

CENTRIC

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

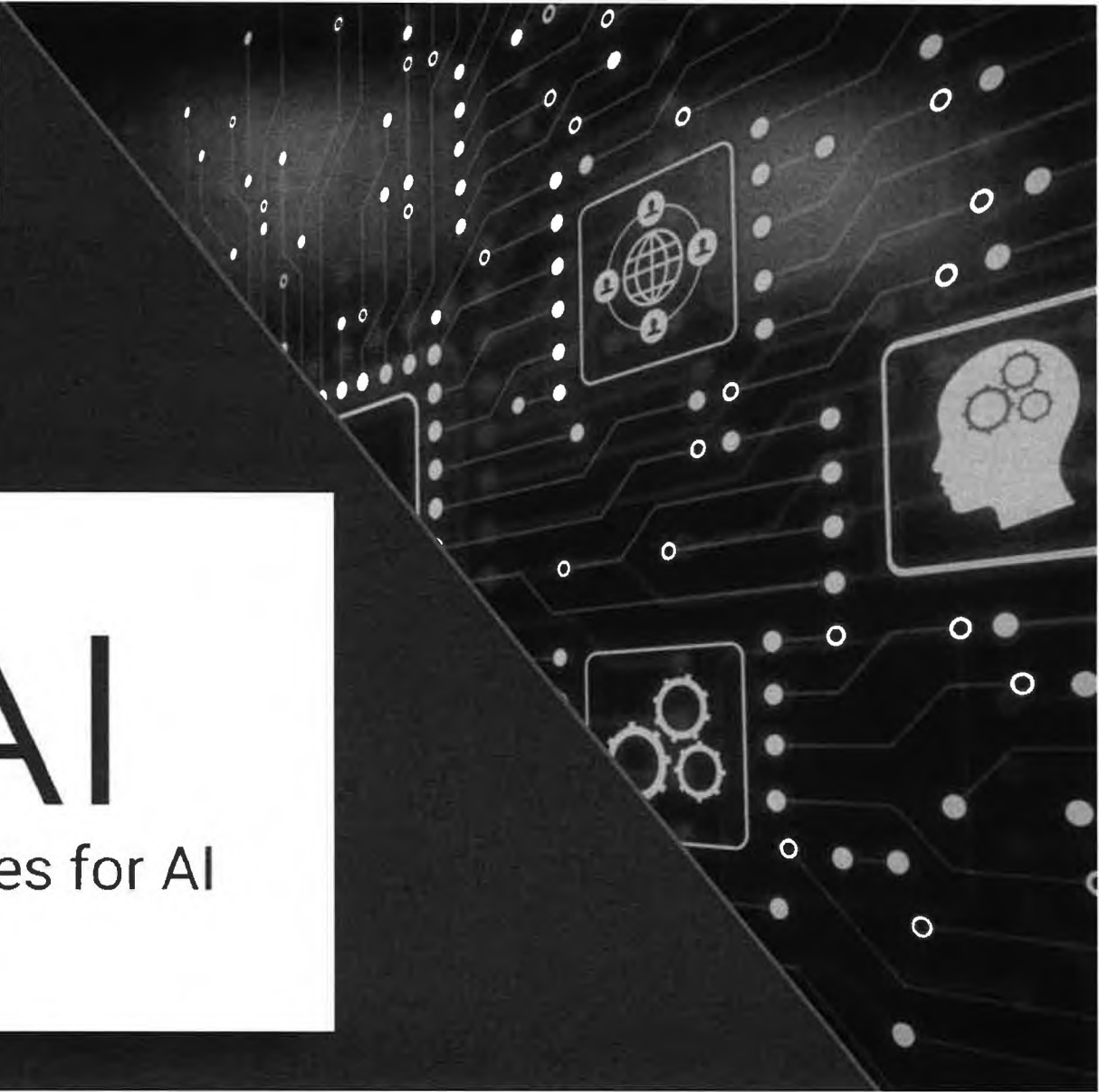
EUROPOL

INNOVATION LAB



AP4AI

Accountability Principles for AI



Session overview

10' Introduction round

20 ' Introduction to AP4AI

30' Interactive session 1

10' Coffee break

30' Interactive session 2

15' Coffee break

20' Review of discussions and next steps



AP4AI

Accountability Principles for AI



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



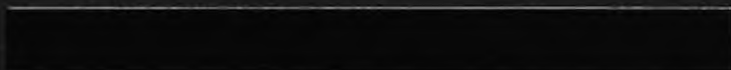
INNOVATION LAB



AP4AI

Accountability Principles for AI

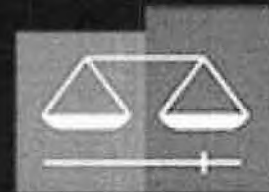
Introduction to AP4AI



Coordinators



Supporting and advising partners



EUROJUST



AP4AI Objectives

- Robust set of agreed and validated accountability principles which integrate practitioners as well as citizens' positions on AI
- Concrete, practical, actionable compliance
- Software based assessment tool for security practitioners

Create



- Security-relevant AI innovation in Europe (significant proportion developed outside Europe)
- EU-R&D (e.g., facilitate social acceptability of future AI tools and capabilities)
- Proposed EU AI Act

Support



AP4AI Framework – Why an Accountability Framework?

Accountability is bound to enforceable obligations and thus actionable.

A practical mechanism to ensure that legitimate interests (as well as concerns, fears and hopes) of all stakeholders are engaged with and factored in throughout the full decision-making process about LEAs' AI capabilities.

Organisational accountability in general (e.g. LED, FR or GDPR) is a well-established concept, at present there is no firm definition of LEA accountability in the context of AI.

(Akhgar/Bayerl, 2021)

**Accountability as
core requirement**

**justification
monitoring
enforcement**

Methodology: Expert driven, Citizen focus, bottom up approach

Law enforcement agencies

Citizens

Judiciary

Human rights experts

Ethical AI experts

Civil society organisations

AI developers / industry

Academia / Research



Cycle 3 – Expert validation



Cycle 2 – Citizen consultation
(30 countries, n = 6,674)



Cycle 1 – Expert consultation and
state-of-the-art review

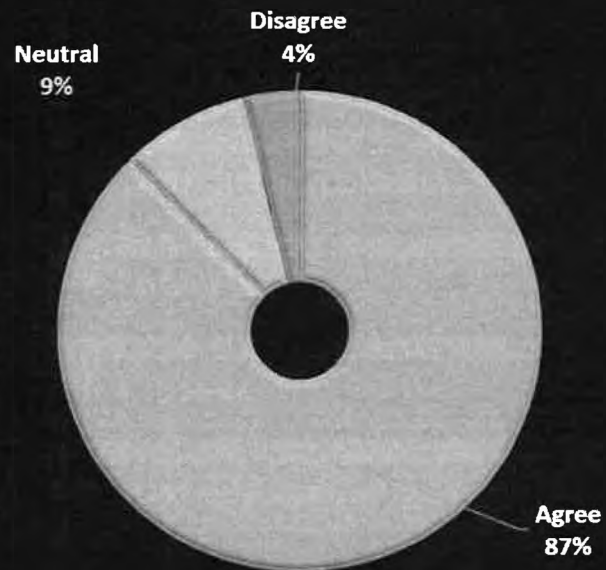


CITIZEN CONSULTATION across 30 countries

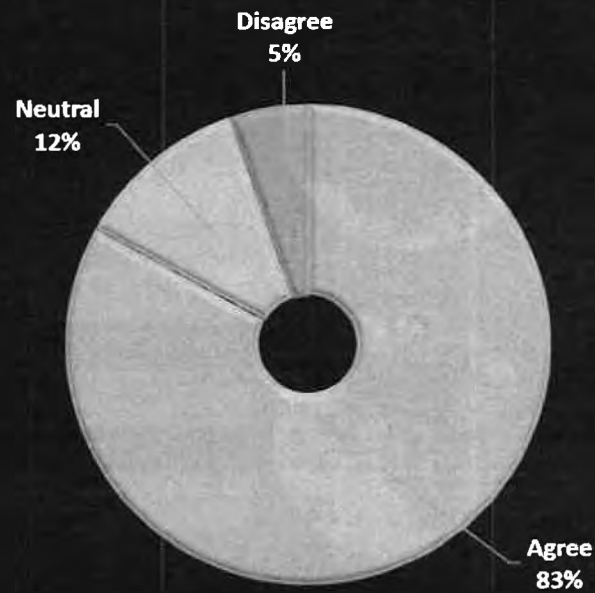
Please note: Results are presented as summaries across all 30 countries (n = 6,591, weighted data, merged categories)

BENEFITS OF AI

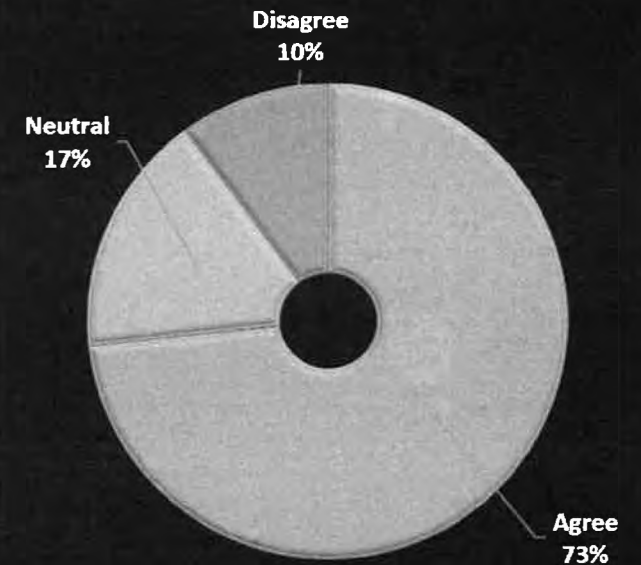
POLICE SHOULD USE AI TO SAFEGUARD CHILDREN AND VULNERABLE GROUPS FROM EXPLOITATION.



POLICE SHOULD USE AI TO DETECT CRIMINALS AND CRIMINAL ORGANISATIONS.



POLICE SHOULD USE AI-BASED PREDICTION TOOLS TO PREVENT CRIMES BEFORE THEY CAN HAPPEN.

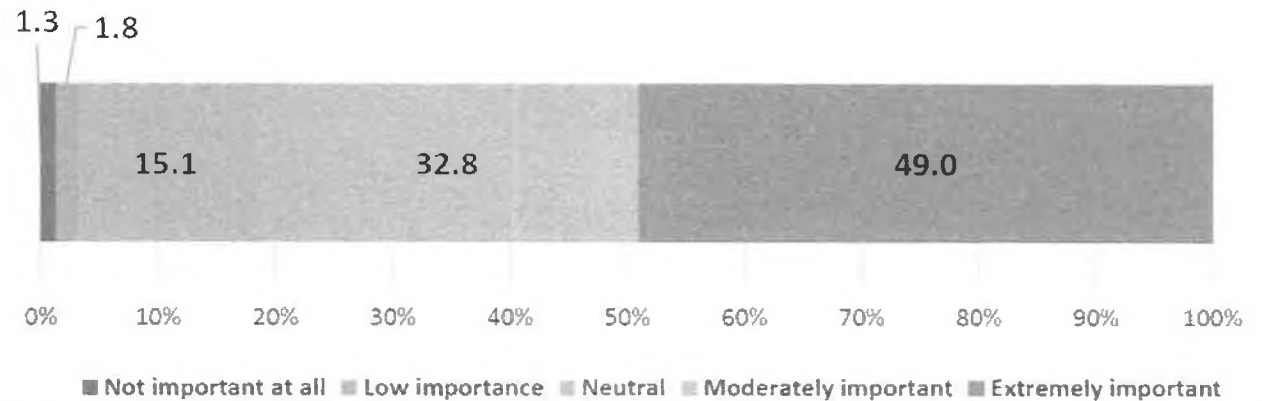


CITIZEN CONSULTATION across 30 countries

Please note: Results are presented as summaries across all 30 countries (n = 6,591, weighted data, merged categories)

HOLDING POLICE ACCOUNTABLE

HOW IMPORTANT IS IT THAT A UNIVERSAL FRAMEWORK IS CREATED THAT ENSURES THE ACCOUNTABILITY OF AI USE BY POLICE?





Review of existing approaches, frameworks (including laws, regulations)

Expert consultations (international, cross-disciplinary)



Expert validation

- AP4AI Principles**
1. Legality
 2. Universality
 3. Pluralism
 4. Transparency
 5. Independence
 6. Commitment to Robust evidence
 7. Enforceability and Redress
 8. Compellability
 9. Explainability
 10. Constructiveness
 11. Conduct
 12. Learning Organisation



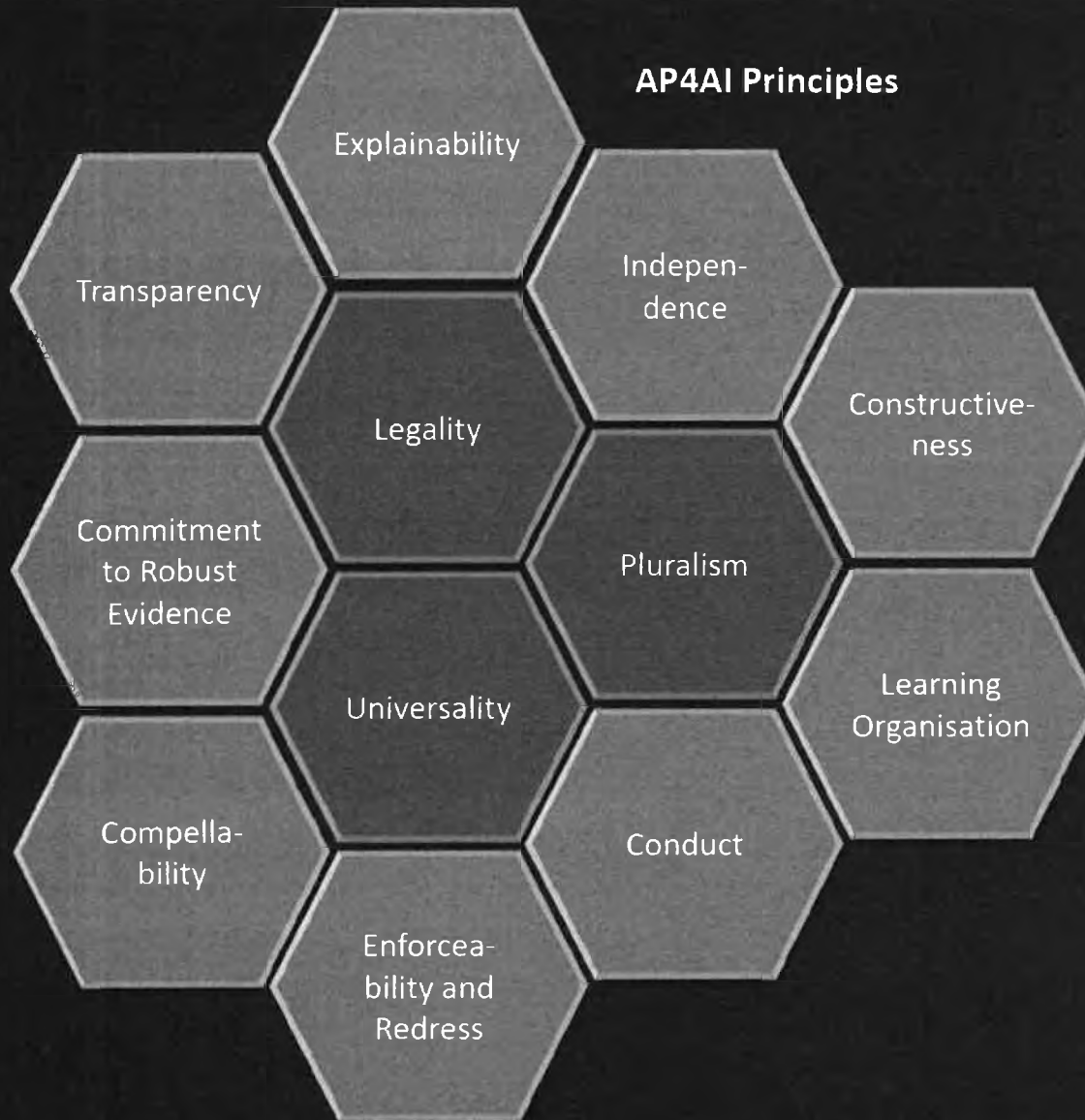
Citizen consultation

AP4AI Framework Blueprint
-> AAA, Implementation mechanism

AP4AI Online Tool

AP4AI Training package
Kite Marking

AP4AI Principles



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

Accountability Principle: Implementation Guidance

Name – Principle name, validated in expert consultations

Meaning – provides the Principle definition contextualised for AI and the internal security domain

Materiality threshold – offers an assessment of the relative impact that something may have an accountability within AI development or utilisation

Examples of applicable law – lists examples of applicable law pertinent to AI Accountability in the internal security domain

Note on Human Right Impact Assessment – provides an initial direction for HRIAs and alerts the reader about the pivotal role of HRIAs in the context of AI Accountability Principles

Note on Data Protection Impact Assessment (DPIA, where applicable) – alerts the reader to legal and ethical requirements of conducting a DPIA and, where applicable, a Privacy Impact Assessment (PIA)

Implementation guide – identifies the processes, activities, tasks, documentations, assessments, actions and communication needed for the realisation of the Principle

Operational considerations – provides clarification and further consideration about implementation of the principles for the operational environment

UNIVERSALITY

Meaning

Universality provides that *all* relevant aspects of AI deployments within the internal security community are covered through the accountability process. Effectively extending the 'jurisdiction' of the Principles to all who are subject to the Legality principle (above), this principle recognises the reality that AI applications are necessarily multi-partner input programmes in a frequently complex process and the need for public trust and confidence must extend to the whole ecosystem. This is not only in respect of the deployment of AI in a criminal justice context, but in all the related processes, including design, development and supply, to which accountability applies equally (including all domains, aspects of police mission, AI systems, stages in the AI lifecycle or usage purposes), and prevents contracting out or offshoring by the relevant accountable organisation.










Materiality threshold

While all organisations and individuals having a significant impact on/involvement with the AI programme must be subject to the Principles, there will be those whose role is too remote from the inputs/outcomes to be included. Examples might include some people who are purely involved in the technical installation of agreed equipment or provide generic project management support (they can be identified in the project's documentation). Universality applies a holistic, catch-all provision to ensure there are no significant accountability gaps, but there will be many potential impacts and outcomes of the project not all of which will be of sufficient relevance/importance to be included. Similarly, some technical processes may not be of sufficient relevance to accountability to be included.

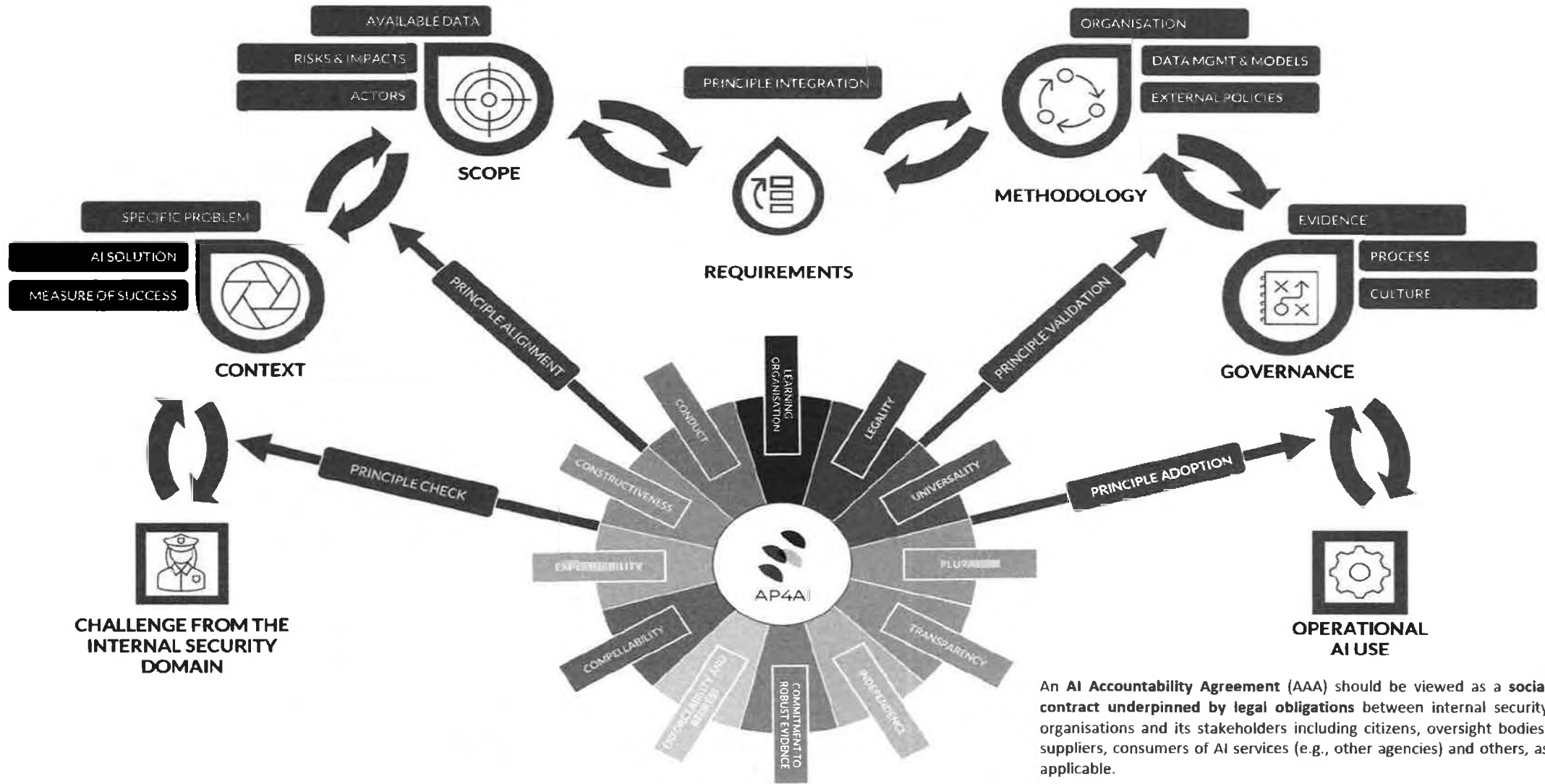
Examples of applicable laws

- National, European and International legal instruments, conventions, declarations and agreements specifically pertaining to Fundamental Rights and freedoms, and secondary provisions relating to identified groups in the same respect.
- National and European legal instruments, conventions and agreements relating to the processing of personal data for criminal justice purposes.
- National laws protecting or creating individual rights in respect of the exercise of powers by police and law enforcement agencies.
- National criminal justice procedural laws, rules and directions, particularly in respect of fairness, presumption of innocence and the prevention of arbitrary decision-making.
- Industry or sector-specific legal standards relating to public safety.
- National and sector-specific tribunals and formal procedures providing means of effective redress in applicable contexts.

Notes on Human Right Impact Assessment and Data Protection Impact Assessment

<h4>AI LIFECYCLE MANAGEMENT</h4> <p>Apply to all components and the complete AI system lifecycle, from design to decommissioning.</p>  <p>What is the goal of the AI system?</p> <p>Who is involved in the development process & what are their roles?</p> <p>Who decides which metrics are optimised?</p> <p>Who defines the training/testing datasets?</p> <p>Who defines the feature selection?</p> <p>Who determines error trade-offs and error discrepancies?</p> <p>Map the entire process, roles and feedback loops & communication.</p>	<h4>OUTCOMES AND IMPACTS</h4> <p>Have all outcomes and possible impacts of AI deployment been considered?</p>  <p>Conduct a fundamental rights and legal impact assessment.</p> <p>Identify risks, appropriate mitigation measures & safeguards.</p> <p>Respect privacy and data protection.</p> <p>Cybersecurity and privacy preserving measures.</p> <p>Deal about marginalised or vulnerable groups.</p>	<h4>STAKEHOLDERS</h4> <p>Have all relevant stakeholders been considered including national regulators and oversight bodies?</p>  <p>Are national stakeholders involved in development?</p> <p>AI ethicists, human rights experts and affected groups involved.</p> <p>Is there an alternative human/technical system?</p>
<h4>UP / DOWNSTREAM PROCESSES</h4> <p>Have all processes affected by AI been accounted for?</p>  <p>Process documentation access and storage for review.</p>	<h4>MEASURING COMPLIANCE</h4> <p>How is compliance with this principle measured? Who is responsible for this?</p>  <p>Is there an system of external/peer assessment?</p>	<h4>SOCIETY AND INCLUSIVITY</h4> <p>What efforts have been made to understand and address concerns and legitimate expectations of specific sections of society and individuals having characteristics requiring additional consideration.</p>  <p>How and when are societal actors consulted & made knowledgeable?</p>
<h4>RESPONSIBILITIES</h4> <p>Does everyone understand their responsibilities in respect of compliance with accountability? How is this ensured?</p>  <p>Define and map the responsibilities for each of role.</p> <p>What are the developer and users responsibilities for impact.</p> <p>Map the chain of accountability from design to deployment.</p> <p>Define the logging protocol for operational workflow.</p> <p>Define the external auditing and oversight for workflow.</p>	<h4>OVERSIGHT OBLIGATIONS</h4> <p>What quality assurance and bias mitigation processes do you have in place for the data lifecycle - for both acquired and collected data?</p>  <p>Who is responsible for systems design?</p> <p>Who is responsible for system implementation and outcome?</p> <p>Who maintains the user feedback and response?</p> <p>Who is responsible to double-check challenges from individuals?</p>	<h4>REASONABLE RISK</h4> <p>What are the remaining security and privacy risks and why are they reasonable?</p>  <p>Understand risks and levels of unfairness.</p> <p>What is the potential harm if the AI system is misused?</p>

AI ACCOUNTABILITY AGREEMENT (AAA) PROCESS



An AI Accountability Agreement (AAA) should be viewed as a social contract underpinned by legal obligations between internal security organisations and its stakeholders including citizens, oversight bodies, suppliers, consumers of AI services (e.g., other agencies) and others, as applicable.



“To recognise always that the power of the police to fulfil their functions and duties is dependent on public approval of their existence, actions and behaviour, and on their ability to secure and maintain public respect.”

Sir Robert Peel, Policing Principles, 1829



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



INNOVATION LAB



AP4AI

Accountability Principles for AI

Interactive session 1



Implementation for core application areas (“scenarios”)

- Investigation of CSE and categorisation of CSEM (Child Sexual Exploitation Materials) Investigation of cyber-dependent crime
- Identification and prediction of serious and organised crime activities including cross-border issues
- Detection of harmful internet content such as terrorist generated internet content
- Protection of public spaces and communities
- Investigation of terrorism (including CVE) related offences
- Investigation and prosecution of financial crime (e.g., money laundry)
- Procurement of AI solutions by internal security practitioners
- Research and development for AI either by the LEA or a 3rd party intended to create the solution to be deployed for the internal security domain

Implementation support



Email

You will receive a 4 digit pin.



Create a new report

You don't have any reports yet!

- 1 Application of law
0% completed
- 2 Necessity and proportionality
0% completed
- 3 Legislative gaps
0% completed
- 4 Demonstration of compliance
0% completed
- 5 Quality assurance
0% completed
- 6 Data provider and purpose
0% completed
- 7 Residual risks
0% completed
- 8 Exemptions and safeguards
0% completed
- 9 Privacy harms
0% completed
- 10 Objective oversight
0% completed
- 11 Equality
0% completed
- 12 Public concerns
0% completed

Step 1 / Application of law

How do the applicable laws apply in this context?

Check the list of applicable laws
Tooltip explaining what this field is for...

- National, European and international legal instruments, conventions, declarations and agreements specifically pertaining to Fundamental Rights and freedoms, and secondary provisions relating to identified groups in the same respect
- National and European legal instruments, conventions and agreements relating to the processing of personal data for criminal justice purposes.
- National laws protecting or creating individual rights in respect of the exercise of powers by police and law enforcement agencies.
- National and criminal justice procedural laws, rules and directions, particularly in respect of fairness, presumption of innocence arbitrary decision-making
- National industry or sector-specific legal standards relating to public safety.
- National and sector-specific tribunals and formal procedures providing means of effective redress in applicable contexts.

Check for infringements against rights and freedoms
Tooltip explaining what this field is for...

Type something here...

Involve data protection and human rights experts
Tooltip explaining what this field is for...

Type something here...

- 1 Application of law
0% completed
- 2 Necessity and proportionality
0% completed
- 3 Legislative gaps
0% completed
- 4 Demonstration of compliance
0% completed
- 5 Quality assurance
0% completed
- 6 Data provider and purpose
0% completed
- 7 Residual risks
0% completed
- 8 Exemptions and safeguards
0% completed
- 9 Privacy harms
0% completed
- 10 Objective oversight
0% completed
- 11 Equality
0% completed
- 12 Public concerns
0% completed

Step 1 / Application of law

How do the applicable laws apply in this context?

Check the list of applicable laws
Tooltip explaining what this field is for...

- National, European and international legal instruments, conventions, declarations and agreements specifically pertaining to Fundamental Rights and freedoms, and secondary provisions relating to identified groups in the same respect
- National and European legal instruments, conventions and agreements relating to the processing of personal data for criminal justice purposes.
- National laws protecting or creating individual rights in respect of the exercise of powers by police and law enforcement agencies.
- National and criminal justice procedural laws, rules and directions, particularly in respect of fairness, presumption of innocence arbitrary decision-making
- National industry or sector-specific legal standards relating to public safety.
- National and sector-specific tribunals and formal procedures providing means of effective redress in applicable contexts.

Check for infringements against rights and freedoms
Tooltip explaining what this field is for...

Regularly done by the supervision through their inspections, but also via Europol's consultations and notifications as well as processes established by Europol itself.

Involve data protection and human rights experts
Tooltip explaining what this field is for...

The DPO is constantly involved where necessary due to applicable laws, but also pre-emptively where possible and advice is needed within Europol

Legality

All aspects and activities of AI accountability must be exercised in accordance with the law.



Universality

Universality requires that all aspects of AI use fall under the remit of accountability.



Pluralism

Ensures participation by all key public and private stakeholders promoting their democratic and collaborative engagement.



Transparency

Ensures availability and ready accessibility of information pertinent for assessing and enforcing accountability to all relevant stakeholders.



Independence

Guarantees that monitoring and enforcement are independent from the people and/or organisations that design implement and/or use the AI system.



Commitment to robust evidence

Ensures that mechanisms are in place that lead to robust evidence which forms the basis for the assessment and enforcement of AI systems and their usage.



Enforceability and redress

Ensures mechanisms are in place to enforce relevant obligations (legal, ethical, AP4AI) and recommend accountability oversight bodies as well as to guarantee implementation of remedies in case of negative consequences or grievances.

Compellability

Requires that obligations are in place that ensure oversight bodies with access to required information systems or individuals.

Explainability

Ensures that AI practices, systems and decisions explained.

Constructiveness

Ensure a dialogical process between law enforcement and judicial actors, and those performing accountability functions, that is enabling and responsive.

Conduct

Requires AI practices of LEAs follow professional ethical standard.

Learning Organisation

Ensure the willingness and ability of organisations change current AI practices based on new knowledge insights.

Legality

All aspects and activities of AI accountability must be exercised in accordance with the law.

Application of law

How do the applicable laws apply in this context?



Necessity and proportionality

Are the overriding principles of necessity and proportionality complied with?



Legislative gaps

Some aspects of AI usage, including new developments and capabilities, may not be regulated in existing laws and standards.



Demonstration of compliance

How can compliance be demonstrated?



Quality assurance

What quality assurance and bias mitigation processes do you have in place for the data lifecycle - for both acquired and collected data?



Data provider and purpose

Will any data being used in the production of the AI system be acquired from a vendor or repurposed from existing datasets?



Residual risks

Despite legal compliance, any residual risks particular to AI should be addressed.

Exemptions and safeguards

Do any legal exemptions apply? If so, are appropriate safeguards in place?

Privacy harm

Does the use of AI deal with special categories of personal data, as defined by applicable legal norms?

Objective oversight

Is the appropriate oversight body engaged, in respect of the activity?

Equality

An equality impact assessment (EIA) should be conducted considering impacts on affected individuals

Public concerns

Legal compliance alone may not address wider public concerns.



Create a new report

Report	Completion	Actions
Report #01 - 21/09/2022	100%	Edit Download
Report #02 - 21/09/2022	30%	Edit Download

New report - 21/09/2022
100% completed

Save

Exit

Your report has been generated!

Accountability principles framework

21/09/2022



Principle 1 - Legality

Step 1 / Application of law

How do the applicable laws apply in this context?

Check the list of applicable laws

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean feugiat iaculis elit id sodales. Nam aliquam cursus erat, vitae rhoncus sem porttitor in. Suspendisse quis risus vitae urna dapibus rutrum. Aenean ac fermentum metus. Sed rhoncus posuere nibh vel fringidit. Integer eu diam ac mauris scelerisque facilisis. Cras maximus, neque in facilisis aliquam, velit magna semper nibh, ac tempus orci nisi id massa.

Download

Coffee Break
10 min

CENTRIC

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

EUROPOL

INNOVATION LAB



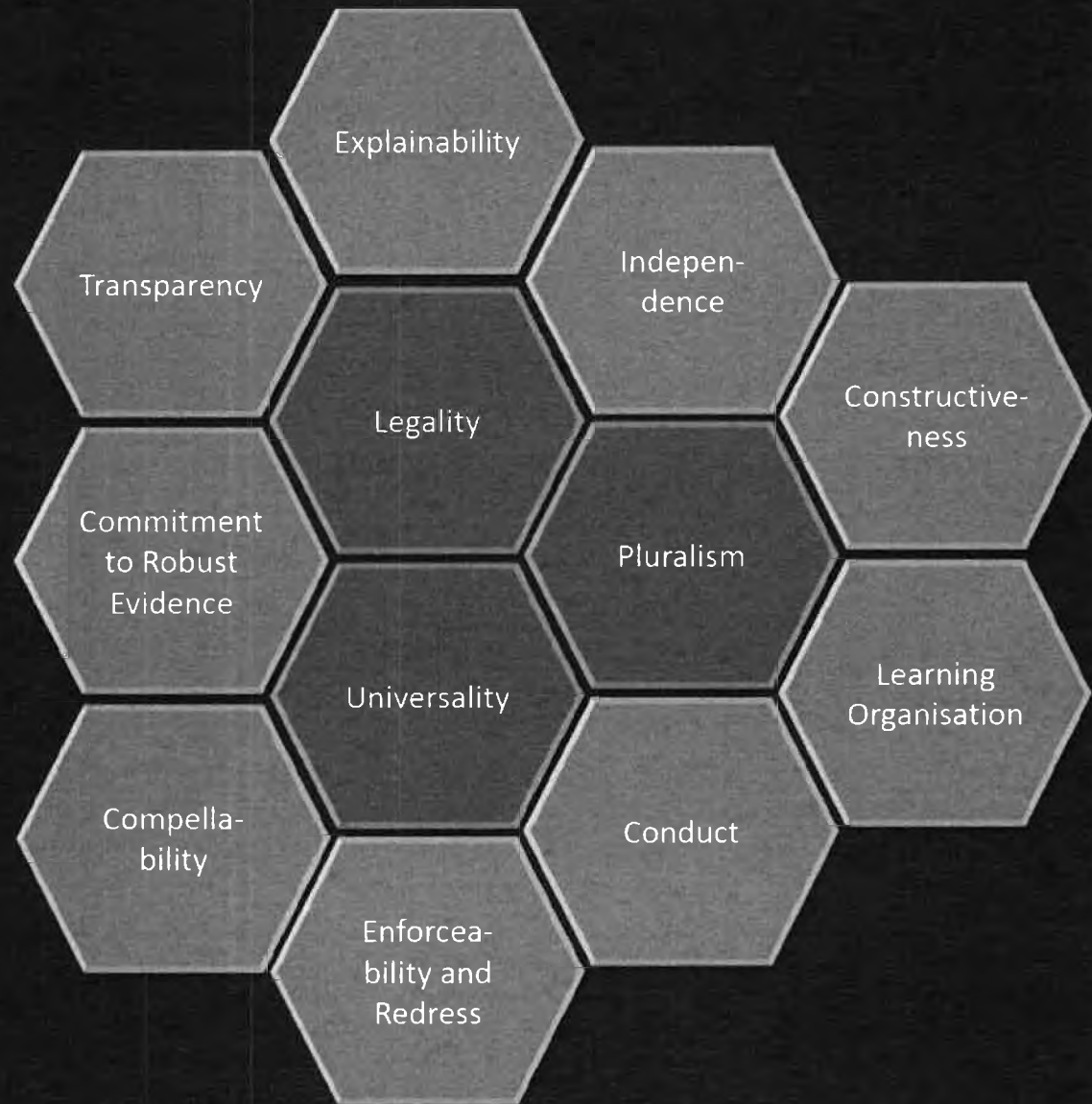
AP4AI

Accountability Principles for AI

Interactive session 2



AP4AI Principles



Conduct

all police uses of AI
strictly follow
professional
standards

- **Personnel obligations:** Are all the people involved in making AI and putting it into place aware of their responsibilities and those of their teams?
- **Oversight bodies:** How are the rights and mechanisms of oversight bodies linked to existing LEA-internal processes with respect to AI principles?
- **Existing frameworks:** Are existing AI frameworks relevant for conduct?
- **Process documentation:** The processes facilitating accountability in respect of Conduct should form part of the information made available in respect of specific deployments of AI under the transparency principle.
- **Available remedies:** What remedies are available to and readily accessible by the complainant?
- **Complaints procedure:** How are complaints documented?

Pluralism

every group involved
in and affected by AI
use has a voice in
monitoring and
assessing police use
of AI

AI lifecycle management: Are all components and the complete AI system lifecycle, from design to decommissioning, considered?

Stakeholder evolution: Should stakeholders remain the same at all stages of accountability procedures and engagements?

Procedural information: Has all the information about procedures been given in a way that is clear and makes sense? Does this also manage expectations?

Stakeholder roles: Do participants understand their role within the process and the purpose of it?

Engagement strategies: In the true spirit of being open to everyone, have a variety of ways to get involved been used?

Citizen engagement: What form should citizen engagement take?

LEAs engagement: In which form should law enforcement agencies be included?

Universality

every aspect of AI use without exception can be monitored and assessed

- **AI lifecycle management:** Are all components and the complete AI system lifecycle, from design to decommissioning, considered?
- **Up/Downstream processes:** Have all processes affected by AI been accounted for?
- **Responsibilities:** Does everyone understand their responsibilities in respect of compliance with accountability? How is this ensured?
- **Outcomes and impacts:** Have all the outcomes and possible impacts of AI's deployment been considered?
- **Measuring compliance:** How is compliance with this principle measured? Who is responsible for this?
- **Oversight obligations:** What quality assurance and bias mitigation processes do you have in place for the data lifecycle for both acquired and collected data?
- **Stakeholders:** Have all relevant stakeholders been considered, including national regulators and oversight bodies?
- **Society and inclusivity:** What efforts have been made to understand and address the concerns and legitimate expectations of specific sections of society and individuals having characteristics requiring additional consideration?
- **Reasonable risk:** What are the remaining security and privacy risks and why are they reasonable?

Transparency

all information to assess AI use + to enforce consequences is easily + fully accessible to groups that judge police use of AI

- **Recipients:** Who needs to offer Transparency? And to whom?
- **Public concerns:** Are public concerns being addressed when making decisions about Transparency?
- **Dataset scope:** Consider the importance of the size, nature, and source of the datasets being used and the criteria for algorithmic processes.
- **Maximisation:** Maximising Transparency should be considered at all stages, from system development to results.
- **Delivery:** Make sure that Transparency is done in a timely, meaningful, and appropriate way.
- **Measurement:** What methods and standards are used to decide if the principle of Transparency Where has been followed enough?
- **Restrictions:** Are public concerns being addressed when making decisions about Transparency?

Independence

people/groups that monitor police + enforce consequences are totally independent from police + organisations that design AI systems for police

- **Operational definition:** Determine the nature and extent of Independence in a practical sense.
- **Limitations:** Determine potential practical or legal limitations to the overall aim of Independence
- **Regulatory relationships:** How are relationships of the accountability oversight body regulated with pre-existing oversight bodies?
- **Scope:** If total Independence is not possible, which form, and level of Independence is (in)appropriate?
- **Knowledge acquisition:** How will oversight bodies acquire the necessary specialist knowledge to be able to carry out informed, effective decision-making?
- **Completeness:** Information being provided to the oversight body must be adequate for the purpose of accountability.
- **LEA positioning:** Does independence exclude LEAs from accountability bodies?
- **Communication:** Have effective lines of interaction and communication with the oversight body been established?
- **Process relationships:** How are relationships between accountability processes regulated if (non-AI specific) accountability processes are already in place?
- **Component procurement:** If an institution is procuring parts or elements of the system from third parties, how are they instituting appropriate governance controls?
- **Data procurement:** If third-party data is being used in the production of the AI system, how are they instituting appropriate governance controls across the data lifecycle?

Commitment to Robust Evidence

police are committed to providing evidence that is so robust that their AI use can be judged with confidence

- **Operational definition:** How to define and assess "robustness", and who is responsible to determine "robustness"?
- **Process management:** Are these processes and procedures documented and understood by those who need to know?
- **Resilience:** Is the evidence sufficiently robust for these purposes?
- **Intention:** For what purposes might the evidence be used?
- **Evidence capture:** Are processes and procedures in place to allow the capture of the evidence in the required way?
- **Storage and access:** Is the evidence stored in a meaningful and accessible way?
- **Evidential constraints:** Is the evidence in its original form subject to legal or sector-specific constraints?
- **Interpretation:** How should non-AI experts learn to interpret AI outputs in the evidential context?

Enforceability and Redress

it is possible to compel police to comply with all requests to improve their AI practices

- **Obligations:** Which obligations are capable of enforcement?
- **Fulfilment:** Who determines whether obligations have been fulfilled?
- **Selection:** Which forms of redress will be chosen and how are they related to existing (national, international) redress possibilities?
- **Responsibility and independence:** Who determines the appropriate level of redress?
- **Comprehension:** Have steps been taken to ensure that the enforceability mechanisms are clearly understood?
- **Conflict resolution:** Has a conflict resolution and escalation process been identified?
- **Intervention:** When and for what reasons can regulators intervene?
- **Harm management:** Are there internal responsibility procedures in place to address any unintended harm caused by the design, development, or deployment of AI?
- **External oversight:** Are there any internal or external monitoring, auditing, or oversight procedures for evaluating the use of AI and assessing their impact on users or other individuals or groups?
- **Human oversight:** Is there continuous and effective human oversight over decisions made based on AI findings?
- **Accessibility:** Is information relating to obtaining an effective remedy clear, easily understood, and accessible?
- **Contestability:** Are there options for people affected by a decision to learn about the output of the automated system and to challenge predictions, recommendations, or decisions influenced by the system?
- **Recourse:** Is there any recourse available for any harm caused by AI during the decision-making process, such as complaints or appeal procedures?
- **Reversibility:** Is the harm of a wrong decision by the AI system fully reversible?

Constructiveness

police/groups that assess police use of AI always have a constructive attitude in their negotiations with each other

- **Mechanisms and safeguards:** What are the mechanisms to safeguard Constructiveness in discussions and negotiations?
- **Risk management:** Has this principle's specific risk(s) been added to the risk register?
- **Communication:** How is communication managed internally and externally to ensure this principle does not dilute accountability and transparency?
- **Disconnect:** How to handle actors that fail to adhere to a basic foundation of Constructiveness?
- **Engagement:** Has an independent spokesperson been chosen who can talk about the most important questions of accountability that come up at each stage of the project?

Compellability

it is possible to compel police to provide access to all necessary information, systems or individuals to judge their use of AI

- **Oversight capacity:** The oversight body's role and authority, functions and powers should be determined
- **Oversight powers:** On what grounds can oversight bodies interrupt, interrogate, or compel LEAs or programme partners, either directly or via national bodies such as regulators?
- **Requirements:** What process is in place to clarify and explain what is required in respect of information and access?
- **Information security:** Have legal and industry-specific obligations for information security been met?
- **Security and safeguards:** What security measures and other safeguards are in place in respect of the provision of information?
- **Notification:** What methods are used to tell LEAs about compellability and carry out actions related to it?
- **Non-compliance:** Have the sanctions or consequences of noncompliance been clearly communicated?

Explainability

all AI practices,
systems and
decisions can be fully
explained to the
public and oversight
bodies

- **Scope of application:** Explainability is relevant for which aspects of AI or AI usage?
- **Fulfilment:** How to determine whether Explainability has been satisfied? Who judges whether Explainability has been satisfied?
- **Communication strategies:** Are clear communication strategies in place that account for the different needs of individuals and groups?
- **Risks and consequences:** Is there a clear understanding of the significant risks and consequences of not complying with this principle?
- **Effectiveness:** How is the effectiveness of this principle measured?
- **Review mechanism:** Have mechanisms to facilitate reviews, challenges, and complaints been established?

Learning Organisation

police are continually willing to change their current AI practices based on new knowledge and insights

- **Understanding:** How do security practitioners learn about or are informed about aspects that need to be adapted?
- **Stakeholders:** Is learning only needed for security practitioners, or are other groups equally required to make adjustments?
- **Knowledge management:** How is learning codified to ensure it remains available, replicable, and can spread within the organisation and/or sector?
- **Resource availability:** Are there sufficient resources in place to enable and sustain the learning?
- **Evaluation:** Are there sufficient resources in place to enable and sustain the Learning?

Legality

AI use is entirely in line with the law

- **Application of law:** How do the applicable laws apply in this context?
- **Necessity and proportionality:** Are the overriding principles of necessity and proportionality complied with?
- **Legislative gaps:** Are there aspects of AI usage, including new developments and capabilities, that are not regulated by existing standards?
- **Demonstration of compliance:** How can compliance be demonstrated?
- **Quality assurance:** What quality assurance and bias mitigation processes do you have in place for the data lifecycle - for both acquired and collected data?
- **The data provider and purpose:** Will any data being used in the production of the AI system be acquired from a vendor or re-purposed from existing datasets?
- **Residual risks:** Despite legal compliance, are any residual risks particular to AI addressed?
- **Exemptions and safeguards:** Do any legal exemptions apply? If so, are appropriate safeguards in place?
- **Privacy harm:** Does the use of AI deal with special categories of personal data as defined by applicable legal norms?
- **Objective oversight:** Is the appropriate oversight body engaged in the activity?
- **Equality:** Should an equality impact assessment (EIA) be conducted, considering impacts on affected individuals?
- **Public concerns:** Apart from legal compliance, are there wider public concerns that need to be addressed?

Coffee Break
15 min



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



INNOVATION LAB



AP4AI

Accountability Principles for AI

Review of discussions +

Outlook for AP4AI



Outlook for AP4AI and next steps

- Extension of use cases and application scenarios (AI deployment) – including additional use cases identified in this session – in collaboration with Starlight project (H2020, #101021797)
- Further validation and instantiation of the AI Accountability Agreement using examples and challenges from internal security practitioners
- Further development of the software application as a supporting mechanism for the implementation of AP4AI



AP4AI

Accountability Principles for AI

ap4ai.eu



CENTRIC

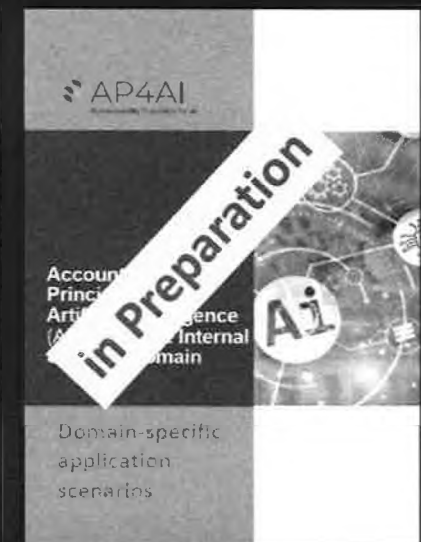
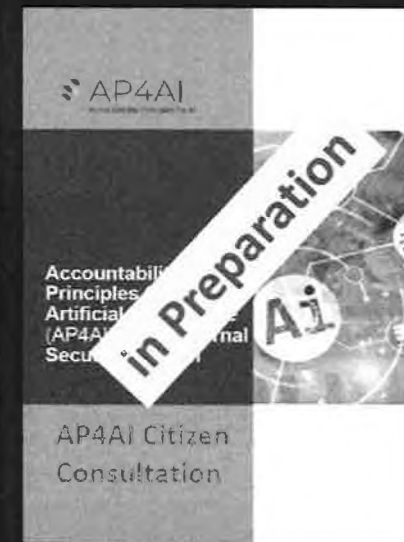
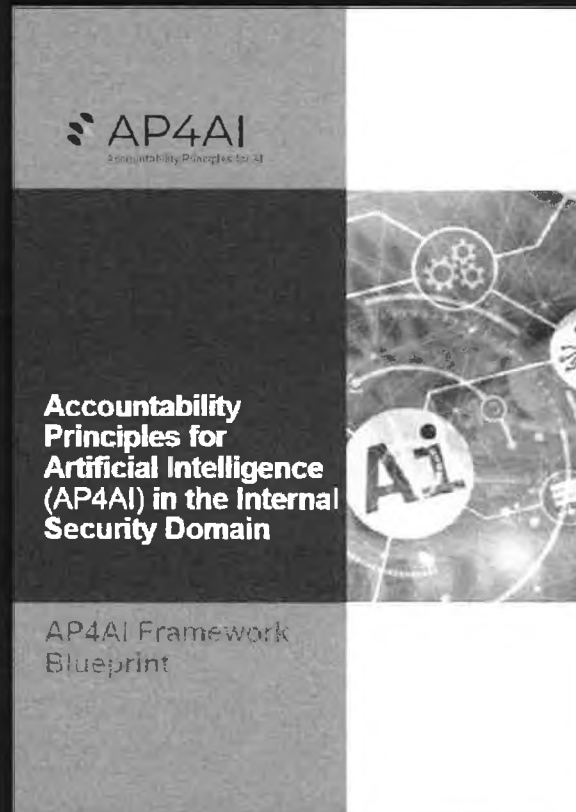
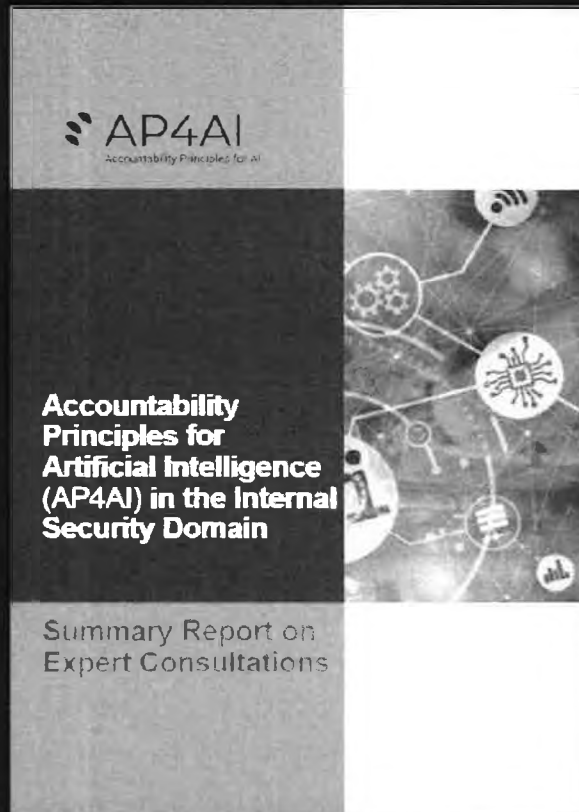
Centre of Excellence in Terrorism,
Resilience, Intelligence and
Organised Crime Research



 **EUROPOL**


INNOVATION LAB

Available from www.ap4ai.eu



Website: www.ap4ai.eu

Twitter: @AP4AI_project

Email: Innovation-lab@europol.europa.eu;
CENTRIC@shu.ac.uk

