



A project of the European Anti-Cybercrime Technology Development Association (EACTDA)



D2.6 Report on contributions to policy making, standardisation, and other knowledge building activities



Co-funded by
the European Union

Version:	1.0	
Delivery date:	June 2025	
Dissemination level:	Public	
Status	FINAL	
Nature:	Report	
Main author(s):	Juan Arraiza	EACTDA
Contributor(s):	Rimantas Žylius (L3CE seconded to EACTDA)	EACTDA

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
0.1	12/09/2023	Juan Arraiza (EACTDA)	TOC and initial text
0.2	18/10/2023	Juan Arraiza (EACTDA)	First version for all sections completed. Requested contributions from EACTDA members and key stakeholders.
0.3	08/05/2025	Juan Arraiza (EACTDA) Rimantas Žylius (L3CE seconded to EACTDA)	Updated with received feedback
1.0	30/06/2025	Juan Arraiza (EACTDA)	Final version, ready to be submitted

TABLE OF CONTENTS

1. Introduction	4
1.1. Overview of the Tools4LEAs project	4
1.2. Main objective of this document.....	5
1.3. Relation to other deliverables	5
1.4. Structure of the deliverable.....	5
2. Summary of Policy Making activities	7
3. Summary of Standardisation activities	8
4. Summary of other knowledge building activities	9
5. Summary.....	10
5.1. Conclusion	10
5.2. Evaluation	10
5.3. Future work	10
ANNEX I – Position paper on datasets management for the EU security research and innovation value chain	11
ANNEX II – Law Enforcement AI with EU Requirements.....	21

1. Introduction

1.1. Overview of the Tools4LEAs project

EACTDA is the acronym of the European Anti-Cybercrime Technology Development Association, which is a private non-profit association, established in San Sebastian, Spain. The members of the Association include European Union (EU) public entities fighting cybercrime, universities and research technology organisations, for-profit private companies, and other relevant actors in the field of the EU security research and innovation.

The Tools4LEAs projects are a series of projects that receive a Direct Award under the ISFP programme, and which main goal is to facilitate and promote the uptake of innovative technologies by EU public entities fighting cybercrime. EACTDA, via the Tools4LEAs projects, aims at further developing pre-existing assets, mainly from EU-funded security research and development projects, so that they are offered with no license cost and with access to the source code to EU public entities fighting cybercrime.

In the first Tools4LEAs project (v1; Jul'21 to Jun'23), the focus was on designing and setting up the infrastructures, processes, and governance / decision-making mechanisms, whilst delivering the first set of “fully-tested and operational-ready” tools via Europol's Tool Repository. Though 11 tools were further developed in the v1 project, it is expected that 3 of them will not be released to their targeted audience as they do not pass the pre-established quality threshold of “operational-ready”. Also, an End-User Advisory Board (EUAB) composed as of Jun'25 by 22 members from 15 EU member states and co-chaired by two Europol units (EC3 and Innovation Lab) was established and it is the body responsible for identifying and prioritising end-user needs and which has veto right over the decisions done by EACTDA/Tools4LEAs with regard to the tool development roadmap.

In the second Tools4LEAs project (v2; Jul'23 to Jun'25), the number of tools delivered has been more than doubled. Also, the repository of tools implemented in v1, and currently used to host the results of the Tools4LEAs projects, has been enhanced and reused to host the results of EU-funded security research projects (when relevant in the field of cybercrime). EACTDA will play the role of custodian of these results, and the technical, IPR, and administrative aspects needed to create this new repository of security research results will be put in place. In addition, the v2 project included a pilot to proof the concept of initial and limited support&maintenance periods for a selection of tools. Besides, a pilot of the concept of EACTDA national nodes was included, with nodes planned in LT, FR, ES. Also, a platform for end-users to evaluate online tools has been implemented. Finally, the v2 project included activities to further build the community of Tools4LEAs stakeholders and to promote the creation and/or adoption of technical blueprints, and in general, of commonly accepted best practices.

Besides, a pilot of the concept of EACTDA National Nodes (NN) has been executed in the v2 project, with nodes in Lithuania, France, Spain. A platform for end-users to evaluate online tools has been implemented. And finally, the v2 project has included activities to further develop the community of Tools4LEAs stakeholders and to promote the creation and/or adoption of technical blueprints, and commonly accepted best practices.

1.2. Main objective of this document

EACTDA is a non-profit association which main goal is to deliver fully-tested and operational-ready software solutions to European public entities fighting cybercrime¹ with no license cost and with access to the source code.

EACTDA has received an operating grant from the European Commission (EC) to implement this Tools4LEAs project, which is the main instrument the association has to achieve its goals. Receiving an operating grant from the EC implies receiving a direct financial contribution, by way of donation, from the budget of the EC in order to finance the functioning of a body which pursues an aim of general EU interest or has an objective forming part of and supporting an EU policy.

With regard to supporting an EU policy, the Tools4LEAs project-v2 includes a task (2.3 - *Contributions to policy making, standardisation, and building knowledge*) which focuses on policy proposals and standardisation, and this document reports the results of the work done in this matter through the duration of the project.

It is important to note that this document is based on the equivalent one (deliverable D2.9) from the Tools4LEAs first iteration project (2021-2023), including several updates and changes based on the experience gained from that previous project and to adapt it to the scope and objectives of the Tools4LEAs-v2 project (2023-2025).

1.3. Relation to other deliverables

This deliverable is closely related to the following deliverables:

- **D2.5 Strategy, plan, and handbook for contributions to policy making, standardisation, and other knowledge building activities:** Deliverable D2.6 provides an update to the activities related to policy making, standardisation, and other knowledge building activities presented in deliverable D2.5.

1.4. Structure of the deliverable

Section 2 presents short descriptions of the activities conducted by EACTDA and the Tools4LEAs v2 project in relation to policy making.

Section 3 presents short descriptions of the activities conducted by EACTDA and the Tools4LEAs v2 project in relation to standardisation.

Section 4 presents short descriptions of the activities conducted by EACTDA and the Tools4LEAs v2 project in relation to other knowledge building activities.

¹ Find the European Commission's definition of cybercrime at: https://homeaffairs.ec.europa.eu/cybercrime_en

Finally, Section 5 summarises key aspects of this document, it acknowledges that there is still work to be done to improve the document, and it presents some of the areas of future work that have already been identified.

2. Summary of Policy Making activities

During the project two main activities related to policy making were carried out, one of which was completed whilst the other one is still in progress.

The first of these two activities was a joint position paper, elaborated in collaboration with ECTEG and the LAGO project, that focused on the access, handling and processing of data in the context of EU-funded security research, technology development, and innovation, where the lack of domain-specific data, in adequate quality and quantity, significantly hampers the implementation of specialised training supported by appropriate educational materials, as well as of the development, testing, and evaluation of new and innovative software tools

In response to a suggestion made by a policy maker from the European Commission, EACTDA contacted ECTEG and the LAGO project to propose them to jointly elaborate a position paper on the topic of data management in the context of EU-funded security research and innovation value chain. Both ECTEG and the LAGO project agreed on the importance of the topic, and the three entities jointly discussed the topic and prepared the position paper in the period that went from June 2024 to January 2025. The position paper is presented in ANNEX I.

The other main policy making activity conducted in the course of the Tools4LEAs v2 project has been to start preparing a document with some policy recommendations on the topic of aligning Law Enforcement AI with EU Requirements. Though the document is well advanced, it is still work in progress, it is still pending to include the changes derived from the review by the Secretariat for the Association, and it also has not been presented to the Board of the Association for its review and validation. Therefore, the draft presented in ANNEX II is still work in progress and should be considered as such. It is presented in this deliverable for the sake of completeness and transparency.

3. Summary of Standardisation activities

Beyond the efforts made by EACTDA to standardise its own processes when implementing the Tools4LEAs project (and all the „last-mile“ development projects within it), and beyond the efforts made to use widely adopted and commonly used international standards (e.g., ISO 25010 on Software Quality or ISTQB for testing), in the course of the Tools4LEAs v2 project, around the summer of 2023, EACTDA received the request to explore how it could support the work and efforts of the European Working Group on Standardisation for Internal Security.

After several webconferences and meetings to understand the need and explore collaboration opportunities, considering the limits of what EACTDA is allowed to do within the limits of the Grant of the Tools4LEAs v2 project, the initial efforts were made by EACTDA member ZITIS, without the need to receive funding from Tools4LEAs.

Next, when discussing the scope and the funding for the Tools4LEAs v3 project, the policy makers from DG HOME and the steering committee and the Secretariat of the European Working Group on Standardisation for Internal Security contacted EACTDA again to ensure that the v3 project was resourced to cover as many of the funding needs as possible. Therefore, a significant budget has been allocated as part of the v3 project proposal that was submitted in May 6th, 2025 to the EC. EACTDA has included in the previously mentioned proposal the internal resources necessary to manage the budget.

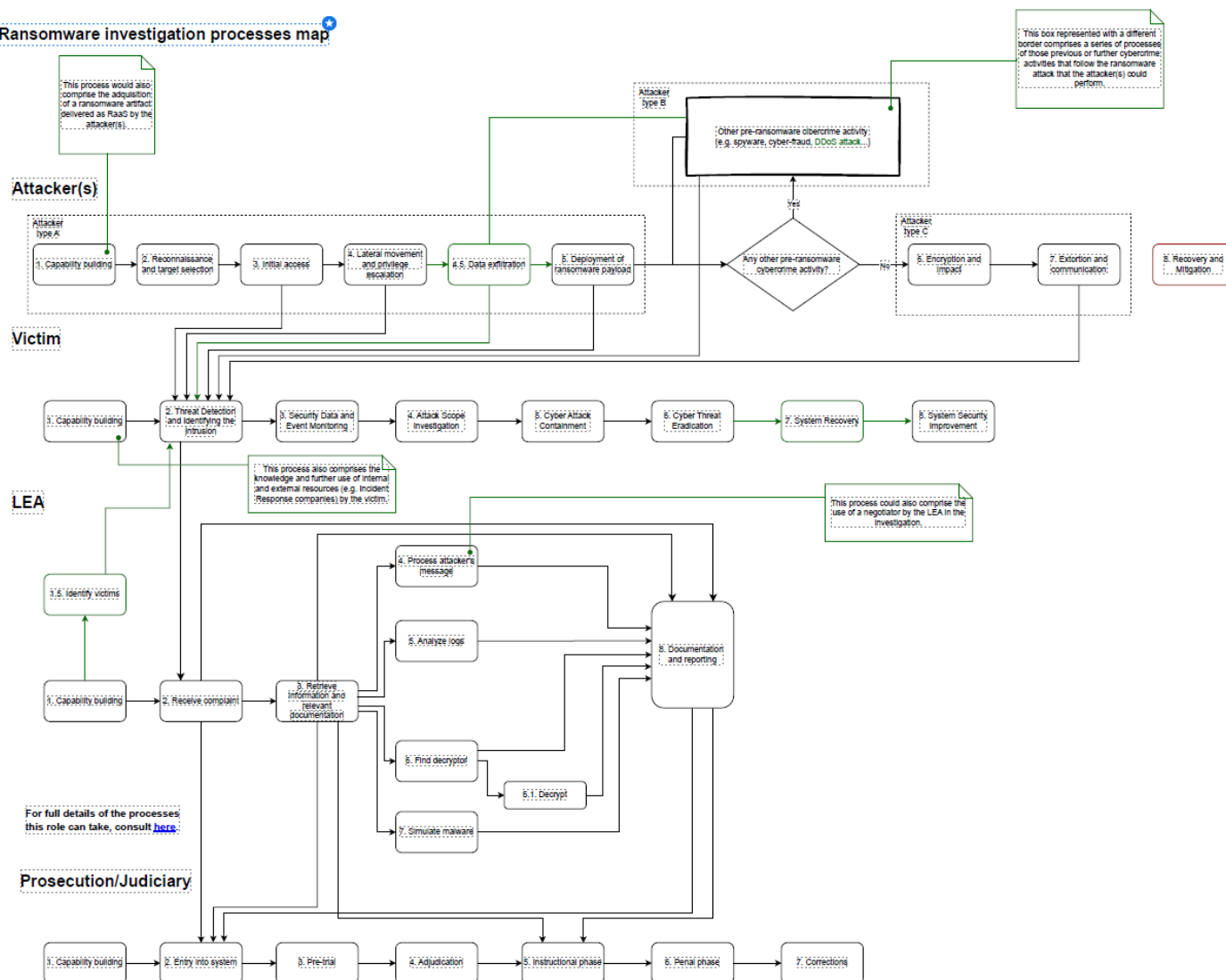
Also, a less important budget from the Tools4LEAs v2 project was re-allocated to provide support to the European Working Group on Standardisation for Internal Security so that a few experts could attend meetings and workshops related to some of the WGs of 3GPP².

² <https://www.3gpp.org/3gpp-groups>

4. Summary of other knowledge building activities

During the 2023-2024 academic year, EACTDA, in collaboration with the University of Deusto, and the Basque Police (Ertzaintza), created a model that represents the typical processes followed by attackers, victims, Law Enforcement Agencies, and the Judiciary in the context of ransomware. The figure below is the final result of this effort. This model was shared with the CYCLOPEs project's group of end-user experts working on the matter of ransomware for their review. The comments made by this group helped refining and improving the model.

Ransomware investigation processes map



5. Summary

5.1. Conclusion

In this document we have presented the different contributions made within the Tools4LEAs v2 project to policy making, standardisation, and other knowledge building activities.

5.2. Evaluation

The contributions made have had various different degrees of success and impact. On one hand, the contributions made to policy making in relation to data governance in collaboration with ECTEG and the LAGO project were considered insufficient by the key targeted stakeholders, and further details were requested, though EACTDA was not the main addressee of the comments and questions made.

On a more positive tone, EACTDA and the Tools4LEAs v2 project reacted swiftly and positively to the request made by the Standardisation WG, offering as much collaboration and resources as it was possible within the limits of the resources available and of the conditions of the Tools4LEAs v2 grant.

With regard to knowledge building, EACTDA participated in several activities that had a positive impact, being the improvement of its own DevSecOps practices and the modelling of the prototypical processes in relation to ransomware the most relevant ones.

5.3. Future work

During the Tools4LEAs v3 project, EACTDA will continue to contribute to these three topics to the best of its capacity and of its capabilities. It is worth noting that the v3 project includes a significant budget allocation to support the standardisation WG activities.

ANNEX I – Position paper on datasets management for the EU security research and innovation value chain

Below we copy & paste the position paper that was elaborated by ECTEG, the LAGO project, and EACTDA and submitted to policy makers from the European Commission:

Position paper on datasets management for the EU security research and innovation value chain

European Anti-Cybercrime Technology Development Association (EACTDA)³

European Cybercrime Training and Education Group (ECTEG)⁴

The “Lessen Data Access and Governance Obstacles (LAGO)” project⁵

INTENDED AUDIENCE

The primary target of this paper are staff and members of the European institutions, bodies and agencies, notably those involved in policy files related with data, research, innovation, and capability development, particularly in the domain of law enforcement and civil security.

In addition, the paper targets all other stakeholders that participate one way or another in the EU security research and innovation value chain including end-users, research and academia, industry, and relevant networks and associations of one or more of the aforementioned three groups of stakeholders.

ABSTRACT

This paper focuses on the access, handling and processing of data in the context of EU-funded security research, technology development, and innovation, where the lack of domain-specific data, in adequate quality and quantity, significantly hampers the implementation of specialised training supported by appropriate educational materials, as well as of the development, testing, and evaluation of new and innovative software tools.

³ <https://www.eactda.eu/>

⁴ <https://www.ecteg.eu/>

⁵ <https://lago-europe.eu/>

The challenge of defining, designing, creating, and maintaining high-quality, relevant, and regulatorily compliant datasets for the different needs at the different stages of the EU research and innovation value chain is enormous. None of the individual actors has the resources, the capacity, or the time to achieve this goal without end-to-end overexertion, which is often unaffordable.

Coordinated EU-funded action is therefore necessary to facilitate the creation of the necessary consensus among the key actors in the chain. Leveraging pre-existing results, relevant stakeholders may jointly define and adopt a series of standards, methodologies, techniques, tools, and governance mechanisms that foster collaboration and cocreation, and which can enable achieving the desired outcome.

POSITION

The lack of sufficient domain-specific high-quality data in general, but specifically in the EU security research, development, and innovation (R&D&I) ecosystem is a well-known issue [1][2][9]. With a sufficient consensus among the key stakeholders of the EU security research and innovation value chain, it is possible to significantly improve in a relatively short period of time the quantity and the quality (from both technical and regulatory compliance) of datasets available to conduct research and innovation activities throughout all the different stages of the value chain.

A standardized data governance framework can have a significant positive impact in the EU Security EU security R&D&I ecosystem.

The authors of this paper advocate for an EU-funded project to define, develop and pilot test the aforementioned standardized data governance framework, leveraging previous EU-funded research results (e.g., LAGO⁶, CEDAR⁷, DIVINE⁸, DATAMITE⁹) and reference international frameworks in the domain of data spaces building the necessary consensus among the community. Should the proposed EU-funded project be successful, follow-up projects should be funded and launched to support the full implementation and rollout of the framework.

KEY POINTS

The EU security R&D&I ecosystem lacks data. This issue has been acknowledged and discussed in the Community for European Research and Innovation Community (CERIS) as well as in other related for a and communities multiple times in the past few yearsⁱ [11].

⁶ <https://lago-europe.eu/>

⁷ <https://cedar-heu-project.eu/>

⁸ <https://divine-project.eu/>

⁹ <https://datamite-horizon.eu/>

Different issues have been noticed in this regard. In cases where exist, some data sets are not known or accessible to those who could benefit from them. In other cases, data simply does not exist in sufficient quantity, quality, complexity or fidelity. Efforts carried out by individual initiatives to satisfy their concrete data needs have proven to be far from cost-effective. Defining, designing, creating, and maintaining the high-quality and regulatorily compliant datasets requires excessive amount of resources which, in many cases, produce sub-optimal results.

Addressing the first situation requires increasing the visibility, accessibility and sustainability of research data to maximize its reuse, system efficiency and avoid cost overruns. Regarding the second one, shared visions and pooling of resources becomes the only viable option.

Therefore, co-creation, collaboration, and sharing datasets between key stakeholders of the community should be pursued. To facilitate this, it is necessary to define and adopt common standards, methodologies, techniques and tools, and governance mechanisms.

Public concerns are present regarding the potential risks involved with data sharing (e.g., data security, safe use, legal and ethical compliance, etc.). Therefore, trust between the different involved stakeholders is at the very core of R&D&I actions. To build the necessary trust, it is paramount to develop a comprehensive data governance framework that outlines policies, procedures, and responsibilities for managing R&D&I data.

Defining, designing, creating and maintaining high-quality domain specific datasets requires domain specific knowledge. Hence, it is important to strengthen existing domain-focused communities of multidisciplinary R&D&I practitioners (or creating new ones as necessary).

DISCUSSION

R&D&I security projects have various needs related to high-quality and regulatorily compliant datasets that often cannot be satisfied with the datasets available.

Complex, high fidelity (i.e. real or realistic), and up-to-date datasets are required to prepare the educational and training materials needed to build the competencies needed by practitioners for real operational cases. Datasets are also needed for development, testing, and evaluating the software tools that practitioners can use in real operational cases. Complex datasets normally include different data sources and require heterogeneous annotations which depend on the intended use.

There are similarities but also differences in the characteristics of the datasets required for each the different needs. Certain dataset usage needs might require large volumes of data. Others might not require as much data but they require the data to be real or very realistic. Or depending on the intended usage need, the dataset might have to be annotated or not.

In the cybercrime domain for example, when there is the need to have complex and realistic datasets, the diversity of devices combining static and dynamic traces and artefacts implies complexity in creating the traces so that at the time of analysis correlation between traces can be established. As the behaviour of human beings is part of the context of the investigated crimes, often considered by court decisions, the realism of the created data implies to act like real criminals or victims. As an example, the activity timeline often demonstrates the preparation stage of crimes or the way that an offender is targeting his/her victims. The evolution of the technology, as the creativity of the criminal side, requires a frequent update of the software tools and investigation strategies. Existing datasets and mocked cases provided from different sources like the NIST¹⁰, or provided as part of the course materials by the industry, mostly focus on one type of device and don't provide the complexity and realism that is needed.

It also happens that when there is a need for a specific dataset, and this dataset exists, the actor that has the need is not aware of its existence. This lack of visibility leads to a lack of uptake of research results and a significant duplication of efforts and inefficient use of resources. To avoid this situation and to maximize sharing and reuse of the results of EU-funded initiatives, it is paramount to ensure that actors of the EU security R&D&I ecosystem have access to a one-stop-shop solution where they can search and find pre-existing datasets of the characteristics they need.

When nothing can be found to meet the data needs of an actor of the ecosystem, creating and maintaining new datasets can be a herculean effort. Even so, many organizations decide to invest in doing so, aware that the results will be valid for a single use. The reason is that R&D&I actions in EU funded programmes are implemented in most cases by a consortium of organisations collaborating in a project. Such projects are, by nature, temporary and complex. They require the collaboration of multiple heterogeneous organisations distributed normally in a minimum of three different countries. Besides, each of those research projects has a different focus, as it addresses a specific topic, and it has specific scope and goals. Hence, the dataset needs within and between R&D&I projects are often various and heterogeneous.

However, despite the diversity of projects' aims and needs, some convergence can be identified. For instance, various projects related to the same domain can agree to define, use, and maintain complex, up-to-date and realistic use-cases. When jointly designing the use case, they can agree for example about including specific devices and traces, and they can share (at least partially) the efforts to ensure legal and ethical compliance. Next,

¹⁰ NIST repository <https://www.nist.gov/el/ammt-temps/datasets>

the jointly defined use-case can be used to create the different datasets needed (i.e., education and training or software tool development, testing, and evaluation).

Such a collaborative approach avoids duplication of efforts and, in a cost-efficient manner, maximizes the synergies. This approach also allows identifying when different actors have the same dataset needs, so that they can then agree to co-create and maintain such datasets. Besides, this approach allows each of the actors investing its limited resources in what is core to its needs, whilst benefiting from the work done by other actors thanks to the complementarity and interoperability of the results produced by all the collaborating parties.

The need for efficient collaboration and joint efforts to share and manage data between key stakeholders of the EU security R&D&I ecosystem has previously been identified by relevant stakeholders [1][2]. In this regard, standards play a pivotal role in facilitating technical collaboration. The benefits and the need for making systems interoperable have been identified as a priority by the EU [4][5][10]. Standards contribute to the creation of a common framework and language for all parties involved. Standardized methodologies and techniques help maintain a high level of quality across different teams and projects. They also facilitate interoperability, efficiency, consistency, and compliance with quality and legal requirements [3]. Interoperability enables organisations to connect, exchange information, and share knowledge effortlessly across all levels. This concept extends beyond just technical aspects; it requires multiple elements, including mutual agreements between various organisations, standardised data descriptions, supportive legislation for data exchange, and a cooperative culture, just to name a few.

But collaboration and sharing datasets will not happen without previously building the necessary trust between the stakeholders. It is paramount to develop a comprehensive data governance framework that is trusted by all parties and which outlines policies, procedures, and responsibilities for managing R&D&I data.

The concept of trust is a cornerstone for enabling secure, effective, and scalable dataset sharing. Trust is a multifaceted notion that encompasses the confidence entities have in each other's intentions, behaviours, and technological infrastructures. It is also vital for ensuring collaboration, protecting sensitive information, and fostering innovation. Especially in the security research domain, without trust, entities might be reluctant to expose or consume data. This is due to concerns about: (i) quality of data, which should be accurate, complete and uncorrupted, (ii) technical security, that is related to data storage, maintenance, access controls, etc., (iii) privacy, especially for sensitive data, where unauthorized disclosure must be prevented, (iv) legal and ethical aspects, such as compliance with regulatory frameworks, like GDPR, and respect of human rights, (v) misuse, to ensure data is used appropriately for security R&D&I purposes, and (vi) potential risks, which are the risks of sharing specific data, potential impacts and mitigation measures.

To this end, establishing well-defined governance mechanisms serves as a foundation for building trust among stakeholders and ensuring that all parties follow established rules. Such governance framework must define policies and rules for accessing and using the datasets. It must define the roles and responsibilities, and it must include decision making and conflict resolution procedures. It also must facilitate compliance with law, accountability, and risk management. Besides, it must allow continuous monitoring and improvement of collaboration among all the different parties [6][7].

In addition, as indicated by the European Data Strategy, the governance framework must ensure data sovereignty, decentralisation, transparency and accountability of the data sharing activities, interoperability, adoption of standards, compliance with legal frameworks (both at EU and national level), respect of ethical and privacy aspects, and proper training [8].

A comprehensive data governance framework defines policies and responsibilities not only at cross-organisational level (how data is shared between organisations), but also at intra-organisational level (how data is managed within an organisation). At cross-organisational level, governance must foresee roles, responsibilities and procedures that organisations have to follow when sharing data, like how access to dataset is granted, anonymisation of data before sharing (in case of sensitive data), establishment of contracts or non-disclosure agreements in case of data with delicate nature, etc. Trust can be even reinforced by adopting proper accreditation procedure, where any organisation that would like to take part to data sharing activities must be validated first by a trusted authority. The validation of the trusted authority is the guarantee for the other participants to the data sharing that an organisation is considered trusted.

At intra-organisational level, governance should provide rules to appoint roles and responsibilities within any organisation to guarantee the proper management of data, like who creates, collects, processes, owns, or administrates datasets, who is in charge of legal aspects in case of data sharing, etc. Every organisation should conduct periodic training courses for its personnel, which can be further specialised with ad-hoc training on aspects related to compliance with national rules, procedures internal to the organisation, etc.

In any collaborative environment the presence of governing bodies is paramount to oversee and periodically review the data sharing processes and governance mechanisms, resolve disputes between parties, provide support, and promote adoption, in this case, among security R&D&I stakeholders.

It should also be stressed that, in many cases, the dataset needs are closely related to the intended use of the dataset, and so they are context and domain specific.

For example, when an entity needs a dataset to develop, test and/or evaluate AI-enabled tools that detects phishing emails to protect users from cyber-attacks, the dataset should

include a large collection of emails labelled as either phishing or legitimate. The emails included in the dataset should include metadata (sender, subject, timestamp), real or realistic content to allow its analysis (keywords, links), and attachment details. The dataset should be diverse to cover various phishing tactics and updated regularly to adapt to new threats.

Creating and maintaining up to date this type of domain specific datasets requires a subject-matter knowledge that is normally available only to domain specialists. Therefore, domain specific communities of multidisciplinary R&D&I practitioners (i.e., end-users, researchers, technology providers, legal and ethical experts) that last over time are the best positioned to identify the needs, prioritise them, agree on common methodologies, standards, and best practices, and to foster collaboration, co-creation, dissemination, and sharing of datasets.

ALTERNATIVE VIEWPOINTS AND REBUTTAL

Some actors of the EU Security R&D&I ecosystem might argue that establishing a shared and commonly used data governance framework, based on standards and strict business rules might reduce the level of flexibility and agility that they need to address their specific needs and priorities. They might argue that a common framework could slow down their progress or force them to lower their standards to align with less advanced systems.

Standards can be designed to be adaptive by including provisions for updates and modifications as new technologies and threats emerge. They can also be designed to be modular, so only the parts that require changes are updated without affecting the others. Such design can ensure that the framework remains relevant and can evolve with the needs of the ecosystem. Besides, standards facilitate interoperability and integration, which can enhance agility in a collaborative environment such as that of the EU Security R&D&I. Challenges can be addressed through collaboration of such stakeholders, which can increasingly work on creating unified standards, making it easier to adopt shared governance models. International standardization initiatives (W3C, OASIS, ISO, etc.) can be valid starting points to reach interoperability and integration not only within the envisioned data governance framework, but also with other initiatives already in place at EU and national levels.

On the other hand, smaller or less prepared actors might argue that developing and implementing a common data governance framework across the EU could be extremely costly and complex. They might say that the resources required for harmonization, training, adoption of required technology, data maintenance, regular audits, and compliance might outweigh the potential benefits.

A standardized framework can foster innovation by providing a clear structure within which organisations, especially smaller and more innovative ones, can conceive and develop new solutions. This can enhance the competitiveness of the EU's security R&D sector on

a global scale. Besides, best practices, bodies of knowledge, and reference architectures can be created to ease the adoption of the standardized framework. Relying on open-source technologies for data processing, storage and sharing can also lower the organizational costs related to the adoption of the framework. Moreover, while initial costs can be significant, the establishment of a standardized framework can provide long-term savings, by reducing risks associated with poor data management, data breaches and inefficiencies. Indeed, proactive investments in governance can cost less than reactive countermeasures to potential damages or mismanagement.

Privileged actors, or actors with sufficient resources, might argue that developing and implementing a common data governance framework across the EU could lower the entry level to their competitors, putting at risk the competitive advantage they already have.

However, a standardized framework can expand the market, bringing new potential customers, creating new opportunities for collaboration, partnerships, and business growth that might not be possible in a smaller and more fragmented system. Privileged actors can also benefit by leading the way in adopting and promoting a standardized framework. This can enhance their reputation, positioning them as industry leaders committed to high standards and best practices, which can be a significant competitive advantage.

WAY AHEAD

In summary, the evidence presented clearly supports the argument that a standardized data governance framework, when combined with domain specific communities, can have a significant positive impact in the EU Security R&D ecosystem. Therefore, we consider that an EU-funded project should be launched to conduct the following actions:

- 1) **Secure the buy-in of the key stakeholders** of the ecosystem by identifying key stakeholders, within the EU and its agencies, in the end-user community, research institutions, private sector partners, and international bodies.
- 2) **Define and establish the governance framework**, supported by all the key stakeholders, establishing clear rules and decision-making processes, to enhance trust, transparency, alignment of interests, and accountability.
- 3) **Identify gaps and areas of improvement** after having conducted research on existing data governance frameworks and best practices. Benchmark current data governance practices, challenges, and needs across the ecosystem against leading international standards and/or best practices.
- 4) **Define the objectives and determine the scope** of the standardized data governance framework, including which data types, processes, and systems will be covered.
- 5) **Establish a 2-level structure of multidisciplinary working groups**, one 1st level working group providing the overall architecture, which should be modular, adaptable, and scalable. This 1st level working group should also be responsible for the harmonization and normalization of the contributions from the 2nd level working groups, which should focus on each of the components identified in the framework's architecture (e.g., data standards, governance policies, and compliance requirement).
- 6) **Improve the draft framework with stakeholder review and feedback**, whilst reinforcing the buy-in of the key stakeholders.
- 7) **Pilot test the data governance framework** in a few specific domains to refine the framework with the data collected on performance, challenges, and outcomes.
- 8) **Define a full implementation and rollout plan**, including timelines, milestones, and resource allocation.

Should the proposed EU-funded project be successful, follow-up projects should be funded and launched to support the full implementation and rollout plan.

REFERENCES:

- [1] "Study to support the technical, legal and financial conceptualisation of a European Security Data Space for Innovation"; by EY and RAND; Feb'23 - https://home-affairs.ec.europa.eu/system/files/2023-02/Data%20spaces%20study_0.pdf
- [2] "Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement", by HLG experts; May'24 - https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en?filename=Recommendations%20of%20the%20HLG%20on%20Access%20to%20Data%20for%20Effective%20Law%20Enforcement_en.pdf
- [3] "ISO Quality management principles: The foundation for success" - <https://www.iso.org/quality-management/principles>
- [4] "Interoperable Europe Act" - https://commission.europa.eu/publications/interoperable-europe-act-proposal_en
- [5] "European Interoperability Framework evaluation & strategy – summary of the impact assessment report" - https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12579-Interoperable-digital-public-services-European-Interoperability-Framework-evaluation-strategy_en
- [6] "EU Data Governance Act" - <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>
- [7] "Understanding the Data Governance Framework: Templates, Examples, and Best Practices" - <https://www.datagovernanceday.info/templates-examples-and-best-practices/>
- [8] "European data strategy" - https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en
- [9] "European Data Act" - <https://digital-strategy.ec.europa.eu/en/policies/data-act>
- [10] "Concluding report of the High-Level Group on access to data for effective law enforcement" - https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en
- [11] "Building resilience in the civil security domain based on research and technology; Report of the CERIS Expert Group, November 2024" - <https://op.europa.eu/en/publication-detail/-/publication/1796b0bd-ad38-11ef-acb1-01aa75ed71a1/>

ANNEX II – Law Enforcement AI with EU Requirements

Below we present the draft version of the document that is being prepared with policy recommendations on the topic of Law Enforcement AI with EU Requirements.

IMPORTANT NOTE: The document below is a draft that has not been finalised and which has not been yet reviewed and validated by EACTDA Secretariat nor by the Board of the Association.

1. Executive Summary

Law enforcement agencies (LEAs) across Europe face a critical tension: the EU AI Act's strict, still-unfolding regulatory requirements for "high-risk" AI systems promise robust protection of fundamental rights but also introduce legal complexity and uncertainty that can stall innovation. At the same time, criminals are rapidly adopting AI technologies, and LEAs must embrace AI-based tools at pace, accepting reasonable, controlled risks through adaptive experimentation to stay ahead.

European law enforcement agencies are increasingly adopting artificial intelligence (AI) tools to enhance security and investigations. However, the forthcoming EU Artificial Intelligence Act (AI Act) imposes strict requirements to ensure such high-risk AI systems are ethical, lawful, and aligned with fundamental rights.

This policy brief examines how current initiatives are embedding ethical and legal safeguards early in innovation development for law enforcement, and what lessons they offer for EU policy. It analyzes four key initiatives – the Tools4LEAs ELSA Working Group, the Europol Innovation Lab, the STARLIGHT "AI Playbook", and Lithuania's regulatory AI sandbox. Based on these insights, the brief recommends leveraging and expanding existing platforms (like EACTDA's Tools4LEAs) rather than creating new institutions, to build a cohesive European ecosystem for responsible law enforcement AI innovation.

Key Findings and Recommendations:

- Early "Ethics by Design" – Projects like Tools4LEAs demonstrate the value of integrating Ethical, Legal, and Social Aspects (ELSA) governance from the start of AI development.
- Structured Ethical Assessment – The Europol Innovation Lab introduced a 7-step ethical assessment framework to guide law enforcement in evaluating new technologies responsibly is a relevant practical example of legal compliance checks under the AI Act.
- Comprehensive "AI Playbook" for LEAs – The STARLIGHT project (H2020) is developing a detailed governance and compliance "PlayBook" to help law enforcement innovate with AI responsibly. Its approach includes a co-development methodology with security and privacy-by-design, ensuring tools are operationally relevant and secure.
- Regulatory Sandboxing – Lithuania's AI sandbox pilot illustrates national effort to accelerate AI Act preparedness. The sandbox will provide a controlled environment for companies to test AI systems with regulatory guidance before full market release. This may offer compliance support to give businesses a head start in meeting AI Act standards while speeding time-to-market.

Policy Recommendation in Brief:

Separate LEAs are often ill positioned to embrace high speed of innovation and integrate these innovations in their processes. AI technologies and requirements of AI Act adds another level of complexity. Thus, support structures to facilitate AI based innovation development and application are clearly needed.

Rather than establish new structures, the European Commission should build on these existing initiatives to create an ecosystem of support for law enforcement AI compliance. In particular, the mandate of the European Anti-Cybercrime Technology Development Association (EACTDA) and its Tools4LEAs platform may be expanded as a central hub to: (1) integrate practical compliance tools (e.g. the AP4AI self-assessment tool for AI Act conformity, shared ELSA guidelines, DPIA templates), (2) coordinate with national AI sandboxes to pilot and validate law enforcement AI solutions under real conditions, and (3) provide shared governance resources such as a repository of best practices, model policies, and maybe even a standing ethics advisory network for security AI. By leveraging Tools4LEAs and related networks (Europol Innovation Lab, AP4AI, etc.), the EU can achieve synergy and consistency in how law enforcement agencies innovate responsibly – ensuring compliance, reducing duplication, and fostering trust in AI-enabled policing across Member States.

2. Introduction

The advent of advanced AI technologies has created both opportunity and urgency for Europe's law enforcement agencies (LEAs). AI-powered tools – from video analytics that monitor public spaces to natural language chatbots that assist in criminal investigations – promise to boost efficiency and outcomes in policing and security. At the same time, these tools pose significant ethical, legal, and societal questions. Improperly designed or deployed AI systems can infringe on fundamental rights (such as privacy or non-discrimination), undermine public trust in law enforcement, or even misfire and compromise investigations.

Recognizing these risks, EU policymakers have moved to establish clear rules on “trustworthy AI.” The EU Artificial Intelligence Act, adopted in 2024, is the world's first comprehensive AI law, applying a risk-based framework to AI systems. It classifies most law enforcement AI applications (e.g. crime analytics, biometric identification, predictive policing tools) as high-risk, subjecting them to strict requirements: conformity assessments, transparency measures, human oversight, data governance, accuracy and robustness standards, and ongoing monitoring once in use.

For European law enforcement, the AI Act creates a pressing compliance challenge – how to harness AI innovations to fight crime while fully adhering to new European norms and safeguards, while increasing the speed of development and adoption of innovations. This challenge is compounded by the pace of technological evolution and the cross-border nature of both AI solutions and security threats. European Commission policy officers and national authorities must ensure that the AI Act's principles are translated into practical guidance, tools, and support mechanisms that enable LEAs to meet their obligations without stifling innovation.

This policy brief reviews four initiatives dedicated to facilitating development and uptake of innovation in depth – Tools4LEAs, Europol's Innovation Lab, STARLIGHT, and Lithuania's AI sandbox – drawing out insights on what works and where gaps remain. By understanding these efforts, policymakers can craft

strategies that scale up best practices and foster synergies, ensuring that compliance with the AI Act is not an afterthought but rather baked into the DNA of AI innovation for law enforcement.

3. Challenges in Aligning Law Enforcement AI with EU Requirements

Before turning to the current initiatives, it is important to outline the core challenges that any policy measures or support frameworks must address:

- **Complex Regulatory Obligations:** The AI Act introduces detailed obligations for high-risk AI systems. Law enforcement agencies (or their technology providers) will need to conduct risk assessments, maintain technical documentation, ensure data quality, implement human oversight, and undergo conformity assessments for tools like forensic AI software or predictive analytics. Navigating these legal requirements is complex, especially for public security organizations that may lack in-house regulatory expertise. A key challenge is operationalizing these requirements in day-to-day development and procurement processes.
- **Ethical and Societal Concerns:** Beyond formal compliance, law enforcement AI faces heightened ethical scrutiny. Uses of AI in policing can be controversial (e.g. facial recognition technology) and risk public backlash or loss of trust if not handled with transparency and respect for rights. Challenges include mitigating bias in algorithms, ensuring accountability for automated decisions, and balancing security benefits against privacy invasion. Traditional oversight mechanisms (like judicial warrants or data protection impact assessments) may not fully address the unique ethical dilemmas posed by AI's complexity and opacity.
- **Rapid Technological Change:** The innovation cycle for AI is fast-moving – new techniques (such as deep-learning models, generative AI, etc.) emerge rapidly and can outstrip existing policy guidance. Law enforcement agencies may adopt experimental tools (for example, an AI system to flag online hate speech, or to predict crime hotspots) in pilot programs or operations. Ensuring governance keeps pace with technology is a constant challenge; frameworks must be flexible and updatable (“living” guidance) to remain relevant as new AI applications arise.
- **Interagency and Cross-Border Coordination:** Security AI often involves collaboration – between different LEAs, between LEAs and private tech developers, and among EU Member States sharing tools or data. A fragmented approach where each agency or country invents its own compliance and ethics process could lead to duplication, inconsistency, and loopholes. The challenge is to achieve consistency and knowledge-sharing across jurisdictions while respecting national autonomy. This is especially pertinent as the AI Act mandates each Member State to establish a national AI sandbox and enforcement structure; without coordination, there's risk of siloed efforts.
- **Resource and Expertise Gaps:** Finally, many law enforcement organizations face constraints in expertise and resources for AI. Smaller police forces or agencies in less funded regions might struggle to employ AI ethicists, data scientists, or lawyers specializing in AI law. Even larger agencies like Europol or national crime units must devote significant resources to build internal frameworks. Thus, a critical challenge is providing common resources, templates, and support that lower the barrier to compliance and trustworthy AI for all, not just well-resourced actors.

Against this backdrop, the following initiatives have emerged as trailblazers, piloting solutions to bridge the gap between AI innovation and governance in the law enforcement context. Each provides valuable insights into addressing the above challenges.

4. Insights from Current Initiatives

4.1. Tools4LEAs ELSA Working Group: “Ethics & Legal by Design” for Law Enforcement AI

One noteworthy effort is the Tools4LEAs project, coordinated by the European Anti-Cybercrime Technology Development Association (EACTDA). Tools4LEAs is an EU-funded initiative that seeks to deliver practical digital investigation tools to law enforcement, free of license costs, by taking promising prototypes and bringing them to operational readiness. What sets Tools4LEAs apart is its strong emphasis on Ethical, Legal, and Social Aspects (ELSA) from the very start of the innovation process. The project established an ELSA Management framework – essentially a working group and process dedicated to embedding ethical and legal safeguards into each tool’s development lifecycle.

Under this framework, two bodies are responsible for oversight: an ELSA Management Team (within EACTDA) and an independent ELSA Committee. The ELSA Management Team works directly with each tool developer early on – as soon as a new law enforcement tech solution is being scoped for development. Key responsibilities of this team include: ensuring a Data Management Plan (DMP) is created to govern data use, reviewing that DMP for adequacy; requiring developers to fill out Data Protection Impact Assessments (DPIAs) and ethical impact questionnaires; analyzing those submissions for potential issues; and conducting deeper Ethical and Social Impact Assessments as needed. In practice, a tool’s developer must cooperate closely with the ELSA team from the design phase onward, providing information and addressing concerns.

The impact of this “ELSA by design” approach is twofold. First, it ensures that compliance is proactive. By frontloading privacy, human-rights and social impact considerations, Tools4LEAs can catch and correct problems (for example, if a tool’s use of personal data might violate GDPR, or if an AI model risks a discriminatory outcome) before the tool is deployed operationally. The ELSA Working Group effectively acts as an internal compliance and ethics auditor during development, giving developers guidance on how to adjust their designs. As noted in the project’s ELSA Management Handbook, the goal is to have reference guidelines so that the project “is implemented in compliance with all ethical, privacy, and data protection principles and regulations”. This means a law enforcement tool coming out of Tools4LEAs is already built with the EU’s legal standards in mind – aligning with the spirit of the AI Act which requires rigorous ex ante risk management for high-risk AI systems.

Second, the Tools4LEAs ELSA model provides a scalable template that could be adopted beyond this single project. Many of the processes it uses mirror what the AI Act will demand across Europe: for instance, conducting DPIAs (which parallels the Act’s requirement for risk assessment and data protection impact in certain cases) and engaging external review (which parallels the notion of notified bodies or expert assessment for compliance). By adapting the Tools4LEAs ELSA procedures, national police forces or other EU projects can create their own “ELSA working groups” to guide AI development. Importantly, this approach integrates with existing law enforcement workflows. It acknowledges that while EACTDA can ensure a tool is designed to be ELSA-compliant, the ultimate responsibility for ethical use lies with the agencies deploying the tool – hence, law enforcement end-users are also involved (via an end-user advisory board) to ensure practicality and correct use. In summary, Tools4LEAs demonstrates successful embedding of ethics/legal compliance effort in the innovation development process.

4.2. Europol Innovation Lab: A 7-Step Ethical Assessment & Real-World Use Cases

At the European level, Europol's Innovation Lab has become a focal point for examining the intersection of emerging tech and ethics in law enforcement. In early 2025, Europol – together with its advisory European Clearing Board (EuCB) and a Strategic Group on Technology and Ethics – published a landmark report, “Assessing Technologies in Law Enforcement: A Method for Ethical Decision-Making.” This report introduces a 7-step ethical assessment framework designed specifically to help law enforcement agencies make “ethically robust decisions” about using new technology. Recognizing that police must balance security objectives with fundamental rights, the framework provides a structured, step-by-step process that any agency can follow when evaluating an AI tool or other advanced technology.

This methodology is deeply grounded in European values. Europol emphasized that it aims to keep technology adoption aligned with core principles like transparency, fairness, privacy, and accountability. By following the steps, law enforcement leadership can demonstrate that they have carefully weighed societal values alongside operational needs. Another benefit is that it creates a common language for ethical deliberation – moving debates away from gut feelings to a more structured analysis, which can help when communicating decisions to external stakeholders or the public.

Crucially, the Europol Innovation Lab didn't stop at theory. The report is envisioned as a “living document” that will be regularly updated with new use cases and lessons as technology evolves. In its initial edition, it applied the 7-step framework to several concrete law enforcement technology use cases as illustrations. These included: AI-driven video analytics for monitoring CCTV footage; AI for risk assessment in criminal justice (e.g. assessing likelihood of reoffending, such as in gender-based violence cases); open-source intelligence (OSINT) data scraping tools; chatbots to prevent online child sexual abuse (for instance, conversational AI agents that might interact in forums to detect grooming activity); and automated analysis of large datasets for investigative leads. The chatbot case highlights questions of dignity and potential entrapment when an AI interacts with potential offenders, as well as the need to safeguard the rights of children the system aims to protect.

The Europol Lab's effort thus serves as both guidance and a confidence-building measure. It shows that law enforcement agencies can self-regulate responsibly by adhering to a transparent process. From a policy perspective, this seven-step framework could be promoted as a de facto standard for ethical evaluation across EU security agencies. For instance, national police AI units might be encouraged to adopt the method when introducing any high-risk AI system, in parallel with performing legal compliance checks. Indeed, the AI Act's requirements on risk management and stakeholder engagement could be complemented by this qualitative ethical reflection. Moreover, the framework's existence under Europol provides a form of soft governance – since Europol is an EU agency, its guidelines, while non-binding, carry influence. Looking ahead, continuous updates to the use case library (the report will expand over time) will keep law enforcement ethics dialog current, addressing new tech like face recognition in public spaces or advanced predictive AI as they emerge. The Commission can support this by funding training programs through CEPOL or others to disseminate the 7-step method, and by integrating it into the forthcoming AI sandboxes as one of the evaluation tools. In summary, the Europol Innovation Lab has delivered a much-needed practical ethics tool for policing, which dovetails with legal compliance and should be widely leveraged.

4.3. *STARLIGHT “AI PlayBook”: Governance, Compliance Alignment, and IP Management for Security AI*

Another major initiative providing insight is the STARLIGHT project (EU Horizon 2020, 2021–2025), which focuses on strengthening AI capabilities for European law enforcement. STARLIGHT brings together 50 partners (including 15 LEAs across 18 countries) to develop a suite of AI tools for tackling priority crime threats, while also building an ecosystem for “responsible AI” in policing. As part of its mandate, STARLIGHT has developed what can be described as a comprehensive AI governance “PlayBook” – essentially a set of frameworks, procedures, and resources to ensure that AI solutions are not only technically effective but also legally and ethically compliant, operationally viable, and sustainable in the long term.

Key elements of the STARLIGHT PlayBook include:

- **Adaptive Co-Development with LEAs:** STARLIGHT adopted an LEA-centric co-development approach. This means that rather than researchers building AI in isolation, law enforcement end-users are involved at every stage: gathering their needs, iteratively testing prototypes, and refining tools based on feedback. Privacy and security features are integrated from the ground up (for example, tools are designed with data encryption, access controls, audit logs, etc., in line with “security-by-design”).
- **Accountability and AI Act Alignment (AP4AI):** STARLIGHT’s governance efforts is aimed for integration of the Accountability Principles for AI (AP4AI) framework. Concretely, AP4AI produced a set of 12 principles defining what accountable AI use entails, and built a web-based tool called “CC4AI” (Conformity Check for AI) that allows agencies to self-assess their AI systems against the AI Act’s requirements. Each AI prototype in STARLIGHT is evaluated via the AP4AI criteria to see if it meets expected standards in areas like transparency, explainability, data governance, bias mitigation, etc., which map to AI Act obligations.
- **Operational Readiness and Training:** A common pitfall in research projects is delivering tools that are not practically adopted. STARLIGHT tackled this by conducting multiple field pilots (three rounds of pilot demonstrations) and training workshops with officers to ensure tools are user-friendly and fit for purpose.
- **IPR and Sustainability Strategy:** STARLIGHT recognized that for its AI innovations to have lasting impact, issues of Intellectual Property Rights (IPR) and sustainability must be addressed.

In sum, the STARLIGHT PlayBook can be seen as a holistic governance and compliance framework for law enforcement AI. It aligns closely with the AI Act (through AP4AI’s concrete tools), ensures operational viability (through co-development and training), and handles practical issues like cross-border data sharing and IP.

4.4. *Lithuania’s Regulatory AI Sandbox: Pioneering a National Approach*

As EU Member States gear up to implement the AI Act, Lithuania has emerged as an early mover by establishing a regulatory AI “sandbox” – one of the first such national initiatives in the EU. Launched in late 2024, Lithuania’s sandbox is a pilot environment where AI developers (especially start-ups and SMEs) can work alongside regulators to test and validate AI systems in a controlled setting before full deployment. The overarching aim is to accelerate AI innovation in the country’s economy while ensuring new solutions are safe, trustworthy, and compliant with upcoming regulations.

Strengths of the Lithuanian model: This sandbox offers several notable strengths that align with EU policy goals:

- **Proactive Compliance Support:** By design, the sandbox gives participants a chance to engage with regulatory requirements early on. A company developing, say, an AI system for medical diagnostics or smart city surveillance can enter the sandbox and receive guidance on how the AI Act would classify their system, what documentation and risk mitigation they need, and even simulate parts of the conformity assessment. This reduces uncertainty and fosters a compliance-by-design mindset among innovators.
- **Holistic Innovation Infrastructure:** Lithuania has set up an institutional structure to run the sandbox that leverages both innovation and regulatory bodies. The government designated Innovation Agency Lithuania (a public body fostering innovation ecosystem) as the national notifying authority for the AI Act, and the Communications Regulatory Authority (CRA) as the market surveillance authority and single point of contact for AI regulation. Together, these bodies manage the sandbox. In effect, Lithuania is aligning its entire innovation ecosystem with the AI Act's implementation – from development support to conformity assessment and market surveillance – creating a feedback loop that could rapidly iterate and improve compliance processes.
- **Integration with EU Digital and HPC Resources:** in its sandbox effort Lithuania plans to link the sandbox to high-performance computing (HPC) infrastructure. The sandbox participants will have access to large-scale computing power (for training AI models, etc.) and datasets through the European HPC network. This is an example of how expensive technological challenges, which may be forbidding for innovators, can be addressed.

In conclusion, Lithuania's regulatory AI sandbox exemplifies a forward-leaning national strategy to implement the AI Act in a way that boosts innovation while safeguarding values. This example is an inspirational effort that needs to be studied. But we have to note its limitation for our cause – while LEAs face specific regulatory and ethical requirements, the discussed sandbox is dedicated to general AI use, so will not help to address specific LEAs challenges.

5. Policy Recommendations

Drawing on the above analysis of current initiatives, this brief recommends a set of actions for EU policymakers and stakeholders to strengthen synergies and prepare a supportive ecosystem for AI Act compliance in law enforcement and security applications. The emphasis is on leveraging existing structures and successes – scaling up what works – rather than creating new bureaucracies. Each recommendation is aimed at ensuring that the investment in ethical, legal, and societal safeguards becomes an integral part of AI innovation in law enforcement across Europe.

5.1. *Expand and Empower the Tools4LEAs/EACTDA Platform as a European Hub for AI Compliance in Law Enforcement*

The European Anti-Cybercrime Technology Development Association (EACTDA), through projects like Tools4LEAs, has proven to be an effective vehicle for delivering ready-to-use, compliant tech solutions to security practitioners. The Commission may consider an expanded role for EACTDA's Tools4LEAs platform as a central hub to coordinate AI Act implementation efforts in the law enforcement domain. In practice, this means providing funding and policy recognition for Tools4LEAs (and its successors) to:

- **Host Practical Compliance Tools and Guidelines:** EACTDA's platform could serve as a one-stop-shop where law enforcement agencies and their tech partners can access resources to help

comply with the AI Act. This includes integrating tools like the AP4AI “CC4AI” self-assessment web tool (developed in STARLIGHT/AP4AI) directly into the platform, so any LEA or vendor can evaluate an AI system’s readiness against AI Act criteria. It also means publishing templates for Data Management Plans, DPIAs, risk assessment checklists, and model policies (for example, template standard operating procedures for human oversight of an AI tool) drawn from the experience of Tools4LEAs, Europol’s framework, and STARLIGHT’s PlayBook. By centralizing these, every police agency – big or small – can readily adopt state-of-the-art compliance practices without starting from scratch.

- **Facilitate Sandbox Collaboration for Security Use-Cases:** The platform should link with the emerging national AI sandboxes (like Lithuania’s) to specifically support law enforcement AI trials. National sandboxes will focus on private sector innovation; security agencies do have unique needs (e.g. testing an AI system on criminal intelligence data, which involves sensitivity and secrecy). EACTDA could act as a coordinator, identifying law enforcement AI projects that would benefit from sandboxing and helping arrange cross-border sandbox exercises. For instance, if a new AI tool for counter-terrorism analytics is being developed in one country, EACTDA could help it get tested in another country’s sandbox with the involvement of local authorities, ensuring mutual learning and validation across jurisdictions. This could evolve into a European network, with EACTDA ensuring that lessons learned (both on compliance and on performance) are shared widely with all Member States.
- **Provide Shared ELSA Governance Resources:** Not every police agency or EU project will have an ethics committee at its disposal. EACTDA could maintain a standing ELSA Committee or expert pool that can be tapped into by any law enforcement AI initiative to get independent review and advice. This mirrors what Tools4LEAs did internally, but scaled up: a roster of legal, ethical, and societal experts (perhaps drawn from academia, civil society, and law enforcement oversight bodies) can be made available to evaluate new AI proposals or deployments on request. For example, if a national police force is unsure about the ethical implications of an AI-driven profiling tool, they could consult this EACTDA-facilitated panel for guidance. Additionally, EACTDA can continue to produce and update handbooks on areas like software quality, IPR management, and social impact – essentially acting as the knowledge center for governance of AI for internal security.

By strengthening EACTDA and Tools4LEAs in these ways, the EU would utilize an existing institution with credibility among LEAs, avoiding the delay of setting up something entirely new. It also cements a public-interest approach in a domain often dominated by commercial vendors – ensuring tools are available without license costs (as Tools4LEAs mandates) and with compliance built-in, which is particularly beneficial for smaller Member States or agencies with limited budgets.

5.2. *Foster Integration of Europol’s Ethical Framework into National Practices*

The Europol 7-step ethical assessment method should not remain confined to a Europol report – it is a valuable tool that ought to diffuse into everyday law enforcement decision-making. The Commission, in collaboration with Europol and CEPOL (the European Union Agency for Law Enforcement Training), should launch an initiative to train and embed this ethical assessment framework across Member States. Specifically:

- **Develop a Training Module:** Create a standardized training curriculum (e.g. an online course and workshop series) on conducting the 7-step ethical evaluation of AI and emerging tech. This could be offered to technology project managers, AI focal points, and oversight officers in each Member State's police forces. The training should include doing mock assessments on scenarios (possibly updated case studies beyond those in the report, e.g. assessing a new facial recognition system or a predictive policing tool), to build familiarity and show the practical benefits.
- **Incorporate into National Guidance:** Encourage national interior ministries or police oversight bodies to incorporate the 7-step process into their official guidance or even requirements for new technology adoption. For instance, a Member State could stipulate that any procurement of AI systems for law enforcement must be accompanied by an ethical assessment report structured according to Europol's framework. This doesn't create new law, but it complements legal DPIA requirements with a broader values-centric review. The Commission could facilitate a forum for Member States to share how they might adapt the framework to their context (some might add an extra step, or combine certain steps, etc., but the core logic should remain).
- **Refresh and Update Use Cases:** Support Europol's Innovation Lab in keeping the ethical assessment framework up-to-date ("living"). Perhaps through an EU research funding stream, regularly convene experts to add new use cases and best practices to the framework – for example, recent experiences with AI-based language translation in cross-border investigations, or lessons from using machine learning in identifying misinformation. Each update should be disseminated to national LEAs so they continuously improve their ethical decision-making skills in light of the latest knowledge. This will ensure that as AI Act enforcement begins, ethical deliberation is running in parallel with legal compliance checks, both reinforcing one another.

By mainstreaming this framework, the EU would help create a common ethical standard across Europe's law enforcement community – demonstrating to the public that, everywhere from Lisbon to Vilnius, police are asking the right questions before switching on a new AI system. This will also help anticipate and defuse potential conflicts between law enforcement objectives and fundamental rights obligations, thus complementing the AI Act's legal enforcement with a culture of self-reflection and accountability.

By implementing these recommendations, EU policymakers would create a virtuous cycle: tools and guidance from projects feed into sandboxes and hubs, which in turn produce improved practices and compliant solutions, which are then distributed out to all Member States via central platforms.

EACTDA's pioneered networked approach reduces duplication of effort (one country's solution can be adopted by another's police rather than building anew) and raises the overall baseline of compliance and capability, as well as facilitates uptake of innovations.

Importantly, it focuses on synergy with existing efforts – Europol's work, EACTDA's role, national initiatives – avoiding the pitfall of proposing brand-new institutions that might take years to establish. New structures should only be considered if absolutely necessary; so far, it appears that by reinforcing and connecting what we already have, the EU can meet the needs.

6. Conclusion

Europe stands at a pivotal moment in steering the future of AI in law enforcement. The dual imperative is clear: we must empower our police and security agencies with cutting-edge AI tools to keep citizens

safe, and we must do so in a way that steadfastly protects the rights and values that define our democracies.

Lessons from current initiatives is encouraging – a range of innovative projects and programs have shown that responsible innovation is achievable. From the micro-level practices of Tools4LEAs' ELSA working group ensuring no algorithm is developed without a privacy and ethics check, to the macro-level structures of national sandboxes aligning innovation ecosystems with EU rules, Europe already has many building blocks of an effective governance regime for AI in the security realm.

European Commission officials and Member State policymakers are in position to leverage knowledge of what works in practice and avoid pitfalls of establishing ever new structures which produce no results. This means actively facilitating collaboration: letting the experts in ethics-by-design (like those in Tools4LEAs and STARLIGHT) teach others; enabling law enforcement units in one country to test their ideas in another's sandbox; and providing common tools so that a small police agency can perform an AI Act compliance self-check just as easily as a large agency can. By amplifying synergies – e.g., integrating Europol's ethical assessment into EACTDA's development workflow, or using Lithuania's sandbox insights to inform all sandboxes – the EU will save time and resources while improving outcomes.

In the coming years, as the AI Act's provisions bite and technologies like advanced analytics, machine learning, and autonomous systems become more commonplace in policing, the EU must ensure that no law enforcement agency is left behind in capability or in compliance. Success will mean that European citizens can reap the benefits of AI-enhanced security – such as faster investigations and prevention of crimes – without fearing abuse or Orwellian outcomes. It will mean that when a new AI tool is introduced by the police, the public can be confident it has passed thorough ethical vetting and legal checks, akin to a new drug passing clinical trials.

ⁱ https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/thematic-areas/fighting-crime-and-terrorism-including-critical-infrastructure-protection_en