

Ongoing dialogue between with the European Commission increase this even further

- AI as a driver for larger mobilization of stakeholders and experts.
- Special focus on the involvement of SMEs and civil society organizations in the standardisation process

# Coffee break

*We will be back at 11:45*

Brussels | 23th March 2023

# Panel 2: Relevance and purpose of a European Security Data Space for Innovation

Brussels | 23th March 2023

# Your experts from DG HOME and EY that have carried out the Study

## ALEKSANDRA OCZKO-DOLNY

European Commission

- European Commission, DG HOME
- Policy Officer in Unit F2: Innovation and Security Research
- Supervisor of the “Study to support the technical, legal and financial conceptualisation of a European Security Data Space for Innovation (EU SDSI)”

## KATARINA BARTZ

EY

- EY Germany
- Partner in the Government & Public Sector Practice
- Close to 20 years’ experience in leading and contributing to impact assessments, feasibility, and evaluations of public policy measures
- Worked on more than 80 assignments on behalf of the EU institutions and national authorities in Germany and Sweden

## FLORIAN LINZ

EY

- EY Germany
- Senior Manager in the Government & Public Sector Practice
- More than 10 years’ experience, worked on around 50 policy studies, evaluations, impact assessments, cost-benefit-analyses on behalf of various European Commission DGs, and clients in Germany.
- Focuses on the intersection of Digitisation, Justice, and Home Affairs.

# AI for security: Maximising benefits & reducing risks

## Session 2: Data Space for Security

Study to support the technical, legal and financial conceptualisation of a European Security Data Space for Innovation (EU SDSI)

23 March 2023

Written by

Katarina Bartz
Partner | EY Economic Advisory

Building a better working world

# Agenda

1

Objectives and scope of the Study

2

Business case for the EU SDSI

3

Draft concept for the EU SDSI

4

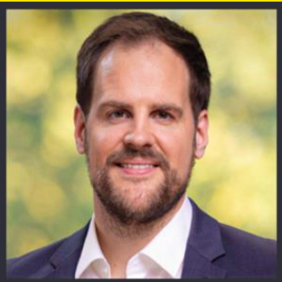
Building blocks at the EU level

5

Building blocks in the Member States

## Katarina BARTZ

EY Germany
Partner
Government & Public Sector
katarina.bartz@de.ey.com



## Florian LINZ

EY Germany
Senior Manager
Government & Public Sector
katarina.bartz@de.ey.com

# The project serves to facilitate innovation in law enforcement. It is one building block among several at EU and Member State levels.

## Policy & project objectives

**Strategic objectives:**

- Increase the level of security in the EU
- Facilitate the development and application of AI in law enforcement
- Improve the access to high quantity and high quality data for law enforcement authorities

**Operational objective:**

- Assess the appetite and develop a concept for a European Security Data Space for Innovation (EU SDSI)

## Project scope

- **Innovation** in law enforcement (police, border guards, customs etc.), i.e. *not* operational aspects
- Examine the situation at the EU level and in all 27 EU Member States from various angles:
  - Legal
  - Technical
  - Organisational
  - Capabilities

## Project structure

- Two main phases
- Information was gathered on the situation:
  - In the 27 Member States
  - At the EU level
- Methodology used:
  - Desk research
  - Online surveys
  - Interviews
  - Workshops and focus groups with EU and Member State stakeholders

Several innovation projects at international, EU, and national levels are running in parallel

# The EU SDSI would fill a gap. There is great appetite for a Data Space within the law enforcement community.

## Challenges for & practical needs of law enforcement authorities

Challenges:

- Serious and organised crime is not bound by national borders
- The threat landscape is increasingly complex
- Criminals themselves become "innovative" through technology

Practical needs:

- Access to data (models) to develop, train, test and validate AI
- Effective and efficient investigations
- Increased cooperation

## Potential solution

- The Member States remain in the driver's seat:
  - Federated architecture and interoperability: Leveraging what already exists
  - Use cases: Focus on what is important to the Member States
  - Governance: Shared ethical principles, values and processes
- Compliance with applicable legislation (in particular GDPR)
- Full respect for Fundamental Rights

## Key take-aways

- Innovation is a crucial enabler for increased security
- The EU SDSI fills a gap at the EU-level. Several data-related innovation projects are already ongoing at national level
- There is great appetite within the law enforcement community for an EU SDSI

The EU SDSI should deal with non-sensitive data (i.e. no operational law enforcement data)

# The first steps towards an EU SDSI have been taken. There is a need for further development in collaboration with the Member States.

## Starting point

- The EU SDSI is a development project with the ability to ‘grow’ and ‘progress’
- Starting point: Development of a Minimum Viable Product to be gradually expanded based on inputs by the Member States

## Foundational principles

- Focus on non-sensitive data (i.e. no operational data)
- Focus on police (and equivalents) at the start; expand to further law enforcement authorities over time
- Set up a hybrid governance model that caters to different needs
- Leverage regulatory sandboxes and actively test the Minimum Viable Product

## First steps taken; Need for further development

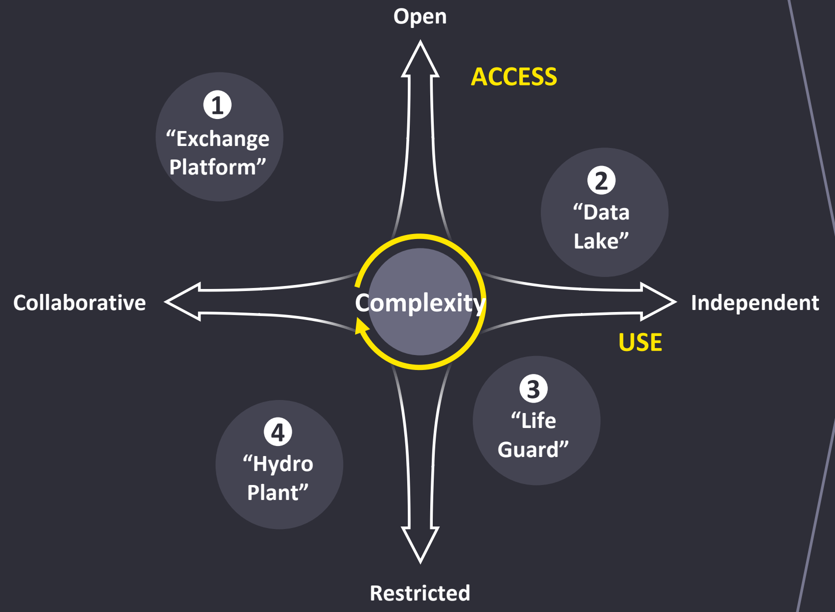
- Governance: Roles and responsibilities of specific stakeholders
- Operation: Specific use cases the EU SDSI should address (examples are available)
- Content: Specific data the EU SDSI should make accessible
- Rules: Specific conditions under which data can be used

**Active collaboration between the EU and Member States**

> “The EU SDSI should leverage existing work and opportunities at the EU-level, while being in compliance with national law and processes”

# The EU SDSI should follow a hybrid governance model.
# Its solutions should cater to needs of the law enforcement community.

## Governance matrix



- Solutions have different purposes
- 'Open & collaborative' vs. 'restricted & independent'
- Varying degrees of complexity

## Solutions in a nutshell

- Exchange platform: Accessible for all stakeholders as a collaborative environment
- Data Lake: Accessed by law enforcement authorities to develop data-driven innovations and AI algorithms
- Life Guard: Central service to facilitate access and use of the data ("do not drown in the data lake")
- Hydro Plant: Central service to help Member States extracting the most value of the data

## Feedback received

Feedback provided by stakeholders:

- Prototypical solutions are relevant and add value
- The practical relevance depends on the concrete use case
- Flexibility is crucial: Solutions may need to be enhanced / adapted over time

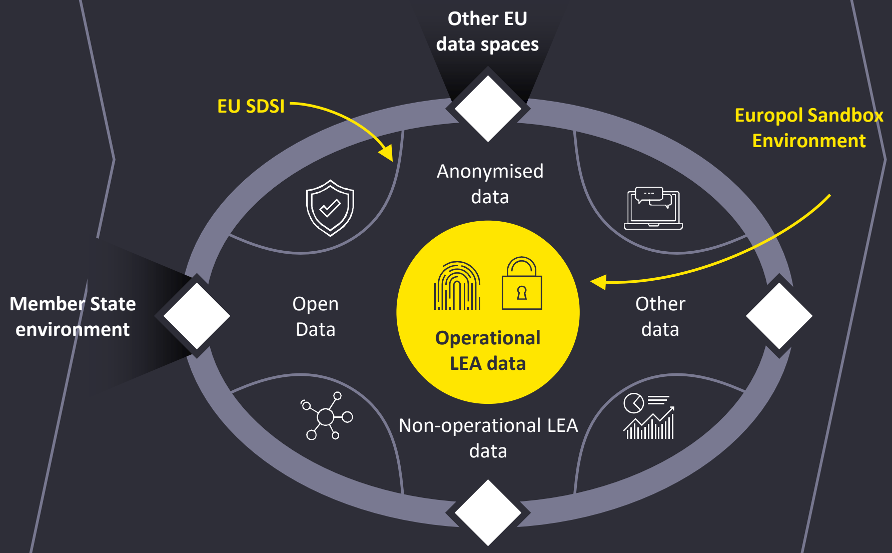
Feel free to provide any other feedback!

# The EU SDSI is a layer in the ecosystem.
# It connects various solutions for data-driven innovation.

## Basic idea

- ▶ Connecting the innovation ecosystem is crucial: The EU SDSI could connect national environments and could be linked to other EU data spaces in the long-term
- ▶ The future Europol sandbox environment is a crucial facilitator for innovation in the Member States
- ▶ Close collaboration between EU SDSI and Europol is only one of several potential options

## Further collaboration with Member States is needed to elaborate the concept



## Vision for the future

EU SDSI:

- ▶ Shell of a larger ecosystem dealing with non-sensitive data
- ▶ The EU SDSI as a secure facility and interoperable connector to other EU data spaces and national environments in which data is stored

Europol sandbox environment:

- ▶ Core of the ecosystem dealing with sensitive data
- ▶ Member States can connect their sensitive data with non-sensitive data from the EU SDSI to test, train and validate AI algorithms

# The EU SDSI will serve clear use cases.
# It will provide specific services to stakeholders.

## Status quo

Work on relevant AI use cases is already ongoing:

- At national level in the Member States
- Across borders between Member States
- With EU-level stakeholders such as Europol

It is important to find the "right" gaps in the current use case landscape for the EU SDSI to fill

Feel free to provide any information about use cases!

## Use cases

Crime scenes in video files

Background noises in phone calls

Smuggling of stolen cars

Any other use case you deem relevant

## Potential service packages

Access to non-sensitive data

Sharing of knowledge and good practices

Establishing a common data ontology

Automated annotation of data

Safety checks for compliance

# The EU is ambitious concerning data-driven innovation. There are strong legal foundations enabling and restricting the use of data.

## Ambition

- The EU aims at becoming ‘a leading role model for a society empowered by data’
- Trusted stakeholders with strong mandates and expertise at the EU-level:

EUROPOL

eu-LISA

DATA SPACES SUPPORT CENTRE

- Reliable and secure funding structures under DIGITAL to ensure the implementation of the EU SDSI and support Member States

## Data protection, privacy and fundamental rights: Key Legal Foundations

- General Data Protection Regulation (GDPR)
- Law Enforcement Data Protection Directive (LED)
- EU Data Protection Regulation (EU-DPR)
- Charter of Fundamental Rights of the European Union

## (Non-) Legal Enablers

### Legislative

- Regulation on the free flow of non-personal data
- Open Data Directive / High Value Datasets
- Data Act
- Data Governance Act
- AI Act
- Europol Regulation
- eu-LISA Regulation

### Non-legislative

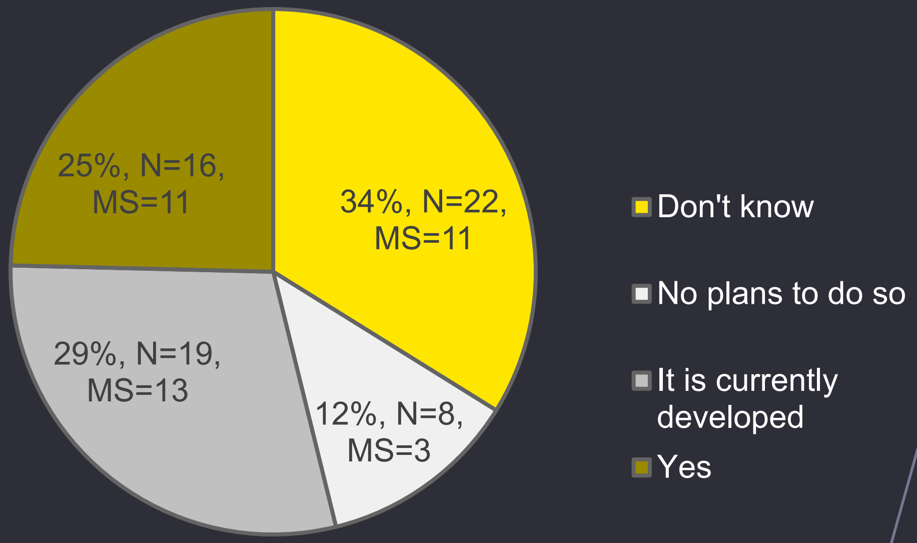
- Data Strategy
- Coordinated Plan on AI
- Digital Europe
- Staff Working Document on EU Data Spaces

# The uptake of AI and the availability of data spaces in national law enforcement is limited.

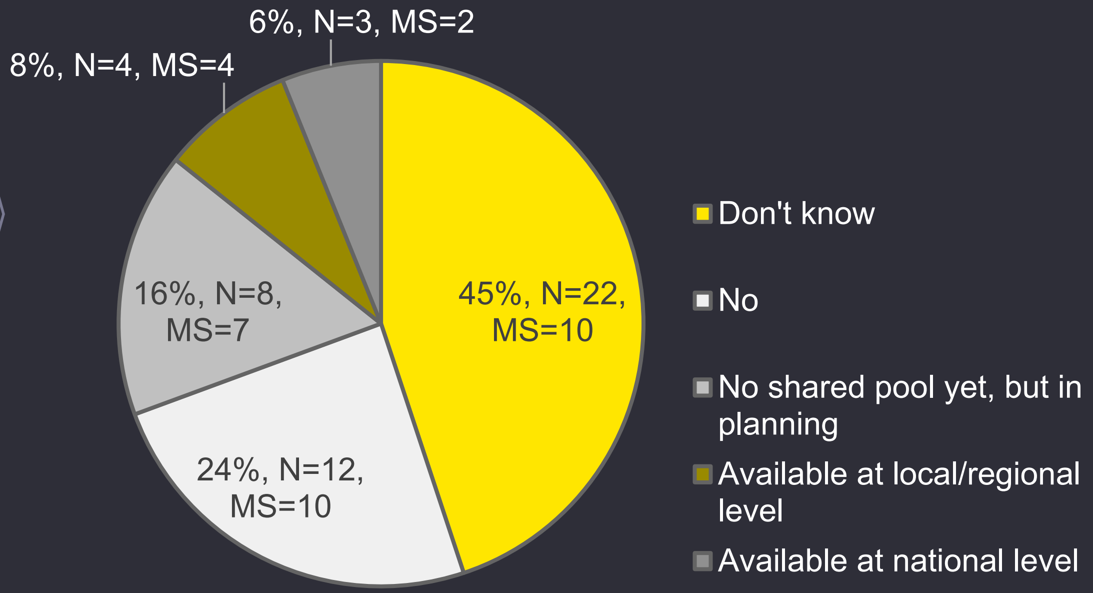
| | Policy | Data | Technology |
|---|---|---|---|
| ✓ | ▶ National competencies regarding AI in law enforcement are mostly clear | Diverse sources and data are used, such as:<br>▶ Investigations<br>▶ Open data<br>▶ Statistically processed law enforcement data | ▶ Focus on technical data security: Member States implement various technical and organisational measures |
| ⚠ | ▶ Law enforcement is not always a priority in national AI strategies<br>▶ The legal framework for the use of AI in law enforcement is ambiguous<br>▶ Limited financial resources | Cross-border data sharing is limited:<br>▶ National limitations<br>▶ Data protection<br>▶ Lack of technical resources<br><br>Room for improvement regarding data literacy and skills | ▶ The necessary infrastructure is not always in place<br>▶ Maturity levels vary across Member States<br>▶ Necessary technical skills are not always available in all Member States |

# The uptake of AI in national law enforcement is limited. Only few Member States already have dedicated data spaces in place.

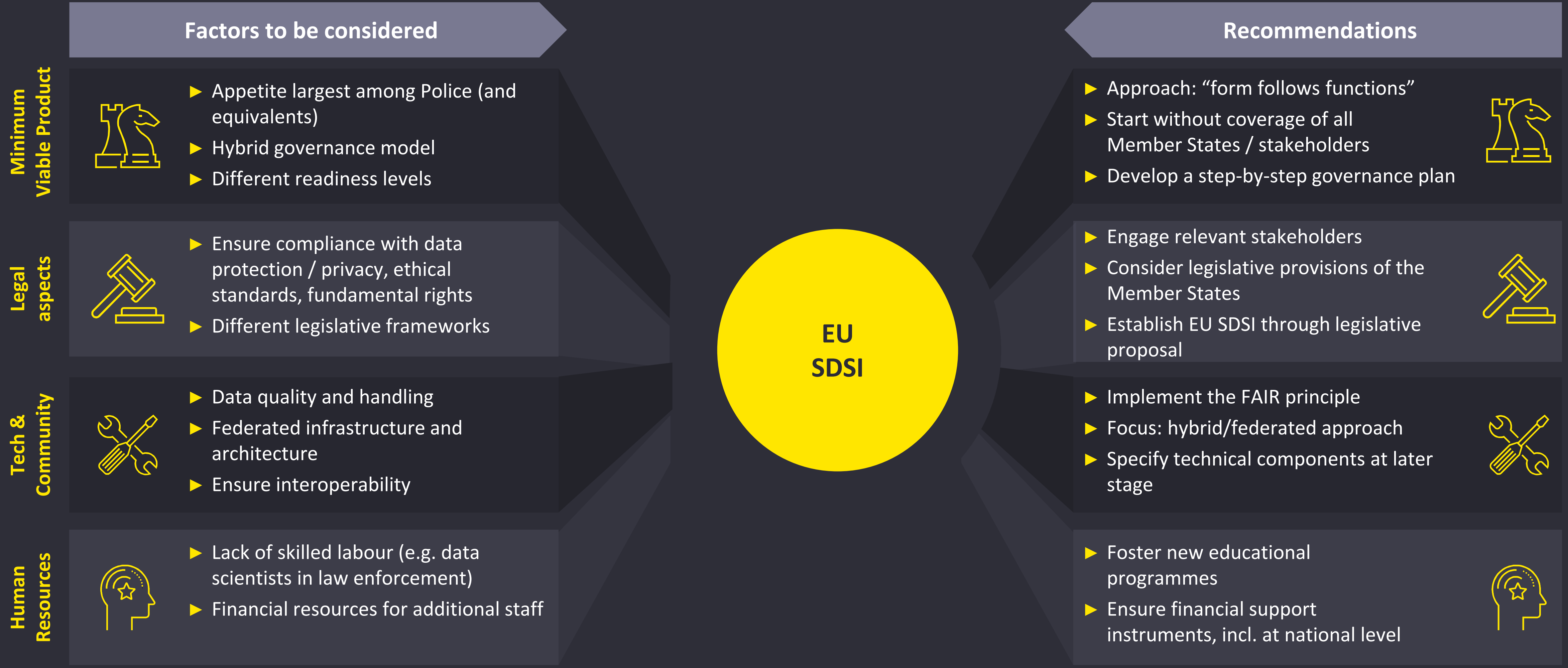
## Do you have a strategy in place in your Member State to develop, train, test, etc. AI solutions in the area of law enforcement?



## Is a data space (…) for multiple law enforcement services available in your Member State?



# Various factors should be considered for the future development.



| | Factors to be considered | Recommendations |
|---|---|---|
| Minimum Viable Product | ▶ Appetite largest among Police (and equivalents)<br>▶ Hybrid governance model<br>▶ Different readiness levels | ▶ Approach: “form follows functions”<br>▶ Start without coverage of all Member States / stakeholders<br>▶ Develop a step-by-step governance plan |
| Legal aspects | ▶ Ensure compliance with data protection / privacy, ethical standards, fundamental rights<br>▶ Different legislative frameworks | ▶ Engage relevant stakeholders<br>▶ Consider legislative provisions of the Member States<br>▶ Establish EU SDSI through legislative proposal |
| Tech & Community | ▶ Data quality and handling<br>▶ Federated infrastructure and architecture<br>▶ Ensure interoperability | ▶ Implement the FAIR principle<br>▶ Focus: hybrid/federated approach<br>▶ Specify technical components at later stage |
| Human Resources | ▶ Lack of skilled labour (e.g. data scientists in law enforcement)<br>▶ Financial resources for additional staff | ▶ Foster new educational programmes<br>▶ Ensure financial support instruments, incl. at national level |

# Thank you for your time and attention!

If you want to share further information, please contact us under:

EUSecurityDataSpace@de.ey.com

# Your experts on stage during the panel discussion

## FEDERICO MILANI

European Commission

- European Commission, DG CNECT
- Deputy Head of Unit, Data Policy & Innovation Unit
- Supports the data economy in the Digital Single Market through policy initiatives addressing new and emerging issues, such as data ownership and brokerage or open data policies.

## LUÍSA PROENÇA

POLÍCIA JUDICIÁRIA

- Polícia Judiciária Portugal
- Deputy National Director, responsible for Innovation, ICT, Finance
- Experienced Head in Research & Innovation for Security (FP7, H2020, HEU)
- Experienced Head with a demonstrated history of working in the government administration. Skilled in Government, International Relations, Management, and Digital Innovation

## NIZAR TOULEIMAT

STARLiGHT

Sustainable Autonomy and Resilience for LEAs using AI against High Priority Threats

- CEA - Commissariat à l'énergie atomique et aux énergies alternatives
- European & International Affairs manager - Smart Digital Systems for Security and Defense
- Coordinator of the STARLIGHT project: Innovation project backed by the EU that aims enhance the EU's strategic autonomy in the field of AI for LEA

## GRÉGORY MOUNIER

EUROPOL

- EUROPOL
- Head of Team, Innovation Lab
- Experienced Policy Advisor with a demonstrated history of working in the law enforcement industry. Skilled in Innovation and Digital Policy, Internet Governance, Data Protection (CIPP/E), Crisis Management, Security Policy and Policy Analysis.

## ALEKSANDRS CEPILOVS

eU-LISA

- eu-LISA - European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
- Research officer
- Research fellow at Tallinn University of Technology

# Session 2: Main messages from the study and the panel discussion

## Overarching strategy

**Starting point:**

- The EU Commission is promoting data sharing to enable better and more efficient services
- Data spaces: Sectoral, multi-dimensional solutions to facilitate the sharing of data across organisations and Member States
- Law enforcement: Appetite and need for a data space for better access to high quality and quantity of data

**Call to action:**

- Work has started: The Commission, Member States and other stakeholders have started to develop a concept for a data space for innovation in law enforcement

**Your support and contributions are crucial and highly appreciated!**

## Data space in law enforcement

**Foundational basis:**

- Purpose: Facilitate developing, testing and training Member States' AI algorithms
- Will focus on enabling data-related innovation / AI
- Will not contain any sensitive, operational data (operational data is addressed in a separate Europol Sandbox)
- Full compliance with data protection and privacy provisions and Fundamental Rights

**Minimum Viable Product:**

- Focus on use cases in the area of police/equivalents and leverage work done at EU and national levels
- Cater directly to the innovation needs of law enforcement ('hybrid governance model')
- Connect with Member States' available IT infrastructure

## Key enablers

**Data sovereignty:**

- Member States remain in control of what they share, with whom and for what purpose
- Regulatory Sandbox: Europol allowed to process operational data in a 'safe haven'

**Trust is crucial:**

- Clear and transparent legal framework across EU - underpinned by an advanced technical system
- Smart Middleware (SIMPL): Cloud to Edge platform expected to solve crucial technical challenges concerning security and privacy
- Establishment of and adherence to common principles, values, standards (e.g. FAIR) within the ecosystem

## Next steps

**Short-term:**

- Finalisation of the conceptual study
- Continued collaboration with the Member States to elaborate the concept

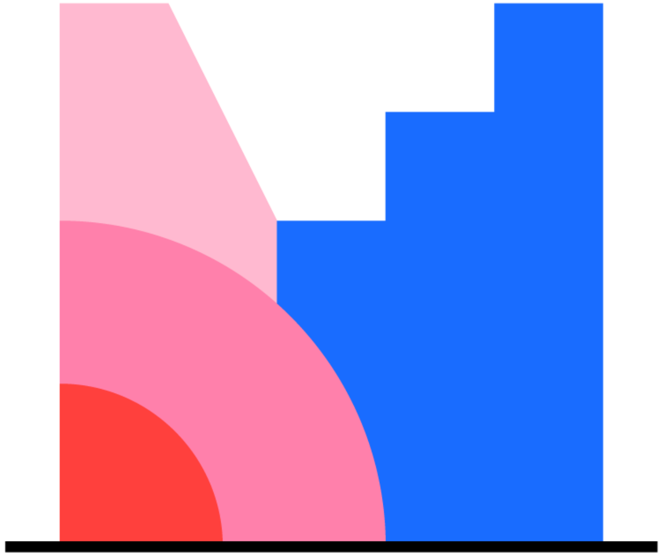
**Medium-term (potentially):**

- Development of a Minimum Viable Product for a data space
- Improvement of readiness of law enforcement to work with and share data

**Long-term (potentially):**

- Further improvement and enlargement of the data space, e.g. to other law enforcement areas, use cases, functionalities etc.

# Time for your feedback!



**Please provide your feedback via Mentimeter!**

Please **scan the QR code** to the right

*OR*

Go to [www.menti.com](http://www.menti.com) and use the code you see to the right

Enter the code

**3940 0880**

Thank you for your time and attention!

If you want to share further information, please contact us under:

EUSecurityDataSpace@de.ey.com

# Lunch break

*We will be back at 14:30*

Brussels | 23th March 2023

# Panel 3: Successful examples and future aspirations for AI in support of civil security

**Moderator:** Ruth Linden, Europol Innovation Lab
Armin Reuter, D4FLY project
Peter Leškovský, GRACE project
Aris Bonanos, S4ALLCITIES project
Anna Beata Kołodziej (eu-LISA)
Gilles Robine, DG HOME D4

Brussels | 23th March 2023

# D4FLY

DETECTING DOCUMENT FRAUD
AND IDENTITY ON THE FLY

Breeder Documents

Travel Documents

Research using AI and ML technologies

along the **identity lifecycle** from

**breeder document analysis** and

**travel document verification** to

**identity verification on-the-move** at border crossing points

to detect fraud and enhance security

Biometrics on-the-move

| | |
|---|---|
| D4FLY runtime: | 09/2019 – 08/2022 |
| Coordinator: | Veridos GmbH/ Germany |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833704

Grace

# Global Response Against Child Exploitation

## H2020-SU-SEC-2019 - Technologies to enhance the fight against crime and terrorism

June-2020 to Nov-2023 (42 months)

Date: 21/02/2023

Peter Leškovský

vicomtech
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

GRACE has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 883341

# Global Response Against Child Exploitation

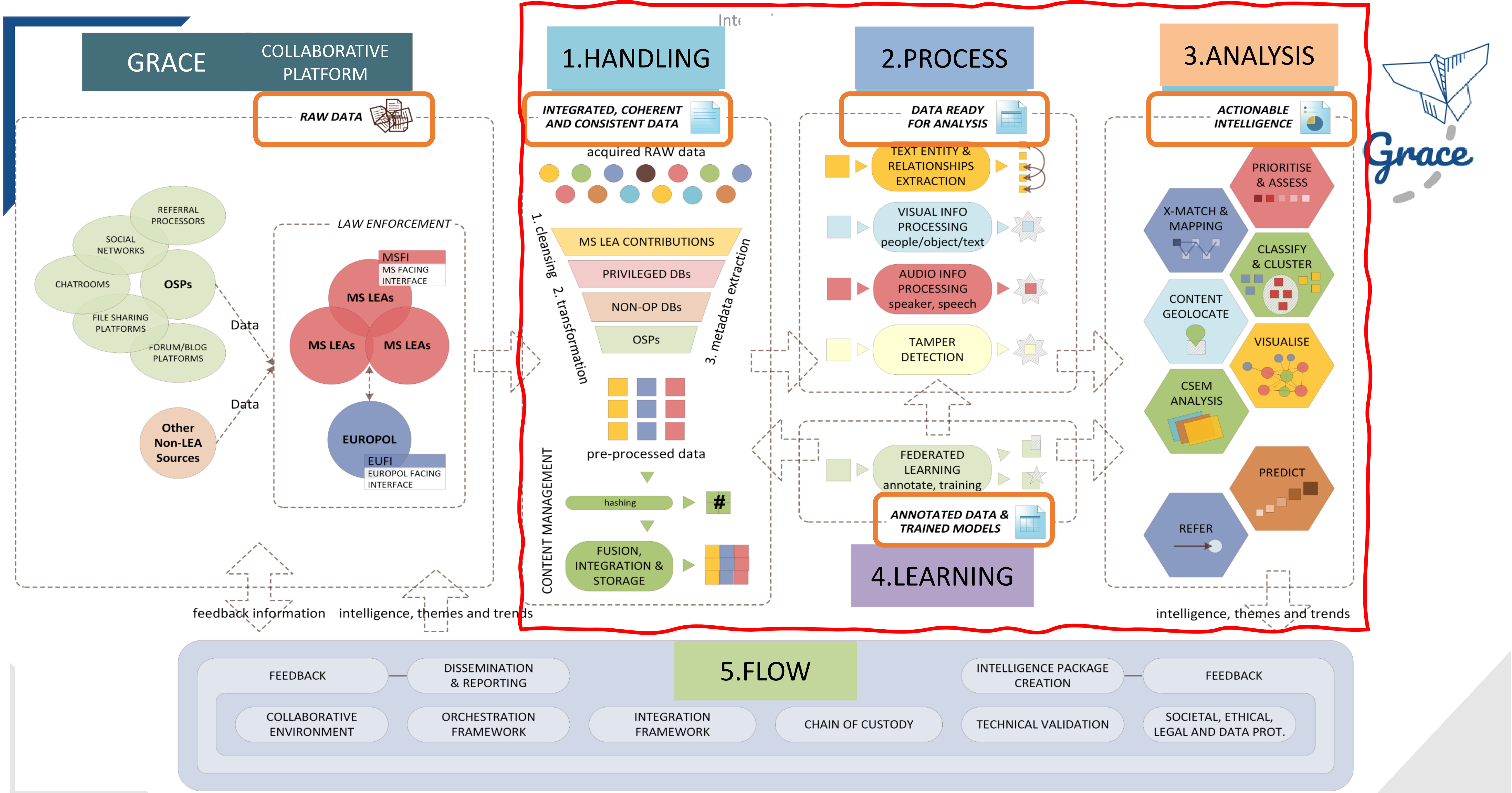
**The use of the Internet to distribute Child Sexual Exploitation Material (CSEM) is an abhorrent crime.** Referrals from **Online Service Providers are key to fighting CSE**.

However, the sheer volume of referrals is pushing MS LEAs to their limits and affecting their capacity to prevent harm to infants and children, rescue those in immediate danger, and investigate and prosecute perpetrators.

**GRACE will apply proven techniques in ML to the referral and analysis process** while embracing the very technical, ethical and legal challenges unique to fighting CSE. GRACE will **leverage resources already in place at EUROPOL and its 8 MS LEAs** and attempt to **provide results early, frequently and flexibly, prioritising easy wins** in the research plan (e.g. deduplication, cross matching, classification).

LEA | Research / University | Industry / SME

GRACE has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 883341



Inte

GRACE COLLABORATIVE PLATFORM

RAW DATA

REFERRAL PROCESSORS

SOCIAL NETWORKS

CHATROOMS

OSPs

FILE SHARING PLATFORMS

FORUM/BLOG PLATFORMS

Other Non-LEA Sources

Data

Data

LAW ENFORCEMENT

MSFI

MS FACING INTERFACE

MS LEAs

MS LEAs

MS LEAs

EUROPOL

EUFI

EUROPOL FACING INTERFACE

feedback information

intelligence, themes and trends

1.HANDLING

INTEGRATED, COHERENT AND CONSISTENT DATA

acquired RAW data

1. cleansing

2. transformation

3. metadata extraction

MS LEA CONTRIBUTIONS

PRIVILEGED DBs

NON-OP DBs

OSPs

pre-processed data

CONTENT MANAGEMENT

hashing

#

FUSION, INTEGRATION & STORAGE

2.PROCESS

DATA READY FOR ANALYSIS

TEXT ENTITY & RELATIONSHIPS EXTRACTION

VISUAL INFO PROCESSING people/object/text

AUDIO INFO PROCESSING speaker, speech

TAMPER DETECTION

FEDERATED LEARNING annotate, training

ANNOTATED DATA & TRAINED MODELS

4.LEARNING

3.ANALYSIS

ACTIONABLE INTELLIGENCE

PRIORITISE & ASSESS

X-MATCH & MAPPING

CLASSIFY & CLUSTER

CONTENT GEOLOCATE

VISUALISE

CSEM ANALYSIS

PREDICT

REFER

intelligence, themes and trends

Grace

5.FLOW

FEEDBACK

DISSEMINATION & REPORTING

INTELLIGENCE PACKAGE CREATION

FEEDBACK

COLLABORATIVE ENVIRONMENT

ORCHESTRATION FRAMEWORK

INTEGRATION FRAMEWORK

CHAIN OF CUSTODY

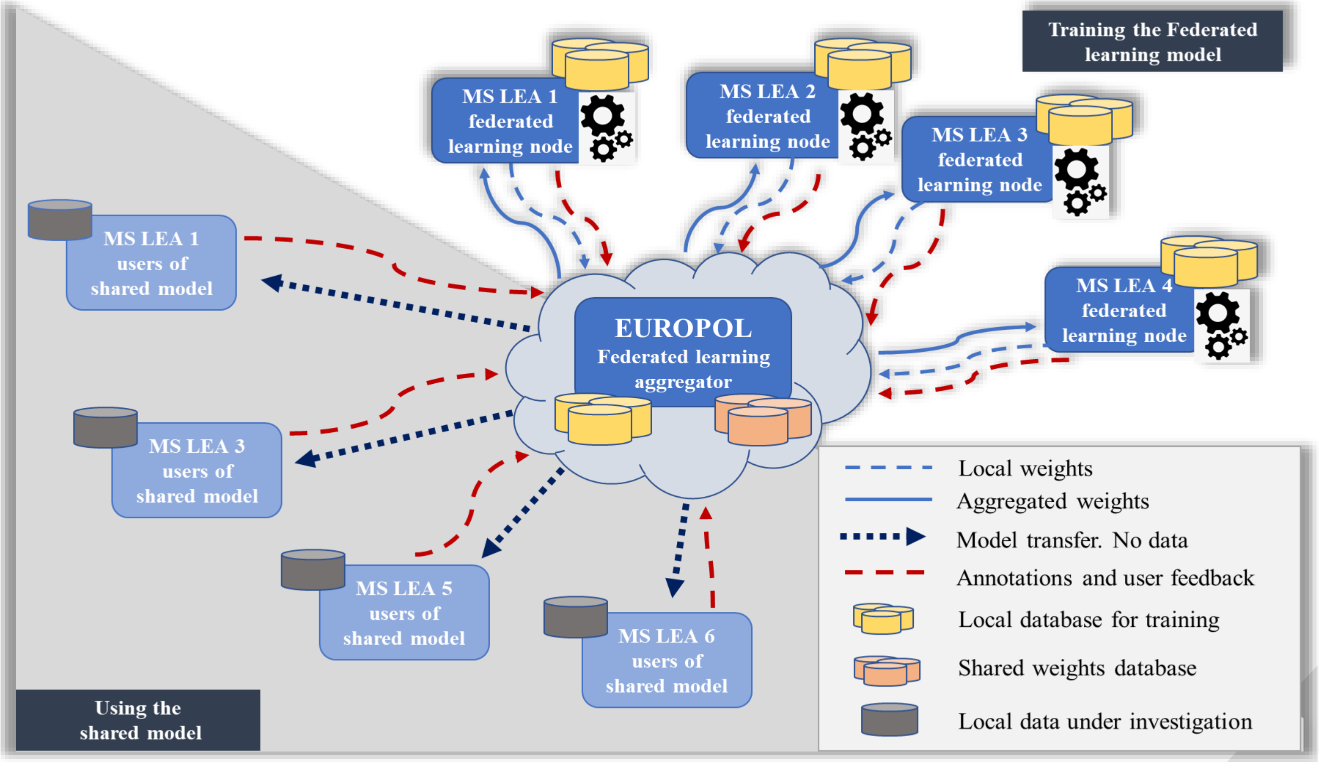
TECHNICAL VALIDATION

SOCIETAL, ETHICAL, LEGAL AND DATA PROT.

GRACE has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 883341

# GRACE tooling

- **Analytics**
  - >30 data enrichment tolos (image/video, audio, text)
  - >11 actionable intellingence tools (cross-matching, prioritisation and geolocalisation)
  - targeted online search tool
- **Operational suitability**
  - Data annotation workshops
  - Federated Learning approach


Training the Federated learning model
MS LEA 1 federated learning node
MS LEA 2 federated learning node
MS LEA 3 federated learning node
MS LEA 4 federated learning node
MS LEA 1 users of shared model
MS LEA 3 users of shared model
MS LEA 5 users of shared model
MS LEA 6 users of shared model
EUROPOL Federated learning aggregator
Using the shared model
Local weights
Aggregated weights
Model transfer. No data
Annotations and user feedback
Local database for training
Shared weights database
Local data under investigation

GRACE has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 883341

# GRACE ethical and legal framework

## D9.1 Ethical report

- general analysis of the available standards and regulations

## D9.5 on Overall legal and ethical framework

- practical guidelines to enhance transparency and explicability

Available at www.grace-fct.eu

- Chapter 2 Draft AI Act related:
  - the achievement of the highest standards in terms of robustness, safety, cybersecurity and accuracy,
  - the establishment of appropriate documentation.
  - the sharing of adequate information about ML modules with the end-user: their principles and limitations
  - the use of high-quality datasets.

GRACE has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 883341

# Thank you for your attention!

**CONTACT US**

info@grace-fct.eu

**WEBSITE**

www.grace-fct.eu

**SOCIAL MEDIA**

@grace_fct_eu

grace_fct_eu

gracefcteu

More information at:

https://cordis.europa.eu/project/id/883341

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883341

# S4ALLCITIES

**Smart Spaces Safety and Security for All Cities**

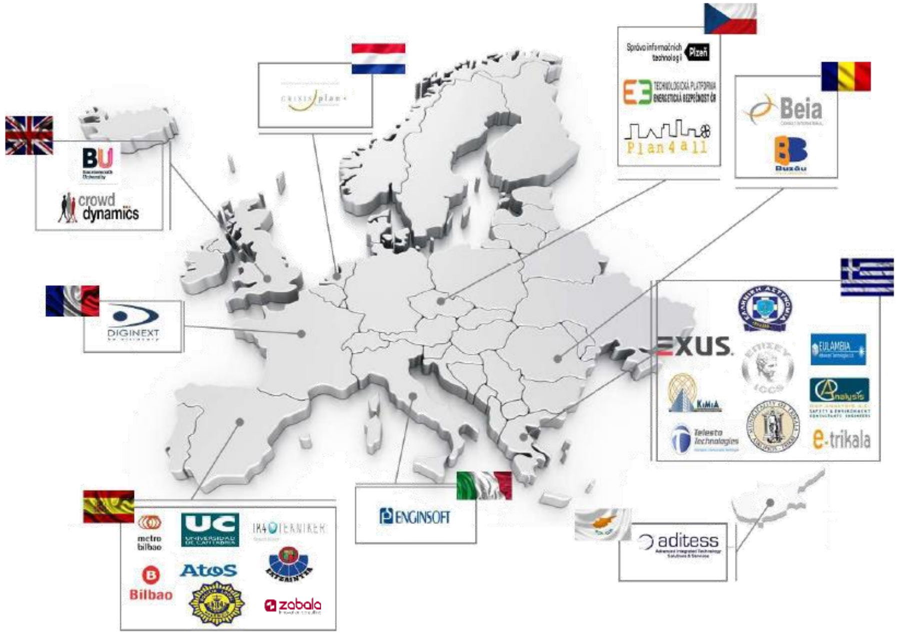
**CERIS workshop on Artificial Intelligence in Security Research**

Aris Bonanos

Project Coordinator
EXUS AI Labs

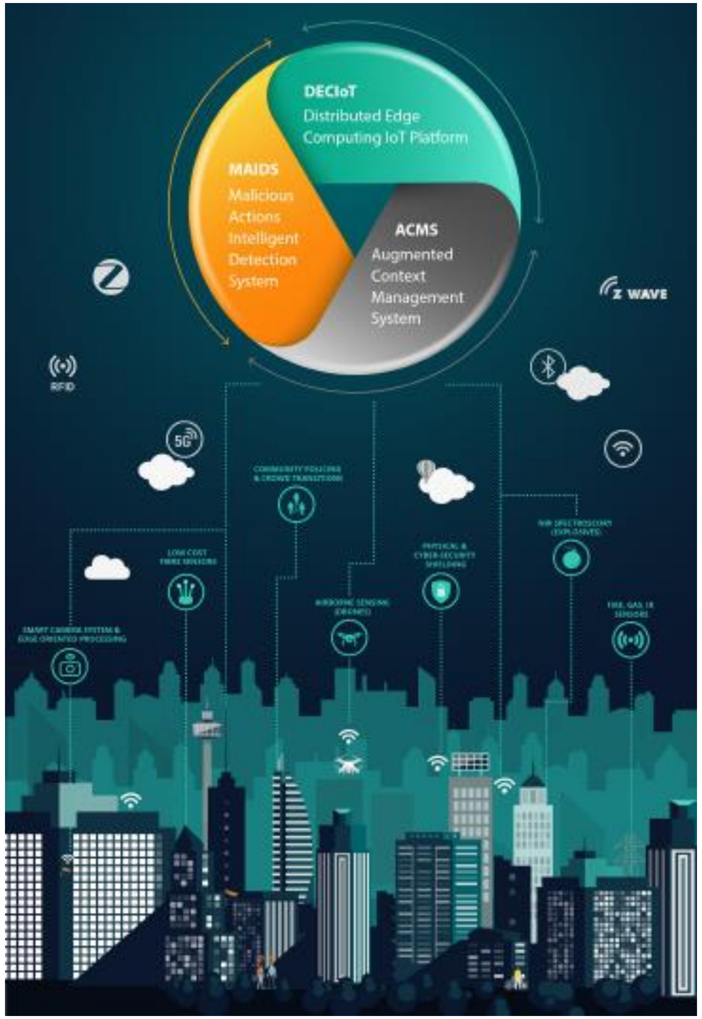
# S4AllCities – At a glance

- Work Programme & Call
  - Secure Societies: Protecting freedom and security of Europe and its citizens
  - H2020-SU-INFRA 2019: Protecting the infrastructure of Europe and the people in the European Smart cities
- **S**mart **S**paces **S**afety and **S**ecurity for **All Cities**
  - Grant Agreement No. **883522**
  - ~~24~~ 28 months:
    - 1/9/2020 – ~~31/8/2022~~ 31/12/2022
  - Total budget **€9.7M**, Requested EC contribution **€8.0M**
  - Consortium of 28 partners
    - 9 EU Countries
    - 5 Smart Cities
    - 3 Law Enforcement Agencies (LEA)
    - 1 Transport Operator
    - 16 Supporting Cities, LEAs, Ministries



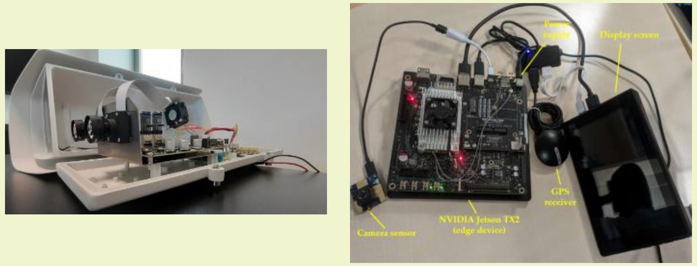
# S4AllCities – Our objective

- Smart Spaces Safety & Security for All Cities
  - Increase resilience of city infrastructure
  - Provide technological & organizationsal solutions for the management of safety and security of public spaces
- Achieve through 3 digital twins
  - *Twin 1*: Distributed Edge Computing IoT Platform
    - Smart City IoT interface
      - Edge gateway and connectivity; Intelligent data streaming; Analytics & Feedback
  - *Twin 2*: Malicious Actions Intelligent Detection System
    - Intelligence
      - Machine detection of usual and unusual behavior; Advanced situational awareness; Data fusion and threat identification
  - *Twin 3*: Augmented Context Management System
    - Common operational picture, decision support
      - Recommendation to first responders; Process augmented representation
  - **AI plays a key role** in the developed System of Systems



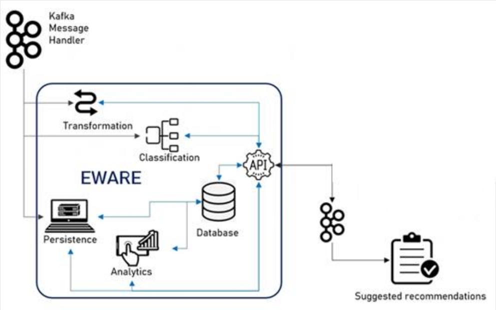
DECIoT
Distributed Edge Computing IoT Platform
MAIDS
Malicious Actions Intelligent Detection System
ACMS
Augmented Context Management System
Z WAVE
RFID
5G
COMMUNITY POLICING & CROWD TRANSITION
LOW COST FIBRE SENSORS
SMART CAMERA SYSTEM & EDGE ORIENTED PROCESSING
AIRBORNE SENSING (DRONES)
PHYSICAL & CYBER-SECURITY SHIELDING
NIR SPECTROSCOPY (EXPLOSIVES)
FIRE, GAS, IR SENSORS

# Solutions: Hardware, Modeling & Situational Awareness

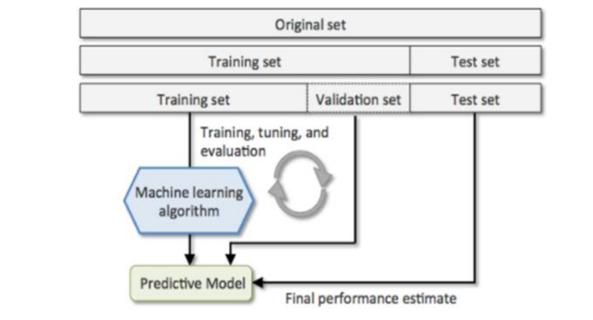


(2) Custom edge hardware for AI enabled video processing

Portable spectrometer for detecting chemical precursors to explosives. ML for spectral analysis

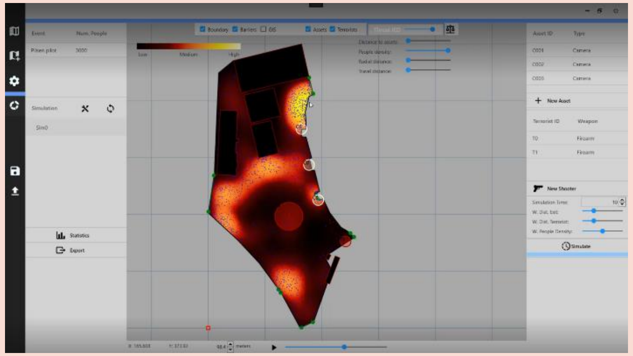


Data fusion, combination and classification for multi-criteria decision analysis


Original set
Training set
Test set
Training set
Validation set
Test set
Training, tuning, and evaluation
Machine learning algorithm
Predictive Model
Final performance estimate

Anomaly detection applied to meteorological parameters

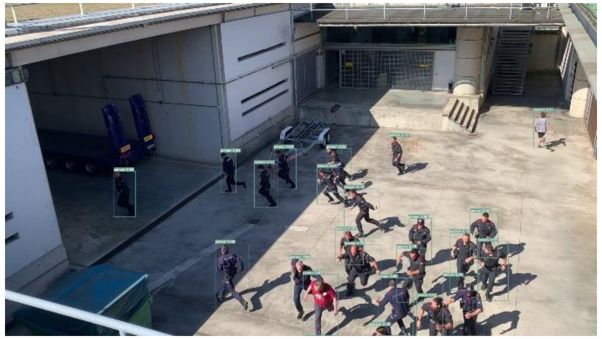
Crowd Simulation Toolkit (Intervention and Evacuation)



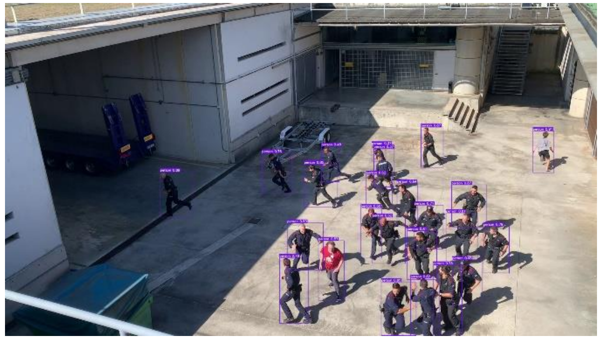
Terrorist Attack Hazard Analysis Toolkit (Mass Shooting impact and IED threat)

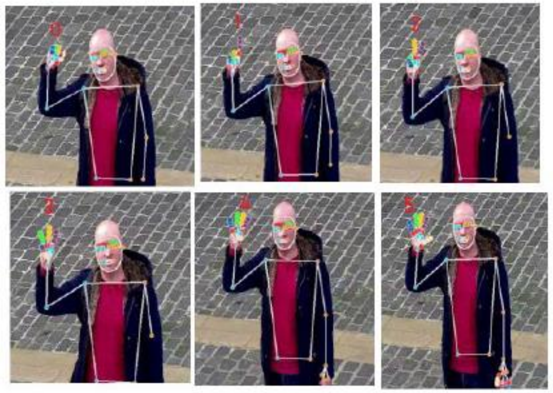
# Solutions: Video analytics

- Detection and tracking of people and cars
- Detection of abandoned luggage
- Re-identification of people using multiples cameras
- Detection of guns
- Detector of knives
- Detection of actions
- Sentiment analysis

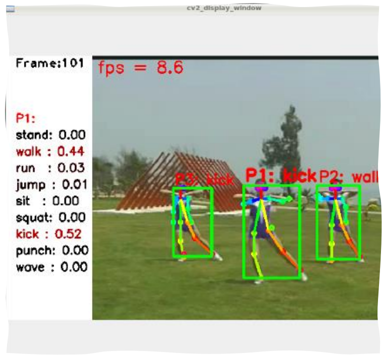


Unusualness in crowd movement

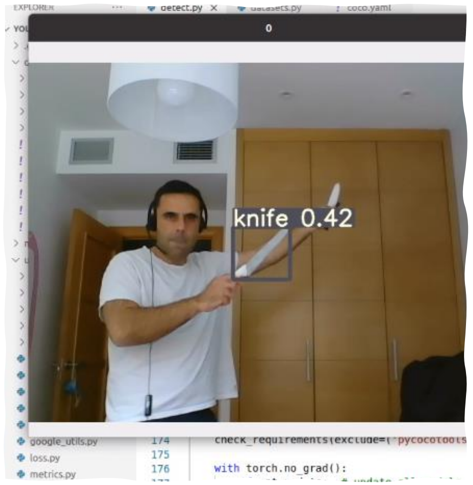




Gesture based communication

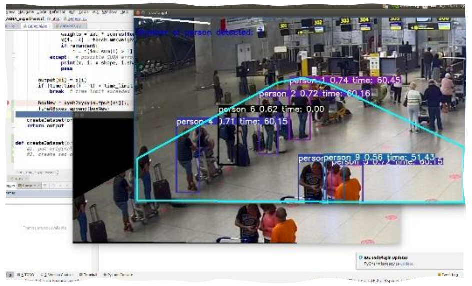


```
Frame:101
P1:
stand: 0.00
walk : 0.44
run  : 0.03
jump : 0.01
sit  : 0.00
squat: 0.00
kick : 0.52
punch: 0.00
wave : 0.00
```



```
174    check_requirements(exclude=('pycocotools
175
176    with torch.no_grad():
```

surprise
neutral
anger
happiness
fear
sadness
contempt
disgust



person 1 0.74 time: 60.45
person 2 0.72 time: 60.16
person 6 0.62 time: 0.00
person 4 0.71 time: 60.15

# Enhanced Situational Awareness

- Scalable solution for city public space security
- Use of AI for threat detection and response
- Comprehensive view of related events in a Common Operational Picture (COP)
- Demonstrate in 3 pilots
  - Trikala
  - Pilsen
  - Bilbao

# Scenario: Attack on Stadium & evacuation

- Pilsen Pilot Scenario
  - Scene: a crowded stadium (Doosan Arena, Pilsen – 600 volunteers)
  - Scenario:
    - An individual draws a weapon (gun/knife) and attacks crowd
    - Several fans are injured & chaos ensues in stands
    - Stadium is evacuated

  - S4AllCities objectives:
    - Detect attack via video analytics
    - Give comprehensive view of situation to security operators
    - Provide optimal evacuation routes
    - Provide optimal routes for first responders

# Scenario: Attack on Stadium & evacuation

vido

S4ALLCITIES

https://www.linkedin.com/in/s4allcities-project/

https://twitter.com/s4allcities

https://www.facebook.com/s4allcities

https://www.s4allcities.eu/

# THANK YOU FOR YOUR ATTENTION

Dr. Aris Bonanos

EXUS AI Labs

a.bonanos@exus.co.uk

EXUS®

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement No. 883522

# eu-LISA examples of AI activities

Anna Beata Kolodziej (IT Officer and Liaison Officer to the EU Innovation Hub for Internal Security)

23 March 2023

# eu-LISA

## European Union Agency for the operational management of large-scale IT systems in the area of Freedom, Security and Justice

# eu-LISA

- Responsible for the operational management of:
  - Eurodac
  - Schengen Information System (SIS)
  - Visa Information System (VIS)
  - ECRIS RI
  - e-CODEX (on-going handover process)

- Mandated for the development and operational management of:
  - European Entry/Exit System (EES),
  - European Travel Information Authorisation System (ETIAS)
  - European Criminal Record Information System for Third Country Nationals (ECRIS-TCN)
  - Interoperability components, shared platforms and tools (ESP, CIR, MID, CRRS, sBMS)

# AI Roadmap

# AI Roadmap

## WGAI & transversal activities

Analysis of the ongoing initiatives in MS;

Support to COM in defining use-cases, etc.

## VisaChat PoC

Developing and testing a chat-bot application for interacting with visa applicants (together with COM & MS)

## Internal AI PoC

AI in Ops,

AI in Sec,

Machine Learning/ Deep learning for biometrics

## AI in the justice domain

Contributing to the DG JUST assessment of the use-cases for JITs + report on AI in justice

## EU Security Data Space for Innovation

Supporting COM and MS in defining the requirements

## AI in ETIAS/CRRS

Under the umbrella of the EU Innovation Hub for Internal Security

# Working Group on AI (WGAI)

- Early 2021: WG established
- May 2021: First meeting
  - Mostly online or hybrid meetings

- MS, Commission and Agencies contributions:
  - DG HOME: Study on the opportunities for AI in the area of internal security, Visa Chatbot project
  - MS: AI activities in the areas of migration, border management & law enforcement
- Workshop on prioritisation of use-cases for the development/ piloting/ implementation of AI in collaboration between MS; based on the COM study: ‘Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security’

# Mandate and Scope

1 PROVIDE A REGULAR FORUM

Provide a regular forum for Member States, the European Commission, and Agencies, to exchange best practices and discuss opportunities and challenges arising from the implementation of AI-based solutions.

2 IDENTIFY USE CASES

Identify use cases for the implementation of AI solutions in the systems entrusted to eu-LISA, and prioritize them, maximizing the added value of the services provided by eu-LISA to its stakeholders.

3 DEVELOPMENT OF A COMMON APPROACH

Facilitate the development of a common approach for the use of AI-based solutions in the context of the operational management of large-scale IT systems in the JHA domain.

4 FACILITATE ALIGNMENT

Facilitate alignment across stakeholders in the practical implementation of AI-based solutions, in particular with the aim to provide standardised solutions and mitigate possible risks in their deployment.

# VisaChat

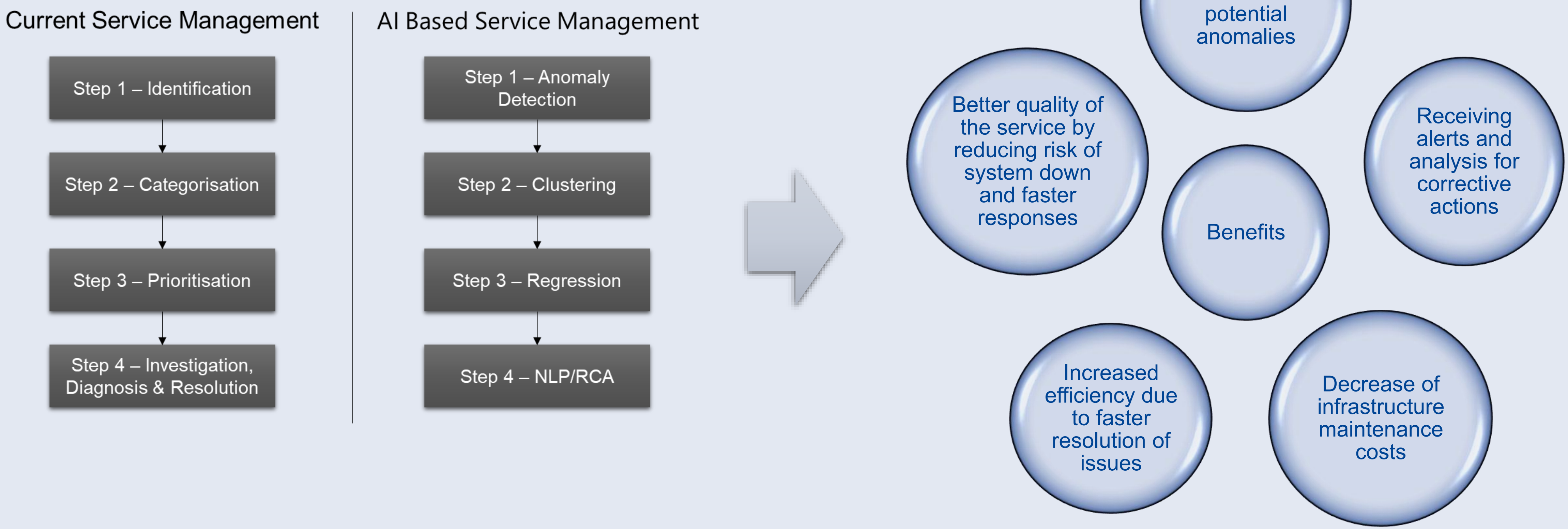
| | |
|---|---|
| COM Study in collaboration with MS and eu-LISA | Objective: Design an EU cross-border chatbot for visa processing within broader context of the Commission-led project to digitalise the visa application process |
| | 2019/2020 – AI Strategy study: Opportunities and challenges for the use of artificial intelligence in border control, migration and security |
| | 2020/2021 – Online Visa Application Platform pilot: Platform prototype where applicants could receive general and personal support for their application |
| | Aug 2021 – VisaChat kick-off: Initiation of the VisaChat Phase 1 project |
| | Nov 2021 – Future State definition: Workshop with MS and EC to validate the future state |
| | Mar 2022 – Operating model: Development and operation of the solution |
| | Currently part of the Visa Digitalisation Programme |

# AI in Operations

| | |
|---|---|
| Study and PoC on applying AI for operational management of IT Systems | Objective 1: Perform data processing, analysis and build an AI model for the implementation of a proof-of-concept, based on the application of AI to automate the process of fault identification and recovery, by using historical data |
| | Objective 2: Build up on the fault identification model (or models) and develop the related identification of correlations, detection of degradation of performance, detection of root causes and description of corrective actions |
| | Objective 3: Support the setting up of the eu-LISA AI environment by creating blueprints for its architecture and recommend the use of key technologies and functionalities for future AI related implementations |

# Expected benefits

## Moving from a manual process to an AI-driven process



Current Service Management

Step 1 – Identification

Step 2 – Categorisation

Step 3 – Prioritisation

Step 4 – Investigation, Diagnosis & Resolution

AI Based Service Management

Step 1 – Anomaly Detection

Step 2 – Clustering

Step 3 – Regression

Step 4 – NLP/RCA

Benefits

Efficient detection of potential anomalies

Receiving alerts and analysis for corrective actions

Decrease of infrastructure maintenance costs

Increased efficiency due to faster resolution of issues

Better quality of the service by reducing risk of system down and faster responses

# AI in Security

Machine learning

Machine learning to augment the SIEM (Security Information and Event Management) monitoring capabilities on both, on the corporate and the Core Business Systems (CBS)

In particular the specific machine learning algorithms applied to improve in outlier detection capabilities on network traffic and authentication log data

Currently used on production systems in the CBS and the Corporate Infrastructure

Ongoing assessment of the potential to expand this capability to other security detection use cases.

# Thank you !

eu-LISA
European Union Agency for the Operational
Management of Large-Scale IT Systems in
the Area of Freedom, Security and Justice

www.eulisa.europa.eu

- facebook.com/agencyeulisa/
- twitter.com/EULISA_agency
- linkedin.com/company/eu-lisa/
- youtube.com/c/euLISAagency

European
Commission

# Conclusions

Brussels | 23th March 2023

# Thank you!

Brussels | 23th March 2023