Tools4LEAs

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

EACTDA

D2.5 Strategy, plan, and handbook for contributions to policy making, standardisation, and other knowledge building activities

Co-funded by
the European Union

Version:	1.0	
Delivery date:	October 2023	
Dissemination level:	Public	
Status	FINAL	
Nature:	Report	
Main author(s):	Juan Arraiza	EACTDA
Contributor(s):	Rimantas Žylius	L3CE seconded to 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	29/10/2023	Juan Arraiza (EACTDA) Rimantas Žylius (L3CE seconded to EACTDA)	Updated with received feedback
1.0	30/10/2023	Juan Arraiza (EACTDA)	Final version, ready to be submitted

Co-funded by the European Union

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. Strategy for policy making and standardisation 7
3. Policy Proposals 9
3.1. Plan of the Policy Proposal Development 9
3.2. Handbook for Policy Proposals Development 11
3.3. Timeline 12
4. Standardisation and other knowledge building activities 13
4.1. Handbook 13
4.2. Plan 13
4.2.1. DevSecOps Body of Knowledge 13
4.2.2. Collaborations with standardisation related organisations 15
5. Summary 16
5.1. Conclusion 16
5.2. Evaluation 16
5.3. Future work 16
ANNEX I – Relevant policies and regulations identified 17
Cybercrime 17
State of play 17
Upcoming proposals 18
Privacy and data protection 19
State of play 19
Upcoming proposals 19
Security research work programmes 20
State of play 20
Upcoming proposals 20

Co-funded by the European Union

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 Jul’23 by 23 members from 14 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), it is proposed to double the number of tools delivered. The repository of tools implemented in v1, and currently used to host the results of the Tools4LEAs projects, will be 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. The technical, IPR, and administrative aspects necessary to create this new repository of security research results will be put in place. In addition, the v2 project will include 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 (NN) will be included, with nodes planned in Lithuania, France, Spain, and maybe one or two additional ones. A platform for end-users to evaluate online tools will be implemented. Finally, the v2 project will include 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 cybercrime[1] 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:

- **D2.6 Report on contributions to policy making, standardisation, and other knowledge building activities:** Deliverable D2.6 will provide an update to the content presented in deliverable D2.5.

1.4. Structure of the deliverable

Section 2 presents the targeted contributions of this document and introduces the concept of regulatory frameworks as an environment for innovations.

Section 3 describes the process designed within the Tools4LEAs project for policy proposals development. This process is being used and will continue being used until the end of the project.

Section 4 presents the work done around standardisation, which mainly focuses on the preparation of a DevSecOps Body of Knowledge document.

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.

[1] Find the European Commission's definition of cybercrime at: https://home-affairs.ec.europa.eu/cybercrime_en

Co-funded by the European Union

ANNEX 1 presents the list of policies and regulations which have been identified as relevant for process for policy proposals development.

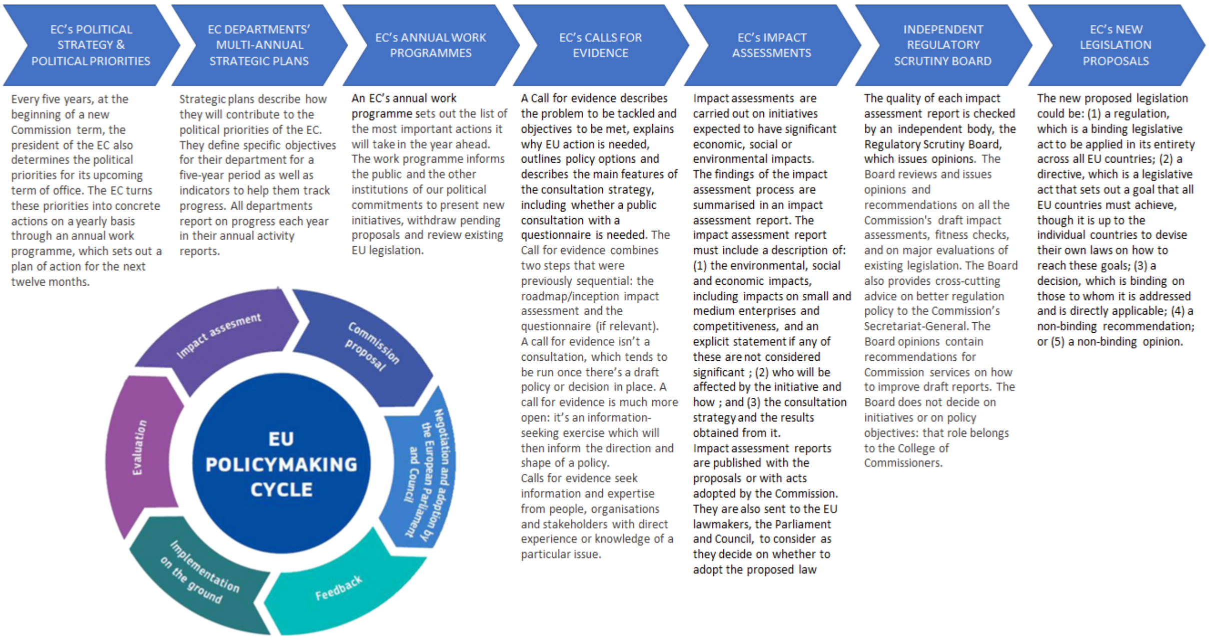
Co-funded by the European Union

2. Strategy for policy making and standardisation

A policy is a set of ideas, principles or plans that define a course of action. In the case of public policy making, it can be used, for example, to decide about new regulation, design of multi-annual work and financial programmes, etc. Organisations of all types may define their own policies, in compliance with public policies, but which might go beyond and/or be more tailored to the characteristics and/or needs and specific context of each specific organisation.

In the context of the Tools4LEAs project, and more specifically the focus of this deliverable, is on providing proposals to public policy making, mainly by the European Commission but also to EU member states, in the domain of research and innovation related to fighting cybercrime.

Within the European Union, the policy making cycle can be summarised as depicted in Figure 1. The contributions of a project such as the Tools4LEAs must be aware of this framework and of its current status before making any effort to recommend and/or make any policy proposals to the European Commission and/or to any other relevant policy makers. The policy proposals included in this document fit under the "EC's calls for evidence" step of the process described in the figure.



EC's POLITICAL STRATEGY & POLITICAL PRIORITIES

Every five years, at the beginning of a new Commission term, the president of the EC also determines the political priorities for its upcoming term of office. The EC turns these priorities into concrete actions on a yearly basis through an annual work programme, which sets out a plan of action for the next twelve months.

EC DEPARTMENTS' MULTI-ANNUAL STRATEGIC PLANS

Strategic plans describe how they will contribute to the political priorities of the EC. They define specific objectives for their department for a five-year period as well as indicators to help them track progress. All departments report on progress each year in their annual activity reports.

EC's ANNUAL WORK PROGRAMMES

An EC's annual work programme sets out the list of the most important actions it will take in the year ahead. The work programme informs the public and the other institutions of our political commitments to present new initiatives, withdraw pending proposals and review existing EU legislation.

EC's CALLS FOR EVIDENCE

A Call for evidence describes the problem to be tackled and objectives to be met, explains why EU action is needed, outlines policy options and describes the main features of the consultation strategy, including whether a public consultation with a questionnaire is needed. The Call for evidence combines two steps that were previously sequential: the roadmap/inception impact assessment and the questionnaire (if relevant).
A call for evidence isn't a consultation, which tends to be run once there's a draft policy or decision in place. A call for evidence is much more open: it's an information-seeking exercise which will then inform the direction and shape of a policy.
Calls for evidence seek information and expertise from people, organisations and stakeholders with direct experience or knowledge of a particular issue.

EC's IMPACT ASSESSMENTS

Impact assessments are carried out on initiatives expected to have significant economic, social or environmental impacts.
The findings of the impact assessment process are summarised in an impact assessment report. The impact assessment report must include a description of: (1) the environmental, social and economic impacts, including impacts on small and medium enterprises and competitiveness, and an explicit statement if any of these are not considered significant ; (2) who will be affected by the initiative and how ; and (3) the consultation strategy and the results obtained from it.
Impact assessment reports are published with the proposals or with acts adopted by the Commission. They are also sent to the EU lawmakers, the Parliament and Council, to consider as they decide on whether to adopt the proposed law

INDEPENDENT REGULATORY SCRUTINY BOARD

The quality of each impact assessment report is checked by an independent body, the Regulatory Scrutiny Board, which issues opinions. The Board reviews and issues opinions and recommendations on all the Commission's draft impact assessments, fitness checks, and on major evaluations of existing legislation. The Board also provides cross-cutting advice on better regulation policy to the Commission's Secretariat-General. The Board opinions contain recommendations for Commission services on how to improve draft reports. The Board does not decide on initiatives or on policy objectives: that role belongs to the College of Commissioners.

EC's NEW LEGISLATION PROPOSALS

The new proposed legislation could be: (1) a regulation, which is a binding legislative act to be applied in its entirety across all EU countries; (2) a directive, which is a legislative act that sets out a goal that all EU countries must achieve, though it is up to the individual countries to devise their own laws on how to reach these goals; (3) a decision, which is binding on those to whom it is addressed and is directly applicable; (4) a non-binding recommendation; or (5) a non-binding opinion.

EU POLICYMAKING CYCLE
Impact assesment
Commission proposal
Negotiation and adoption by the European Parliament and Council
Feedback
Implementation on the ground
Evaluation

Figure 1 - Summary of the EU policy making cycle

Independently of whether the policies are public or private, standards can be defined after they are outlined to set the rules that must be used to implement the policies. This document also presents Tools4LEAs-v2 strategy, plan, and handbook of planned standardisation efforts.

Some policies can have none, one, or more than one standard associated to it. A handbook with guidelines and recommendations on how the policies can be implemented is to be provided. Finally, affected practitioners will be able to create procedures from the standards and guidelines that implement the policies presented in this document. Organisations become increasingly proactive as they mature and formalise policies, use standards, and create and implement procedures and processes.

Co-funded by the European Union

In the case of standards, they can be *de jure* or *de facto*. *De jure* standards refer to standards that are established or mandated by law, while *de facto* standards are a custom or convention that has achieved a dominant position by public acceptance or market forces.

In the context of the Tools4LEAs -v2 project, and more specifically the focus of this deliverable, is on the efforts to facilitate the creation of *de facto* standards among the European security research community in the area of software development and testing. Though it is not its main focus, EACTDA and the Tools4LEAs series of projects will support to the best of their capacity any efforts of target end-user community or any other key stakeholder in the European security research and innovation value chain that follow the policies and strategies defined by the European Union in relation to the fighting of cybercrime.

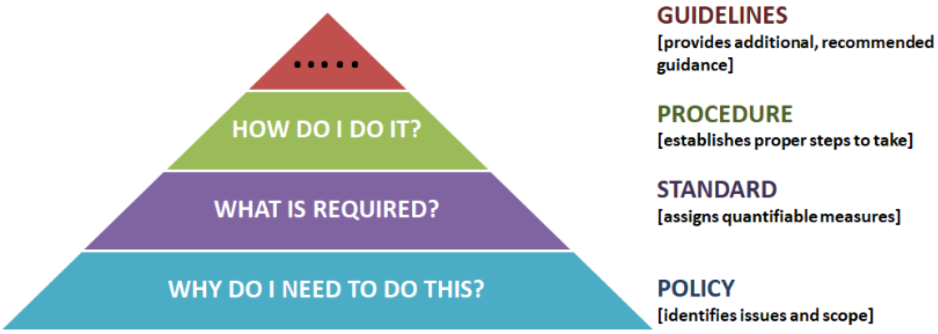

.....
HOW DO I DO IT?
WHAT IS REQUIRED?
WHY DO I NEED TO DO THIS?
GUIDELINES
[provides additional, recommended guidance]
PROCEDURE
[establishes proper steps to take]
STANDARD
[assigns quantifiable measures]
POLICY
[identifies issues and scope]

Figure 2 - Policies, standards, procedures, and guidelines

After presenting the targeted contributions for policy making and standardisation, the next section will present the process that has been designed and that is being used within the Tools4LEAs project to prepare the policy proposals.

Co-funded by the European Union

3. Policy Proposals

3.1. Plan of the Policy Proposal Development

In this section we describe in detail the process used for developing policy proposals. This process aims to analyse innovative solutions (be it technology, or innovative ways of organising work, etc.) against relevant body of regulations. The outcome of such analysis is either a) conclusion, solution fully complies to the policies and regulations, or b) that solutions needs to be modified in order to comply to the policies and regulations, or c) that while the application of the solution has huge value, it can not be used in the current policy/regulatory framework, so they have to be modified.

Importantly, that Tools4LEAs-v2 role will be to develop comprehensive process and facilitate and implementation, but actual compliance check can only be performed by the developers of the tools. So collaborative process will be set up.Further we discuss in more detail the process and plan for implementation to test the solution's compliance to the policy/regulatory environment and policy proposal development.

Analyse innovation in order to identify related regulatory domains.

The evaluation procedure starts with the analysis of innovative tools, which should be described in detail, of how and by whom it would be used, what data should be provided as inputs, what outputs are produced, what technologies are used in processing, how training of algorithms, if relevant, is done, etc.

Tools4LEAs-v2will develop the structured electronic questionnaire, which will guide developers of tools to provide relevant information about the tools.

Identify and list related regulations, policies, legal frameworks.

As per description of the innovative tool, in the step mapping of features of innovation with specific regulations will be done. E.g., if the tool will use personal data, then GDPR will be mapped as one of relevant legislative frameworks.

Tools4LEAs-v2 task team will develop the matrix (and further enhance the model with every iteration enriching it with gathered information), which would cover all relevant aspects for the developed tools.

The regulatory analysis

Understandably, the matrix will be a guiding model rather than complete solution. So additional expert-based evaluation might be done depending on the composition of innovation, functions of the tools and possible way to use for law enforcement or other purposes.

The task team further will make regulatory analysis facilitated by the in previous step mapped innovations' relevant aspects with key regulations. The regulatory analysis will document these aspects related to regulatory environment of innovation:

- which parts of innovation in a tool or it's possible ways of usage complies with laws and policies;

Co-funded by the European Union

- what are the possible areas of conflict with in force or proposed regulation and policies;
- what are the possible gaps in force or proposed regulation and policies;
- what are the grey or dark zones of in force or proposed regulation and policies;
- what are the areas in in force or proposed regulation and policies which can be improved so that to ensure the balance between the rights and freedoms on individuals and law enforcement purposes.

Development of Policy Proposals

The conclusions of regulatory analysis would be presented at the EACTDA Secretariat, innovative technology provider, relevant end-users or other relevant partners for discussion and proposals development.

The focus of the policy proposals will be on three areas/ domains, the first one being cybercrime in general, the second one privacy and data protection, and the third one European security research work programmes.

Ad hoc meetings or workshops might be organised to resolve issues, test ideas. The aim is to reach consensus on these recommendations:

- Recognition that there are no policy obstacles for innovation in question uptake (or identification of areas where no changes are needed).
- Policy uptake recommendation, in case innovation can be leveraged, but its use requires specific considerations to be considered (e.g., specific ways of implementation, etc.).
- Potential regulatory changes, in case current regulation must be changed for innovation to be fully leveraged.
- Remaining unsolved barriers/issues, in case there is no reasonable grounds for changes in existing regulations, but current regulation does not allow leveraging potential of innovation (e.g., innovation would require unacceptable intrusion to privacy).
- Proposed action plan for uptake of each recommendation.

The figure below summarises the aforementioned process.

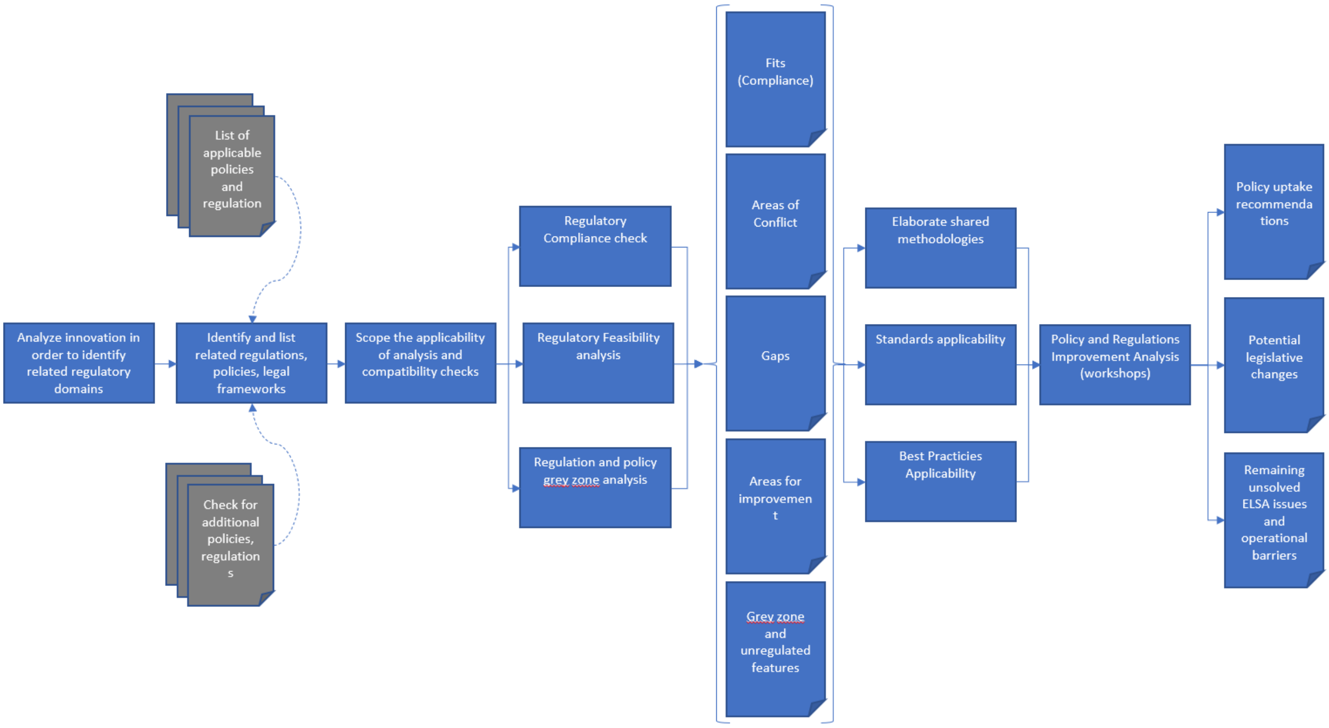

List of applicable policies and regulation
Check for additional policies, regulations
Analyze innovation in order to identify related regulatory domains
Identify and list related regulations, policies, legal frameworks
Scope the applicability of analysis and compatibility checks
Regulatory Compliance check
Regulatory Feasibility analysis
Regulation and policy grey zone analysis
Fits (Compliance)
Areas of Conflict
Gaps
Areas for improvement
Grey zone and unregulated features
Elaborate shared methodologies
Standards applicability
Best Practicies Applicability
Policy and Regulations Improvement Analysis (workshops)
Policy uptake recommendations
Potential legislative changes
Remaining unsolved ELSA issues and operational barriers

Figure 3 - Process of development of policy proposals for innovations

ANNEX I includes all the policies and regulations, in force and upcoming, that have been identified and considered relevant. The list presented in ANNEX I is not exhaustive and will be updated as necessary during the course of the rest of the Tools4LEAs-v2 project.

Actions to Uptake Developed Policy Proposals

Every organization deemed responsible will further execute actions for uptake of policy proposals. Organizations will report execution of tasks which will be consolidated in the task report.

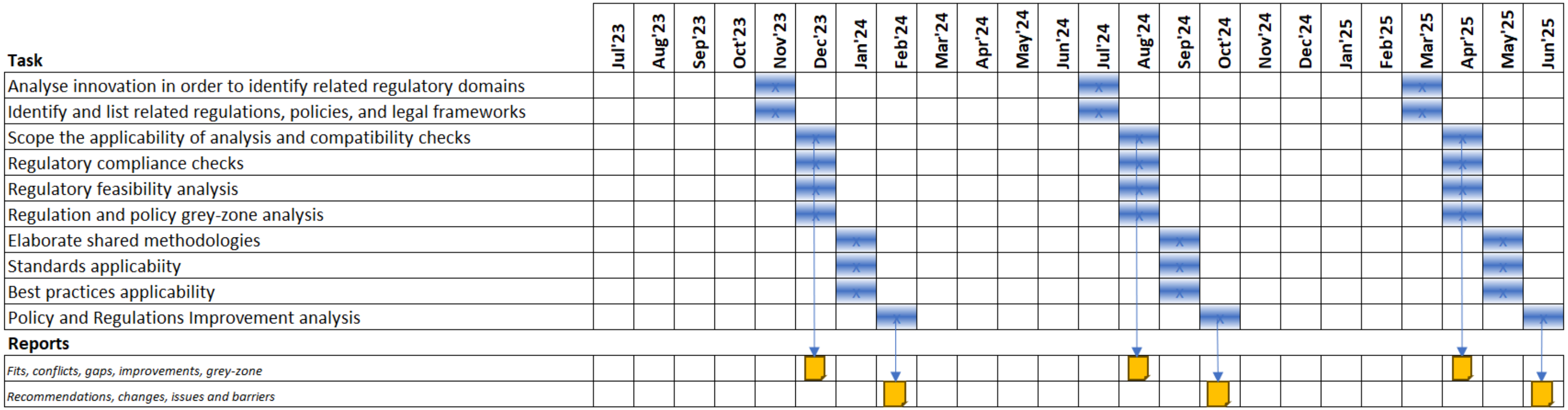
3.2. Handbook for Policy Proposals Development

Based on the experience of first iteration of Policy Proposal Development, task team will decide if it would be useful to consolidate material prepared for the Policy Proposal Development to practical handbook to further facilitate participation of developers of innovative tools in this process.

This decision will be made on from solely practical considerations with the only aim to facilitate relevant participation of stakeholders in the process.

3.3. Timeline

The Tools4LEAs v2 project will continue implementing the process to develop policy proposals defined in the Tools4LEAs v1 project. The Gantt below summarises the high-level plan that has been prepared for the Tools4LEAs v2 project:



Task	Jul'23	Aug'23	Sep'23	Oct'23	Nov'23	Dec'23	Jan'24	Feb'24	Mar'24	Apr'24	May'24	Jun'24	Jul'24	Aug'24	Sep'24	Oct'24	Nov'24	Dec'24	Jan'25	Feb'25	Mar'25	Apr'25	May'25	Jun'25
Analyse innovation in order to identify related regulatory domains					▨								▨								▨			
Identify and list related regulations, policies, and legal frameworks					▨								▨								▨			
Scope the applicability of analysis and compatibility checks						▨								▨								▨		
Regulatory compliance checks						▨								▨								▨		
Regulatory feasibility analysis						▨								▨								▨		
Regulation and policy grey-zone analysis						▨								▨								▨		
Elaborate shared methodologies							▨								▨								▨	
Standards applicabiity							▨								▨								▨	
Best practices applicability							▨								▨								▨	
Policy and Regulations Improvement analysis								▨								▨								▨
Reports																								
Fits, conflicts, gaps, improvements, grey-zone						🗎								🗎								🗎		
Recommendations, changes, issues and barriers								🗎								🗎								🗎

Figure 4 - high-level work plan for the contributions for policy making

4. Standardisation and other knowledge building activities

4.1. Handbook

Task 2.4 of the Tools4LEAs project takes care of all the work done by EACTDA within the Tools4LEAs project to promote voluntary and consensus-based standards developed in the partnership with security practitioners with the aim of playing a critical role to increase the trust and to foster innovations adoption by European public security entities fighting cybercrime. By providing agreed ways of naming, describing and specifying, testing and validating, managing and reporting, EACTDA will take a proactive role in transferring the research results into more standards that could have a significant impact on the implementation and extensive use.

EACTDA and the Tools4LEAs project focus on the "*de facto*" standardisation approach, more than on the "*de jure*" approach, which implies that compliance with the standard is mandated by law. De facto standards are those that have a high penetration and acceptance in the market, but are not yet official or which are not mandated by law. *De Facto* standards can be defined and/or promoted by individual organisations that have a key role in the community of practitioners, or by the community as such. *De jure* or official standards are normally defined by standardisation organisations such as the CEN, CENLEC, ETSI, ISO, IEC, ITU, ISO, ANSI, among others. While standardisation organisations are key stakeholders for *de jure* standards, the success of *de facto* standards is based on the use of the standard practically by the targeted community.

When the efforts to define a "de facto" standard are promoted or led by EACTDA, a methodology based on the Capability Maturity Model Integration (CMMI)[2]. This model can be used to provide guidance for developing or improving processes that meet the business goals of an organisation. A CMMI model may also be used as a framework for appraising the process maturity of the organisation. In short, the CMMI methodology is based on process areas, which are clusters of related practices in an area that, when implemented collectively, satisfy a set of goals considered important for making improvement in that area. Also, CMMI provides a staged representation, which is designed to provide a standard sequence of improvements that can serve as a basis for improving the overall maturity level of the organisation.

4.2. Plan

4.2.1. DevSecOps Body of Knowledge

DevSecOps is short for development, security and operations. DevOps is a methodology in the software development and IT industry used as a set of practices and tools which integrates and automates the work of software development (Dev) and IT operations (Ops) as a means for improving and shortening the systems development life cycle. DevSecOps integrates security initiatives at every stage of the DevOps to deliver robust and secure applications.

The Tools4LEAs-v2 project will invest an important part of its *de facto* standardisation efforts around the completion of the DevSecOps Body of Knowledge initiative.

[2] https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration

Once the DevSecOps BoK is ready and published, EACTDA intends to use it to improve its own DevSecOps practices. Besides, EACTDA's own implementation of the DevSecOps BoK will be used in the Tools4LEAs-v2 (and subsequent iterations/projects) and it is the intention to make it public so that other organisations can use it as a reference or model for their own implementations of the DevSecOps BoK.

In a nutshell, DevSecOps is the acronym for development, security, and operations, and it can be defined as the integration of security at every phase of the software development and operations lifecycle, from initial planning, design, development, build, integration, testing, release, delivery, deployment and operation in production environments.

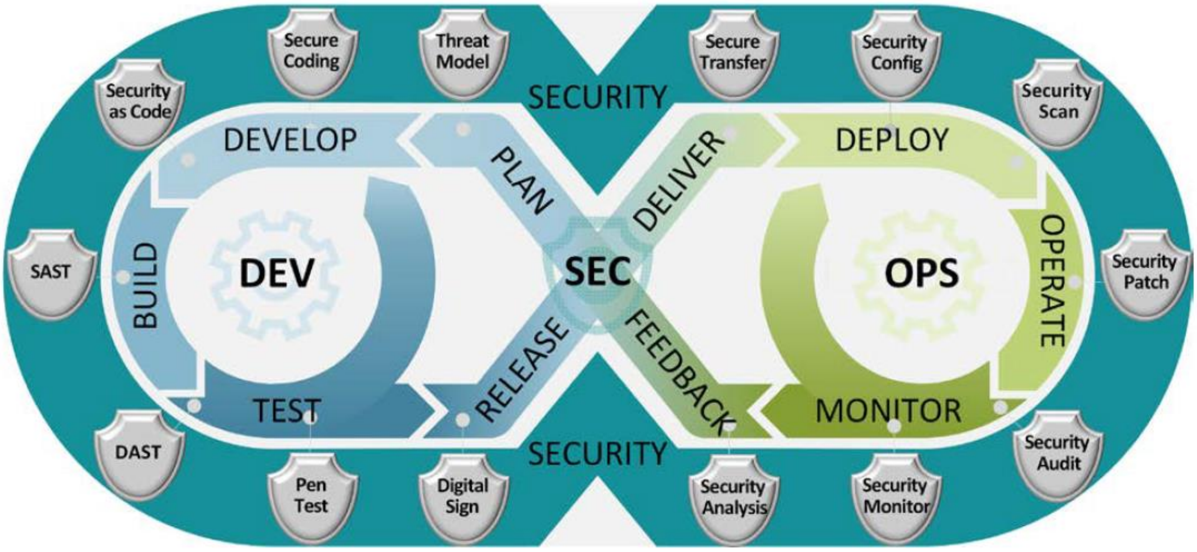


Figure 5 - DevSecOps Lifecycle (source: US DoD Enterprise DevSecOps Reference Design)

The first public release of the EACTDA / Tools4LEAs DevSecOps Body of Knowlege document was planned for late Summer 2023. It was delayed, due to the lack of sufficient volunteers and contributions by the community.

Now, as it has been included in the scope of the Tools4LEAs-v2 project, EACTDA will lead and promote the completion of the DevSecOps Body of Knowledge, with an additional twist in order to add to it the specificities of software that is developed for and operated by public entities fighting cybercrime.

Once it is ready, special efforts will be made to promote the DevSecOps Body of Knowledge for practical use within the European security research and innovation community.

Two target groups will be engaged:

- LEAs of member states will be informed about the EACTDA / Tools4LEAs DevSecOps Body of Knowledge and its relevance. This is additional opportunity to promote EACTDA as key player in LEAs domain.
- Active EU funded projects should be scanned and if relevance can be recognized, they will be contacted to the proposal to uptake EACTDA / Tools4LEAs DevSecOps Body of Knowledge

Depending on the response of the reached-out groups, it further might be necessary to develop a comprehensive governance structure of the DevSecOps Body of Knowledge with the clear path how other parties can join the governance and impact development visions.

4.2.2. Collaborations with standardisation related organisations

At first, it was the intention/plan for EACTDA and the Tools4LEAs-v1 project that during the second year of the project contacts with EU standardisation and related organisations such as CEN, CENELEC, ETSI, or ISO where to be launched. However, considering the limited resources available and the prioritisation made to promote and contribute to the DevSecOps Body of Knowledge, these contacts were suspended/postponed.

During the Tools4LEAs v2 project it is planned to activate the aforementioned contacts with the EU standardisation and related organisations. But instead of directly approaching these organisations, the plan is to firstly contact ENISA and Europol to ensure that whatever efforts are made by EACTDA/Tools4LEAs are in alignment with their plans and strategies. The main goal of these preliminary contacts with the EU agencies is to explore and identify areas of collaboration so that conflicts or unnecessary overlapping are avoided and that the limited efforts EACTDA and Tools4LEAs-v2 can spend have the greatest and most beneficial impact possible.

Co-funded by the European Union

5. Summary

5.1. Conclusion

In this document we have presented the strategy for contributions to policy making, standardisation, and other knowledge building activities. Next, for each of those types of activities, a handbook with the detailed steps, processes, and recommended best practices is presented along with the work-plan that has been prepared to conduct such activities.

5.2. Evaluation

This deliverable builds on the experience gained during the Tools4LEAs-v1 project, which has proved to be valid. This document serves the purpose for which it is intended, which is to set the strategy, plan, and operational handbook that will be used by the EACTDA personnel when working on contributions to policy making, standardization, and other knowledge building activities within the Tools4LEAs-v2 project.

However, as a continuous improvement approach will be implemented, the on contributions to policy making, standardization, and other knowledge building activities to be conducted within the Tools4LEAs-v2 project might be updated during the lifetime of the project to adapt to the new needs.

5.3. Future work

Though there is no official update of this document within the Tools4LEAs-v2 project, EACTDA will continue working on policy and standardisation proposals during the Tools4LEAs-v2 project, and the knowledge gained in v2, and that will be reported in deliverable D2.6, will serve as a starting point for the Tools4LEAs-v3 project, which if everything goes well, will start in July 2025.

ANNEX I – Relevant policies and regulations identified

Below we present a list of policies and regulations that have been identified as relevant to the Tools4LEAs project. Innovations will be tested in policy proposals process against them. This is a not exhausting list, and it is planned to amended it as necessary during the rest of the Tools4LEAs project.

Cybercrime

State of play

Policies

- The **European Security Union** - https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en; and more specifically the **policy on cybercrime** - https://home-affairs.ec.europa.eu/cybercrime_en
- European Commission – **Cybersecurity strategy** - https://digital-strategy.ec.europa.eu/en/policies/cybersecurity
- **e-Evidence** - https://home-affairs.ec.europa.eu/cybercrime/e-evidence_en
- **Encryption** - https://home-affairs.ec.europa.eu/cybercrime/encryption_en
- **EU strategy for a more effective fight against child sexual abuse** - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0607&from=ES
- A Digital Decade for children and youth: the **new European strategy for a better internet for kids (BIK+)** - https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik
- The **2022 Code of Practice on Disinformation** - https://ec.europa.eu/newsroom/dae/redirection/document/87585

In force regulation

- **Convention on Cybercrime** (aka, Budapest Convention) - https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN
- DIRECTIVE (EU) 2019/713 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on **combating fraud and counterfeiting of non-cash means of payment** and replacing Council Framework Decision 2001/413/JHA - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0713&from=EN
- **NIS Directive** - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN https://www.enisa.europa.eu/topics/nis-directive
- **NIS 2 Directive** - https://eur-lex.europa.eu/eli/dir/2022/2555
- Directive 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on **attacks against information systems** and replacing Council Framework Decision 2005/222/JHA - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33193 / https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

Co-funded by the European Union

- Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the **European Electronic Communications Code (Recast)Text** with EEA relevance. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG
- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on **open data and the re-use of public sector information** - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L1024&from=EN (aka, OPEN DATA DIRECTIVE)

Upcoming proposals

- Proposal *the* ***new European Cyber Resilience Act*** - https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act#:~:text=According%20to%20the%20European%20Commission,common%20standards%20for%20cybersecurity%20products.
- ***Proposal*** for *an* ***Artificial Intelligence Act*** - (AI system intended for biometric identification of natural persons = high-risk AI system) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
- ***Proposal*** *for a* ***Police Cooperation Code****:* This legislative package includes these two relevant components: (a) Prüm II Regulation - automated comparison of facial images, driving license data and police records in LEA & Europol databases on hit/no-hit bases - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0784&from=EN; and (b) Information Exchange Directive - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0782
- *Amendments to* ***Europol Regulation*** - expanding Europol's mandate to proactively contribute to research & innovation by training, testing and validation of algorithms for LEA tools - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0796

  NOTE: the current (in-force) regulation is: "Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016", available here: https://www.europol.europa.eu/cms/sites/default/files/documents/celex_32016r0794_en_txt.pdf
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down **rules to prevent and combat child sexual abuse** - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0209&from=EN

Privacy and data protection

State of play

Policies

- European **Data Strategy** - https://digital-strategy.ec.europa.eu/en/policies/strategy-data
- **EU strategy for a more effective fight against child sexual abuse** - https://home-affairs.ec.europa.eu/system/files/2020-07/20200724_com-2020-607-commission-communication_en.pdf
- **Ethics and data protection** - https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf
- European Strategy for Data - **Data Governance Act** - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868

In force regulation

- **Charter of Fundamental Rights of the European Union** - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
- **GDPR** - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- **Data Governance Act** - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN
- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on **a framework for the free flow of non-personal data in the European Union** (Text with EEA relevance.) - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1807&from=EN
- REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the **protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies** and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1725&from=ES
- National laws of the European Union member states implementing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the **protection of natural persons with regard to the processing of personal data by competent authorities** for the purposes of the **prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties**, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN
- **National Constitutions** of the European Union member states
- **National laws** of the European Union member states on criminal procedures.

Upcoming proposals

- **ePrivacy regulation** - https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
- **Data Act** - https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data
- **Regulation to prevent and combat child sexual abuse -** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472

Co-funded by the European Union

Security research work programmes

State of play

Policies

- The **European Security Union - Innovation and security research programme** - https://home-affairs.ec.europa.eu/policies/internal-security/innovation-and-security-research_en
- **Horizon Europe** - Cluster 3: Civil security for society - https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en
- **Digital Europe** - https://digital-strategy.ec.europa.eu/en/activities/digital-programme; and more specifically, the cybersecurity work programme - https://ec.europa.eu/newsroom/repository/document/2021-45/C_2021_7913_1_EN_annexe_acte_autonome_cp_part1_v3_zCcOBWbBRKve4LP5Q1N6CHOVU_80908.pdf
- **Internal Security Funds** - https://home-affairs.ec.europa.eu/funding/internal-security-funds_en

In force regulation

- COMMISSION REGULATION (EU) No 1217/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of research and development agreements - https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:335:0036:0042:EN:PDF
- Commission Regulation (EU) No 557/2013 of 17 June 2013 implementing Regulation (EC) No 223/2009 of the European Parliament and of the Council on **European Statistics as regards access to confidential data for scientific purposes** and repealing Commission Regulation (EC) No 831/2002 Text with EEA relevance - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013R0557&from=EN
- Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 **establishing Horizon Europe – the Framework Programme for Research and Innovation**, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (Text with EEA relevance) - https://eur-lex.europa.eu/eli/reg/2021/695/oj
- Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 **establishing the Internal Security Fund** - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R1149&from=EN
- Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 **establishing the Digital Europe Programme** and repealing Decision (EU) 2015/2240 (Text with EEA relevance) - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R0694&from=EN

Upcoming proposals

- Research and Development agreements: The European Commission approves the content of its **revised draft block exemption regulation on research and development agreements** - https://www.concurrences.com/en/review/issues/no-2-2022/chroniques/research-and-development-agreements-the-european-commission-approves-the

Co-funded by the European Union