



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



D1.5 Report on Ethical, legal, privacy, and social impact activities



Co-funded by
the European Union

Version:	1.0	
Delivery date:	August, 2025	
Dissemination level:	Public	
Status	FINAL	
Nature:	Report	
Main author(s):	Juan Arraiza	EACTDA
Contributor(s):	Sigute Stankeviciute	L3CE (seconded to EACTDA)
	Eva Skruba	EACTDA

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
0.1	07/08/2025	Sigute Stankeviciute (L3CE, seconded to EACTDA) Eva Skruba (EACTDA) Juan Arraiza (EACTDA)	First version for all sections completed.
1.0	07/08/2025	Juan Arraiza (EACTDA)	Final version, ready to be submitted

TABLE OF CONTENTS

1. Introduction	4
1.1. Main objective of this document	4
1.2. Relation to other deliverables	4
1.3. Structure of the deliverable	4
2. ELSA management at Tools4LEAs V.2.	5
2.1. Organization of ELSA assessment activities	5
2.2. Data Protection Impact Assessments	15
2.3. Social Impact Assessments	20
2.4. Ethics Assessments	21
3. Summary	25
3.1. Conclusion	25
3.2. Evaluation	25
3.3. Future work	25
ANNEX I ELSA final audit report	26
<i>ANNEX A (of ANNEX I): Recommendations for ELSA compliant tool usage</i>	<i>27</i>
ANNEX II User Acceptance Test Questionnaire on ELSA	30

1. Introduction

1.1. Main objective of this document

The main objective of this document is to report on the activities conducted in relation to the ethical, legal, privacy, and social impact matters of the Tools4LEAs project.

This deliverable is based on the previously submitted deliverable Ethical, legal, privacy, and social impact (hereinafter – ELSA) handbook and ELSA activities that were done during the project.

1.2. Relation to other deliverables

This deliverable is closely related to the following deliverables:

- **Tools4LEAs v2 project's D1.4 ELSA management handbook:** Deliverable D1.5 reports on the project ethical, legal, privacy, and social impact activities conducted until July 2025, which are directly related to the handbook presented in D1.4.
- **Tools4LEAs v1 project's D1.10 Final report on Ethical, legal, privacy, and social impact activities:** Tools4LEAs v2 deliverables D1.4 and D1.5 build on top of the work done during the Tools4LEAs v1 project, which concluding report was presented within deliverable D1.10.

1.3. Structure of the deliverable

Section 2 presents a summary of the originally planned activities and the real/actual activities that have taken place until July 2025.

Section 2.1 presents organization of ELSA assessment activities

Section 2.2 presents Data Protection Impact Assessments

Section 2.3. Social Impact Assessment activities.

Section 2.4 presents Ethics Assessment activities.

Section 3 introduces with the proposed improvement of ELSA assessment, 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. ELSA management at Tools4LEAs V.2.

Below we summarise the originally planned data management, ethical, legal, privacy, and social impact activities versus the real/actual activities that have taken place in the Tools4LEAs v2 project until July 2025.

2.1. Organization of ELSA assessment activities

The Ethical, Legal, and Social Impact Assessment (ELSA) of tools developed under EACTDA are overseen by two bodies:

1. ELSA Management Team, and
2. ELSA Committee.

The ELSA Management Team is the primary EACTDA body responsible for ensuring ELSA compliance. The key responsibilities of the ELSA Management Team include:

1. Implementing and supervising ELSA compliance management procedures.
2. Analyzing Data Management Plans (DMPs) provided by tool developers.
3. Assessing Data Protection Impact Assessments (DPIAs) submitted by tool developers.
4. Conducting Ethical Impact Assessments.
5. Conducting Social Impact Assessments.
6. Organizing meetings with technology developers to discuss the DPIA
7. Organizing ELSA Committee meetings.
8. Presenting the results of DMP analyses to the ELSA Committee and sharing insights on which projects are proposed for further DPIA, Ethical, and Social Impact Assessment evaluations.
9. Presenting the results of DPIA, Ethical, and Social Impact Assessment evaluations to the ELSA Committee.
10. Drafting the deliverable "D1.5 Report on ELSA management activities."

The ELSA Committee serves as an advisory body to the ELSA Management Team regarding ELSA-related matters. The primary roles of the ELSA Committee are:

1. Providing consultations to the ELSA Management Team on issues related to DMPs, DPIAs, Ethical Impact Assessments, Social Impact Analyses and AI assessment
2. Helps to identify if there is any potential risks with ELSA assessments under the ELSA management team request.

The technology developers also have an active role in ELSA compliance assessment. They are required to:

1. Provide timely and comprehensive Data Management Plans (DMPs), Data Protection Impact Assessments (DPIAs), the ELSA questionnaires and other ELSA-related documentation as requested by the ELSA Management Team.
2. Participate in meetings and consultations with the ELSA Management Team to clarify technical, ethical, or legal aspects of their work.
3. Implement recommendations and corrective actions resulting from ELSA reviews.

4. Cooperate in the preparation and execution of social and ethical impact assessments, including facilitating access to technical documentation and end-user feedback
- 5.

The process of ELSA management is based on cooperation between ELSA Management Team, ELSA Committee and the technology developers. The cooperation between the technology developer and ELSA Management Team is crucial for effective ELSA evaluation.

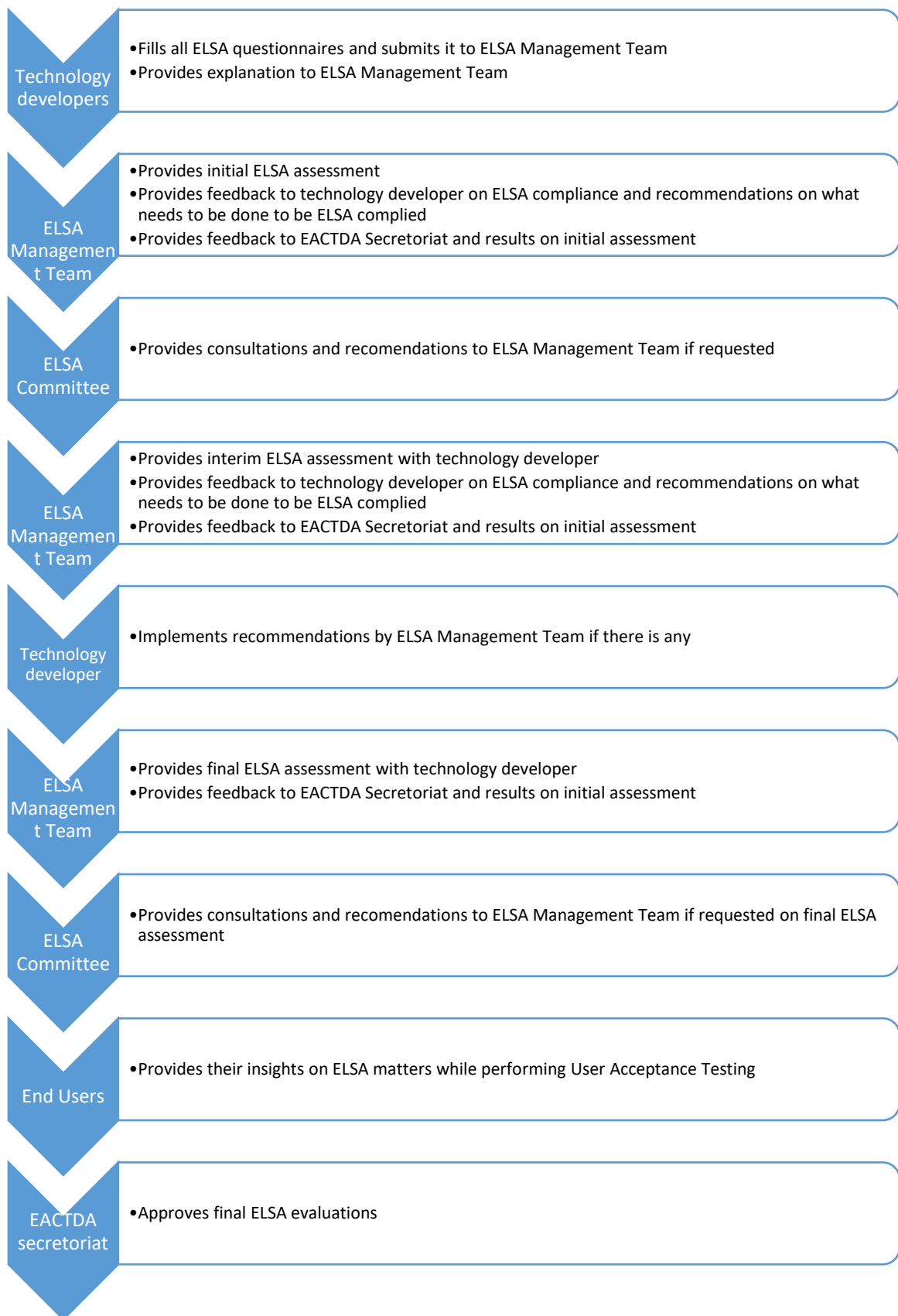
The process of cooperation of technology developer, ELSA Management Team and ELSA Committee is described in the chart below.

Technology developer	ELSA management team	ELSA Committee
• Fills in all ELSA questionnaires and DMP required by EACTDA secretariat or ELSA Management Team • Cooperates with ELSA Management Team on ELSA assessment	• Implements and supervises implementation of ELSA procedures • Analyses all the ELSA questionnaires and DMPs filled inn by Technology developers	• Provides consultations to ELSA Management Team • Helps in difficult ELSA assessment cases

EACTDA can only ensure that the tool is designed to be ELSA compliant and meets the ELSA requirements itself.

Besides, **Law enforcement institutions or any other end users** of tools developed by EACTDA are responsible for ensuring ELSA compliant use. While EACTDA can provide recommendations for the ELSA compliant use of the tools, it cannot assume responsibility for their use by end users or for compliance with national regulations.

ELSA Compliance Process: A Step-by-Step Guide



This section outlines the systematic procedure for ensuring ELSA compliance throughout a project lifecycle, involving key stakeholders such as Technology Developers, the ELSA Management Team, the ELSA Committee, End Users, and the EACTDA Secretariat.

1. Initial Engagement and Assessment Preparation

Role: Technology Developers

At the outset, Technology Developers are responsible for completing all required ELSA questionnaires¹. These documents serve as the foundational input for the ELSA assessment process. They must then submit these completed questionnaires to the ELSA Management Team. Additionally, Technology Developers are expected to provide any necessary explanations or clarifications regarding their responses to facilitate a thorough understanding by the ELSA Management Team.

2. Initial ELSA Assessment

Role: ELSA Management Team

Upon receiving the questionnaires, the ELSA Management Team conducts an initial assessment of the project's ELSA compliance. This involves a detailed review of the submitted information. The team then provides specific feedback to the Technology Developers, highlighting areas of non-compliance and offering concrete recommendations on what actions are required for the project to become ELSA compliant. The ELSA Management Team also reports the findings and results of this initial assessment to the EACTDA Secretariat.

3. Consultation and Guidance (As Needed)

Role: ELSA Committee

The ELSA Committee acts as an advisory body. If requested by the ELSA Management Team, the Committee provides expert consultations and recommendations. This guidance helps the ELSA Management Team navigate complex ethical, legal, or social challenges identified during the assessment phase.

4. Interim ELSA Assessment

Role: ELSA Management Team

Following the initial assessment and any subsequent adjustments, the ELSA Management Team conducts an interim ELSA assessment with the Technology Developers. Similar to the initial phase, this involves a review of updated information, provision of further feedback on compliance, and recommendations for continued adherence to ELSA requirements. The ELSA Management Team

¹ ALIGNER questionnaire <https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/>

once again provides an update to the EACTDA Secretariat regarding the progress and results of this interim assessment.

5. Implementation of Recommendations

Role: Technology Developers

Technology Developers are responsible for actively implementing all recommendations provided by the ELSA Management Team. This step is crucial for addressing identified gaps and ensuring that the project evolves towards full ELSA compliance as development progresses. This phase emphasizes iterative improvement based on expert guidance.

6. Final ELSA Assessment

Role: ELSA Management Team

Once the Technology Developers have implemented the necessary changes, the ELSA Management Team performs a final, comprehensive ELSA assessment. This assessment aims to verify that all ethical, legal, and social requirements have been met. The team provides final feedback to the Technology Developers and delivers a conclusive report of the assessment results to the EACTDA Secretariat.

7. Final Consultation and Recommendations (As Needed)

Role: ELSA Committee

At this critical stage, the ELSA Committee may again be called upon by the ELSA Management Team to provide consultations and recommendations, particularly if there are outstanding questions or complex issues requiring expert opinion before the final approval. Their input ensures robust scrutiny of the final ELSA assessment.

8. User Acceptance Testing (UAT) Insights

Role: End Users

During the User Acceptance Testing (UAT) phase, End Users play a vital role in providing their insights on ELSA matters from a practical, real-world perspective. Their feedback helps identify any unforeseen ethical, legal, or social implications of the technology in actual use, contributing to a more holistic ELSA review.

9. Final Approval

Role: EACTDA Secretariat

The ultimate responsibility for approving the project's ELSA evaluations rests with the EACTDA Secretariat. Based on all assessments, feedback, and reports from the ELSA Management Team,

the ELSA Committee, and End Users, the EACTDA Secretariat makes the final decision on whether the project has achieved satisfactory ELSA compliance.

This structured breakdown aims to provide a clear, easy-to-understand narrative of the entire ELSA compliance process, detailing each step and the responsibilities of the involved parties.

Acronym / short-title	Project start date	Project end date	Simplified Questionnaire on data processing submitted?	Social impact Questionnaire submitted	Ethical impact Questionnaire submitted	AI evaluation Questionnaire submitted	Questionnaires answered?	AI involved?	Assessment completed?
APINGA	Nov'23	Oct'24	21/01/2024	21/01/2024	21/01/2024	01/08/2024	yes	no	yes
GELATO	Nov'23	Oct'24	21/01/2024	21/01/2024	21/01/2024	01/08/2024	yes	no	yes
CSIM	Nov'23	Nov'24	21/01/2024	21/01/2024	21/01/2024	01/08/2024	yes	no	yes
T4L-VIDSUM	Jan'24	Dec'24	21/01/2024	21/01/2024	21/01/2024	01/08/2024	yes	yes	yes
Vysion Ransomware Monitor	Nov'24	Nov'24	21/01/2024	23/01/2024	24/01/2024	01/08/2024	yes	no	yes
STAMPER	Mar'23	Jun'25	01/08/2024	01/08/2024	01/08/2024	01/08/2024	yes	no	yes
AutoPodMobile	Apr'24	Apr'25	01/08/2024	01/08/2024	01/08/2024	01/08/2024	yes	no	yes
Tattoo Detection	Jul'24	Mar'25	01/08/2024	01/08/2024	01/08/2024	01/08/2024	yes	yes	yes
Transkit	Apr'24	Mar'25	01/08/2024	01/08/2024	01/08/2024	01/08/2024	yes	yes	yes

Robust Hashing	Nov'24	Jun'25	01/08/2024	01/08/2024	01/08/2024	01/08/2024	yes	no	yes
Graphsense Standalone	Jul'24	Jun'25	01/08/2024	03/08/2024	04/08/2024	05/08/2024	yes	no	yes
Discord Scrapper	Jul'24	Jun'25	01/08/2024	01/08/2024	01/08/2024	01/08/2024	Yes	no	Yes
Telegram Grabber	Jul'24	Jun'25	07/08/2024	07/08/2024	07/08/2024	07/08/2024	yes	No	yes
DeepThought	Jul'24	June'25	01/08/2024	01/08/2024	01/08/2024	01/08/2024	yes	no	yes
ARICA	Oct'24	Jun'25	28/09/2024	28/09/2024	28/09/2024	28/09/2024	Yes	Yes	Yes
FaceCog	Oct'24	Jun'25	28/09/2024	28/09/2024	28/09/2024	28/09/2024	Yes	Yes	Yes
Federated Learning	Nov'24	Jun'25	yes	yes	yes	yes	yes	yes	yes
PersonREID	Nov'24	Jun'25	yes	yes	yes	yes	yes	yes	yes
Hashtopolis	Dec'24	Jun'25	yes	yes	yes	no	yes	no	yes
EU DAMA	Jan'25	Jun'25	yes	yes	yes	no	yes	no	yes

The table above shows the list of ELSA assessments that were conducted. Majority of projects had no potential ELSA issues. However, the ELSA compliance recommendations were provided for the following projects:

1. ARICA:

- Implement a comprehensive conformity assessment process that includes DPIA, Ethical Impact Assessment (EIA), and compliance checks according to the AI Act's requirements.
- Ensure that the tool employs advanced encryption, data minimization techniques, and strict access controls.
- Implement strict controls to ensure that all outputs are verified by human analysts before being used in decision-making. Clearly define and document the limitations of the AI algorithms to avoid misinterpretation or misuse.
- Implement mandatory human-in-the-loop processes, where all outputs are reviewed and validated by trained investigators before any action is taken. Establish clear guidelines for the role of human oversight in the decision-making process.
- Develop comprehensive user documentation and training materials that clearly outline the tool's capabilities, limitations, and potential risks. Include mechanisms for users to understand and challenge the tool's outputs.
- Conduct a comprehensive human rights impact assessment and implement ethical design principles to ensure that the tool respects fundamental rights. Engage with civil society organizations and legal experts to validate the tool's compliance.
- Implement state-of-the-art security measures, including encryption, secure storage, and multi-factor authentication. Conduct regular penetration testing and security assessments to identify and mitigate vulnerabilities.
- Establish a post-market monitoring system to track the tool's use and ensure that it remains within its intended legal and ethical boundaries. Any expansions in scope should undergo a thorough compliance review.
- Regularly assess the tool for potential biases, use diverse training datasets, and implement fairness and bias mitigation strategies to ensure compliance with non-discrimination principles.
- Develop a dedicated compliance team to manage conformity assessments, documentation, and risk management activities. Ensure all regulatory requirements are met before the tool is deployed.

2. FaceCog

- Conduct a comprehensive conformity assessment as mandated by the AI Act, ensuring that all necessary documentation, transparency, and risk management measures are in place.
- Implement regular audits and validation processes to ensure that the training data is of high quality, diverse, and representative of the population. Use synthetic and real-world datasets to test for biases.
- 3. Implement state-of-the-art security measures, including encryption and access controls, and conduct regular security assessments. Ensure compliance with the GDPR and the Law Enforcement Directive.
- Conduct thorough bias and fairness evaluations throughout the model's development and deployment phases. Use balanced training datasets and implement bias mitigation strategies.

- Develop clear documentation and user guidelines, explaining how the LR method works, its limitations, and the proper way to interpret its outputs. Provide training to ensure that all end-users have a thorough understanding of the tool.
- Establish strict access controls, define clear boundaries for the tool's use, and conduct regular audits to monitor compliance. Deploy a use-case limitation mechanism to ensure that the tool is only used for its intended purpose.
- Implement mandatory human-in-the-loop processes, where a qualified forensic expert must review and validate all outputs before they are used in legal contexts. Clearly define the role of human oversight in the decision-making process.
- Conduct a thorough human rights impact assessment to evaluate and mitigate any potential negative impacts.
- Implement comprehensive security measures, including advanced encryption, secure storage, and regular penetration testing. Conduct continuous monitoring to identify and address potential security threats.
- Establish a dedicated compliance team to oversee conformity assessments and ensure that all documentation and regulatory requirements are met.

3. EU DAMA

- Privacy Impact assessment: High (due to potential data exposure)
- Public Trust Impact: Medium to High (dependent on transparency and oversight measures)
- Operational/Investigative Impact: High positive impact if the tool is implemented with robust safeguards.

2.2. Data Protection Impact Assessments

Plan				Real				Status
What	Who	When	How	What	Who	When	How	
DPIA evaluation procedure	Authors of this document	Undefined	Undefined	DPIA evaluation procedure prepared	Authors of this document	2024-25	See the description below	Done, not updated since

The DPIA evaluation procedure for the Tools4LEAs project has been defined as follows. Firstly, the GDPR requires to conduct DPIA in case of:

1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
2. processing on a large scale of special categories of data referred to in Article 9(1) of GDPR, or of personal data relating to criminal convictions and offences referred to in Article 10 of GDPR; or
3. a systematic monitoring of a publicly accessible area on a large scale.

When the technology is developed or improved within the Tools4LEAs project the DMPs should be the primary source to evaluate if the DPIA is required under GDPR. DPIA should be prepared by technology developers in cooperation with ELSA group.

In case the DPIA is required in accordance of GDPR, it should be conducted. The template of DPIA presented in Tools4LEAs v1 project's deliverable D1.8 and updated (if necessary) can be used for DPIA evaluation, but not compulsory.

The results of DPIA should be presented to ELSA group during it's meetings.

The questionnaires regarding personal data processing were prepared for the evaluators of the tools if they provide the answer that personal data is going to be processed.

Table 1. Updated Questionnaire on personal data processing for development and testing purposes.

All the questions are only about the tool development and testing stages.

Name of the tool: [provide info]

No.	Question	Answer
1.	Will personal data be processed? Personal data – any information that makes possible identify a precise person directly or indirectly in the context of additional information. Processing – any action with personal data, including collection, deleting, anonymization and etc.	<i>If yes, please:</i> 1. list all types of personal data processed; 2. list all the personal data processing operations. 3. Companies, institutions involved in processing and their roles. 4. Provide information which companies/institutions will be controller and processor.
2.	Will you develop <u>new</u> data sets for the tool?	<i>If yes, please:</i> 1. What kind of data sets; 2. How long the data will be stored; 3. Will personal data be processed; 4. Will the data be transferred to the 3rd countries.
3.	Which <u>existing</u> data sets will you use?	<i>Please:</i> 1. Provide the list of data sets and the links to it 2. Provide information if the data sets used will contain personal data.
4.	Do the privacy and security principles apply for the tool? I. e. Does the tool was designed to observe the principles of data privacy and security.	If yes, please explain how these principles were incorporated in the tool. If not, please explain why it is not relevant and how it will be ensured by default.
5.	Are there any potential for Bias and Algorithmic Discrimination by your tool?	If yes, please describe how do you plan to address potential biases, especially in AI models used in law enforcement or high-risk scenarios

No personal data was processed during the development and testing stages of the tools, therefore, a Data Protection Impact Assessment (DPIA) is not required to be conducted. However, personal data will be processed through the following tools for law enforcement purposes: ARICA, FACECOG, PERSONAL REID, Federated Learning. This processing of personal data is carried out in accordance with national laws that implement 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 (hereinafter – LED directive).

Following the Art. 27 of LED directive the DPIA should be conducted if the processing of personal data will likely result in “a high risk to the rights and freedoms of natural persons”. The ALIGNER project delivered “The ALIGNER Fundamental Rights Impact Assessment”². We recommend to use “The ALIGNER Fundamental Rights Impact Assessment” to evaluate the level of risk to human rights and freedoms before the personal data processing operations will start.

1. Recommendations for operational DPIA of ARICA, FACECOG, PERSONAL REID, Federated Learning: DPIA Competent Law Enforcement body or related institution should conduct a thorough DPIA to identify and assess potential privacy risks and impacts associated with the tools. This assessment should consider data collection, storage, processing, and sharing practices, as well as the potential consequences for individuals' privacy.
2. Fundamental Rights Impact Assessment. As mentioned above, it is recommended to use the methodology developed by ALIGNER project. Competent Law Enforcement body or related institution should conduct it before the operational use.
3. Apply national criminal procedure regulations in a light with human rights impact assessment, ethical and social impact assessment. When applying national criminal procedure regulations, it is crucial to ensure that they are aligned with human rights principles and values. Conducting a human rights impact assessment, as well as ethical and social impact assessments, should help achieve this alignment.
4. Data Minimization: Competent Law Enforcement body or related institution should ensure that only the minimum amount of personal data necessary for the investigative purposes will be collecting and retaining. Competent Law Enforcement body or related institution should limit access to personal data to authorized individuals with a legitimate need to know. The data storage and deletion processes should ensure minimalization principle as well.
5. Anonymization and Pseudonymization: Competent Law Enforcement body or related institution should ensure that any identifying information is adequately protected and accessible only to authorized personnel.
6. Security Measures: Competent Law Enforcement body or related institution should implement robust security measures to safeguard the confidentiality, integrity, and availability of the collected data. This includes encryption, access controls, secure storage, and regular security audits.
7. Retention and Deletion Policies: Competent Law Enforcement body or related institution should establish clear retention and deletion policies to ensure that personal data is not kept for longer than necessary. Regularly review and delete data that is no longer required for the investigative purposes.
8. Accountability and Governance: Competent Law Enforcement body or related institution should designate a Data Protection Officer or privacy team responsible for overseeing the implementation of privacy measures and ensuring compliance with data protection regulations. Foster a culture of privacy and provide training to personnel involved in using the tools.
9. Regular Audits and Assessments: Competent Law Enforcement body or related institution should conduct periodic audits and assessments to evaluate the effectiveness of privacy

² <https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/>

measures and identify any areas for improvement. Stay up to date with evolving privacy regulations and adapt the tools accordingly.

2.3. Social Impact Assessments

Plan				Real				Status
What	Who	When	How	What	Who	When	How	
Social impact assessment template prepared	Authors of this document	Undefined	Undefined	Social impact assessment template prepared	Authors of this document	2024-25	ELSA Team to revise the assessment template	done

The positive social impact assessment can be attributed to the tools' contribution to the fight against cybercrime. They were specifically developed with the purpose of enhancing criminal investigations and enabling law enforcement agencies to more effectively address cybercrime issues. By providing advanced capabilities and streamlined processes for investigations, these tools have the potential to improve the efficiency and effectiveness of combating cyber threats.

On the other hand, the potential negative social impacts should also be considered and assessed. As these tools involve the processing of personal data for law enforcement purposes, there may be concerns related to privacy and data protection. It is essential to ensure that the use of these tools aligns with legal requirements and safeguards the rights and freedoms of individuals.

To fully evaluate the social impact of the operational use of these tools, a comprehensive social impact assessment should be conducted by competent law enforcement. This assessment should consider factors such as the effectiveness of the tools in combating cybercrime, the potential risks to privacy and data protection, and any broader societal implications that may arise from their implementation.

2.4. Ethics Assessments

Plan				Real				Status
What	Who	When	How	What	Who	When	How	
Ethic assessment template prepared	Authors of this document	Undefined	Undefined	Ethic assessment template	Authors of this document	2024-25	• Relate assertions/questions to different target groups • ELSA team to revise the assessment template	done

During the development and testing phases of the tools, an Ethical Impact Assessment was conducted. Since no personal data was processed and no real-life testing was performed during these phases, no ethical issues were identified at that time. However, it is important to recognize that the operational use of some of the tools will involve the processing of personal data, which could potentially impact human rights.

Countries may have varying criminal procedure laws, which can result in different levels of protection for human rights. Therefore, when applying criminal procedure regulations, it is necessary to take ethical considerations into account. This entails ensuring that the regulations align with ethical principles such as respect for autonomy, fairness, and the protection of vulnerable individuals.

In this context, it becomes important for the National Competent Law Enforcement body or related institution to carefully evaluate not only the legal requirements for the application of the tools according to national laws (such as judicial authorization, time limits, and information provided to data subjects), but also whether the national criminal procedure laws ensure the ethical use of the tools. Merely adhering to the law does not guarantee ethical use from a human rights perspective.

The lawfulness of data processing and use of the tools should be evaluated in a light the European Convention on Human Rights and case of European Court of Human Rights, not only national criminal procedures law.

To ensure ethical use of the tools, the National Competent Law Enforcement body or related institution should analyze whether the national laws adequately safeguard against potential ethical concerns. This analysis should involve assessing whether the laws provide sufficient protection for individual rights, privacy, and other relevant ethical considerations.

By conducting a comprehensive evaluation that includes both legal requirements and ethical considerations, it is possible to promote the ethical use of the tools in accordance with human rights principles. This approach helps to ensure that the operational use of the tools not only complies with the law but also upholds ethical standards, safeguarding the rights and dignity of individuals throughout the criminal procedure process.

The template for Ethics assessment was updated based on AI developments and the need to ensure Ethics compliance for AI tools.

For AI tools additionally we evaluate these aspects:

1. Impact on Human Rights and freedoms:

Does the AI system respect and protect human rights, particularly those related to criminal investigation, such as the presumption of innocence, right to a fair trial, freedom of expression, and privacy?

How does the tool ensure that it does not infringe upon the rights of individuals, particularly in high-risk law enforcement or criminal justice contexts?

What measures are in place to ensure that the AI system does not disproportionately affect marginalized or vulnerable groups?

2. Compliance with AI Act (for AI tools)

Please describe how do you ensure that AI systems are categorized according to risk levels, providing transparency, robustness, and traceability, and complying with necessary legal and ethical requirements for high-risk AI systems, especially in law enforcement contexts.

How does the AI system align with the requirements of the EU AI Act (Regulation (EU) 2024/1689), particularly in terms of risk categorization, transparency, robustness, and traceability?

Is the AI system classified as high-risk, and if so, how does it comply with the additional requirements for high-risk AI systems used in law enforcement, including the provision of transparency, accountability, and public trust?

3. GDPR and Data privacy

Please describe how personal data is handled (e.g., consent, data minimization, data protection impact assessments), storage, anonymization, and cross-border data transfers, as well as how do you ensure that data privacy principles are integrated into the tool's design and functionality.

How is personal data handled in compliance with the GDPR (General Data Protection Regulation), including data collection, consent management, data minimization, and data protection impact assessments (DPIAs)?

How is personal data stored and secured, and what protocols are in place to ensure its protection from unauthorized access or misuse?

Does the AI system process any special categories of personal data (e.g., sensitive data), and if so, how are these categories handled in compliance with GDPR provisions?

Are there any cross-border data transfers involved? If so, how are these transfers conducted in compliance with GDPR and applicable international data protection laws?

4. Ethics by design (for AI tools)

Please describe how did you embed ethical considerations from the earliest stages of AI development, ensuring that ethical issues, including bias, fairness, and privacy, are addressed proactively throughout the tool's lifecycle.

How were ethical considerations (e.g., fairness, transparency, privacy) integrated from the earliest stages of the AI system's design and development?

What steps were taken during the design and development process to prevent ethical issues, such as bias and discrimination, from arising?

How are ethical issues, including those related to data protection and fairness, continuously monitored and addressed throughout the tool's lifecycle?

5. Transparency and Accountability (for AI tools)

Please describe how will you ensure that stakeholders, including affected individuals, can understand and challenge the outcomes of the AI tool, particularly in legal and law enforcement settings.

How transparent is the AI system's decision-making process, and how is this transparency communicated to stakeholders and affected individuals?

What mechanisms are in place to ensure accountability for decisions made by the AI system, and how can these decisions be challenged or reviewed?

How are stakeholders, including affected individuals, informed about the functioning and limitations of the AI tool, and how can they participate in the decision-making process?

6. Security and Cybersecurity Measures

Please describe how the tool is designed to resist cybersecurity risks, such as unauthorized access or manipulation, ensuring data protection and the safety of sensitive law enforcement information. What security measures are implemented in the AI system to prevent unauthorized access, tampering, or misuse of personal and sensitive data?

How does the system ensure the integrity of the data it processes, especially in high-risk environments like law enforcement?

What steps are taken to protect the AI system from potential cyberattacks, and how are vulnerabilities identified and addressed throughout the system's lifecycle?

3. Summary

3.1. Conclusion

Deliverable D1.5 reports on all the ethical, legal, privacy and social impact activities conducted 2024-2025.

No personal data was processed for development and testing of the tools. Therefore, DPIA was not conducted and no social or ethical impact made. However, some of the tools will process personal data in operational implementation. Therefore, Competent Law Enforcement body or institution should conduct DPIA, Human Rights Impact Assessment, Ethical Impact Assessment and Social Impact Assessments.

Recommendations for operational use of the tools that process personal information is provided above.

By conducting these assessments, the aim is to strike a balance between effective law enforcement and safeguarding individual rights and societal well-being. It enables policymakers and stakeholders to identify any potential conflicts between the regulations and human rights, ethics, or social values.

The lawfulness of data processing and use of the tools should be evaluated in a light the European Convention on Human Rights and case of European Court of Human Rights, not only national criminal procedures law.

The outcome of DPIA, Human Rights Impact Assessment, Ethical Impact Assessment and Social Impact Assessments might be that national criminal procedure laws do not ensure adequate protection of human rights. Based on the findings of the assessments, appropriate measures can be taken to address any identified issues, modify the regulations if necessary, or introduce safeguards to protect individual rights.

3.2. Evaluation

There has been an important work conducted to setup and appropriately tackle the ethical, legal, privacy and social aspects of the project. However, there have been certain delays in in conducting the ELSA assessments. As a consequence, important lessons learned have been extracted which will serve in the future Tools4LEAs v3 project. As for example, we will send ELSA questionnaire templates with examples how the answer should look like, also will focus more on AI assessment methodology.

3.3. Future work

The ELSA related work and knowledge gained in the Tools4LEAs v2 project, reported in this deliverable, will serve as the ground, the starting point for the Tools4LEAs v3 project.

ANNEX I ELSA final audit report

[Name of the Tool / Product]

[Name of the Developer / Company]

Date of Issue: [Insert Date]

This document confirms of successful development and testing in compliance with the Ethical, Legal, and Social Aspects (ELSA) framework of the above-mentioned tool, as outlined under European human rights principles and legal requirements. The tool has been assessed to meet the necessary requirements for privacy protection, legal compliance and responsible use, ensuring alignment with the following standards:

1. **Transparency and Accountability:** Demonstrated clear and comprehensive documentation of processes and decisions.
2. **Privacy and Data Protection:** Adherence to the principles of proportionality and necessity, respecting the right to privacy as guaranteed under European human rights law.
3. **Fairness and Non-Discrimination:** Prevention of any form of bias or discrimination in its development and application.

Important notes on ELSA compliance: [provide any important notes, comments that are important to ELSA compliance, comments what aspects were evaluated and why].

Conditions for further ELSA Compliance: To maintain compliance, the tool must be utilized in accordance with the recommendations outlined in Annex A. Any deviation from these recommendations may invalidate this certification.

Issued by: EACTDA

[name, title, position]

Signature: _____

ANNEX A (of ANNEX I): Recommendations for ELSA compliant tool usage

1. Judicial Authorization

Recommendation: All decisions or actions utilizing the tool that impact individual rights must receive prior judicial authorization.

ECtHR Guidance: In *Zakharov v. Russia*, the Court emphasized the necessity of prior judicial authorization to prevent arbitrary surveillance, stating that "a system of secret surveillance... may undermine or even destroy democracy under the cloak of defending it."

What to Do: LEAs must obtain a court order before using a surveillance tool to monitor a suspect's communications or any other privacy intrusive activity that requires judicial authorization.

Example: Before deploying a wiretap on a suspect's phone, the agency submits detailed evidence to a judge explaining why the surveillance is necessary and proportionate to the investigation.

2. Data Minimization

Recommendation: Collect and process only the data necessary to achieve the intended purpose, avoiding overreach.

ECtHR Guidance: The Court has underscored the importance of data minimization, asserting that "the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life."

What to Do: Collect only the data essential to the investigation and delete any unrelated information promptly, enshrine this principle in the privacy policy or any other document that sets out the rules for personal data processing,

Example: While analyzing a suspect's financial transactions, the LEA excludes records unrelated to the crime, such as personal purchases, to limit unnecessary data retention.

3. Transparency Reports

Recommendation: Provide regular transparency reports documenting how the tool is used and its impact.

ECtHR Guidance: The Court has advocated for transparency in surveillance practices to ensure public oversight and trust.

What to Do: Publish regular reports outlining the tool's usage, ensuring accountability.

Example: The LEA issues an annual report summarizing how often the tool was used, the types of crimes investigated, and measures taken to prevent misuse.

4. Regular Audits

Recommendation: Conduct periodic audits to ensure continued compliance with privacy and human rights standards.

ECtHR Guidance: Regular audits are essential to uphold data protection standards and prevent misuse.

What to Do: Conduct periodic reviews to ensure compliance with human rights standards.

Example: An independent oversight body reviews the agency's use of surveillance tools every six months, identifying and addressing any procedural breaches.

5. Mitigation of Bias

Recommendation: Implement safeguards and perform regular evaluations to detect and address potential biases.

ECtHR Guidance: The Court has recognized the necessity of preventing discrimination and bias in data processing activities.

What to Do: Implement controls to prevent discriminatory practices or outcomes.

Example: Before deploying facial recognition technology, the LEA conducts tests to ensure the tool performs equally well across different demographics, avoiding racial or gender bias.

6. Access to Redress Mechanisms

Recommendation: Ensure that individuals affected by decisions made using the tool have access to clear and effective mechanisms for redress.

ECtHR Guidance: The Court has emphasized the right to an effective remedy for individuals whose rights have been violated.

What to Do: Provide a process for individuals to challenge decisions made using the tool.

Example: If someone suspects they were wrongfully surveyed, they can file a complaint with the LEA, which is reviewed by an independent ombudsman.

7. Training for Users

Recommendation: Provide comprehensive training for all users to understand the ethical, legal, and operational considerations for compliant tool usage.

ECtHR Guidance: Proper training ensures that those handling personal data do so in compliance with human rights standards.

What to Do: Train all officers on the legal and ethical use of tools.

Example: Officers undergo mandatory workshops on privacy laws and the ethical implications of using AI tools in investigations.

8. Safeguards for Law Enforcement Use

Recommendation: Ensure the tool is used strictly within the scope of lawful investigations and adheres to principles of proportionality and necessity.

ECtHR Guidance: In *Zakharov v. Russia*, the Court stressed that surveillance measures must be "necessary in a democratic society" and proportionate to the legitimate aims pursued.

What to Do: Limit tool usage to lawful investigations with appropriate documentation.

Example: For a cybercrime case, the LEA logs every action performed using the investigative tool, ensuring it aligns with the authorized scope.

ANNEX II User Acceptance Test Questionnaire on ELSA

ELSA Topic	Question	End User Feedback / Comments	Additional Notes (Optional)
Judicial Authorization	1. Before using the tool for activities that may impact individual rights (e.g., surveillance), would you verify that a valid court order or judicial authorization was obtained?		
	2. Did you see if there is a clear process in the tool or workflow for documenting judicial authorization prior to engaging in privacy-intrusive actions?		
	3. If you initiated a privacy-intrusive action, would you be prompted to provide or reference judicial authorization?		
Data Minimization	1. Does the tool allow you to select only the data necessary for your investigation, avoiding unrelated or excessive data collection?		
	2. Were you able to exclude or promptly delete information not relevant to the case?		
	3. Is the principle of data minimization clearly communicated in the tool's user guidelines or privacy policy?		
Transparency Reports	1. Does the tool provide you with information on how your actions are logged and reported for transparency purposes?		
	2. Are you aware of procedures for generating or contributing to regular transparency reports on tool usage?		

ELSA Topic	Question	End User Feedback / Comments	Additional Notes (Optional)
	3. Did you receive any guidance on what information should be included in transparency reports?		
Regular Audits	1. Were you informed about periodic audits or reviews of tool usage for compliance with privacy and human rights standards?		
	2. Did you have an option of receiving any notifications or reminders regarding upcoming audits or the need to maintain accurate records?		
	3. Is there a clear process for addressing audit findings or procedural breaches?		
Mitigation of Bias	1. Before using features such as facial recognition or data analytics, did the tool provide information on how bias is detected and mitigated?		
	2. Were you trained or prompted to check for potential discriminatory outcomes when using the tool?		
	3. Is there an option to report suspected bias or unfair outcomes within the tool?		
Access to Redress Mechanisms	1. Are you aware of the procedures for individuals to challenge decisions made using the tool?		
	2. Is information about redress mechanisms accessible to you and communicated to affected individuals?		

ELSA Topic	Question	End User Feedback / Comments	Additional Notes (Optional)
	3. Have you ever received or processed a complaint regarding tool usage, and if so, was the process clear and effective?		
Training for Users	1. Did you receive comprehensive training on the ethical, legal, and operational use of the tool before starting?		
	2. Were training materials or workshops provided that covered privacy laws and human rights considerations?		
	3. Do you feel adequately prepared to use the tool in compliance with ELSA requirements?		
Safeguards for Law Enforcement Use	1. Does the tool restrict usage to authorized, lawful investigations only?		
	2. Are there built-in safeguards to ensure actions are documented, necessary, and proportionate to the case?		
	3. Is there a clear audit trail for all actions performed within the tool, and are you aware of your responsibilities in maintaining it?		