A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights

D4.4: Synthesis - a collection of the best multidisciplinary practices

Grant Agreement ID	101022001	**Acronym**	popAI
Project Title	A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights		
Start Date	01/10/2021	**Duration**	24 Months
Project URL	https://www.pop-ai.eu/		
Document date	30/09/2023		
Nature	R = Document, report	**Dissemination Level**	PU = Public
Authors	Dimitra Papadaki (KEMEA), Georgia Melenikou (KEMEA), Panagiotis Douris (KEMEA), Claire Morot-Sir (ECAS)		
Contributors	All partners		
Reviewers	Evangelia Mitrou (EAB), Eleftherios Chelioudakis (SAB), Donatella Casaburo (SAB), Ezgi Eren (SAB), Philippe Puginier (SAB), Dimitris Kyriazanos, Andreas Ikonomopoulos (NCSRD)		

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 101022001.

Executive Summary

Nowadays, the advancements in the field of Artificial Intelligence (AI) as well as the number and variety of its applications keep increasing at a rapid pace. The dynamics and the impact of AI on the society and the environment necessitate the existence of harmonised legal rules that will accompany the technological developments in order to mitigate potential risks and smoothly incorporate AI-based technologies into our lives. Therefore, the role of policymakers is decisive.

At the same time, apart from the risks that are likely to emerge from new technological solutions, the benefits are also indisputable. One of the examples is the high benefits for Law Enforcement Agencies (LEAs). LEAs will start using more and more AI technologies and tools to assist them in carrying out law enforcement activities and meeting the demanding needs of their job more efficiently. Due to the position of LEAs in the society and the significant degree of power imbalance that characterises their actions, it is critical that AI applications in law enforcement are designed, developed and deployed in a way that will not only facilitate the work of LEAs but will also take into account the concerns and requests of the civil society and prioritise fundamental rights in order to be accepted and valued by all interested parties.

This deliverable receives input from previous work done as part of the popAI project and mainly from the recommendations included in the submitted deliverables of WP4. It constitutes a synthesis of the emerging best multidisciplinary practices and is addressed to LEAs, policymakers, citizens (as potentially affected persons) and technology developers with the aim to ensure the ethical use of AI in law enforcement. The recommendations have been created following a specific methodology. The opinions of LEAs, citizens, technology developers, ethics and legal experts and other interested stakeholders have been taken into consideration for the production of recommendations and for the evaluation and selection of the best multidisciplinary practices in line with the current ethical and legal framework. As a result, a White Paper in the form of a public report is delivered to the European Commission.

Table of Contents

List of Terms & Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
Charter	Charter of Fundamental Rights of the European Union
CoE	Council of Europe
Council	Council of the European Union
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EDPB	European Data Protection Board
EP	European Parliament
ESIA	Ethical and Social Impact Assessment
FRIA	Fundamental Rights Impact Assessment
FRT	Facial Recognition Technologies
GA	Grant Agreement
GDPR	General Data Protection Regulation
HRESIA	Human Rights, Ethical and Social Impact Assessment
HUDERIA	Human Rights, Democracy and the Rule of Law Impact Assessment
LEA	Law Enforcement Agency
LED	Law Enforcement Directive

Terminology

“artificial intelligence system” (AI system) means:

software that is developed with one or more of the techniques and approaches listed in Annex I (of the Draft AI Act) and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with (definition proposed by the European Commission)[1];

a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge-based approaches, and produces system-generated outputs such as content, predictions, recommendations, or decisions influencing the environments the system interacts with (definition proposed by the Council of the European Union)[2];

a machine-based system designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments (definition proposed by the European Parliament)[3].

“affected person” or **“AI subject”** means any natural person or group of persons who are subject to or otherwise affected by an AI system[4].

“citizens” or **“civil society”** means natural persons (not only EU citizens) potentially subject to or otherwise potentially affected by an AI system.

“Draft AI Act” is the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21.4.2021 COM (2021) 206 final 2021/0106 (COD) as issued by the European Commission and as it has been amended so far by the Council of Europe and the European Parliament.

“instructions for use” means the information provided by the provider to inform the deployer of an AI system’s intended purpose and proper use, as well as information on any precautions to be taken; inclusive of the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used[5].

“law enforcement” means activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security[6].

“Law Enforcement Authority or Agency (LEA)” means:

[1] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21.4.2021 COM (2021) 206 final 2021/0106 (COD)

[2] Council of Europe, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach, 25.11.2022

[3] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts

[4] Ibid.

[5] Ibid.

[6] Ibid.

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security[7].

“lifecycle” means all phases of existence of an artificial intelligence system ranging from its design and development (including sub-phases such as requirement analysis, data collection, training, testing, integration), installation, deployment, operation, maintenance, to its decommissioning[8].

“personal data” means any information relating to an identified or identifiable natural person **(“data subject”**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[9].

“policymaker” means a member of a government department, legislature, or other organisation who is responsible for making new rules, laws, policies etc. Examples include EU and national legislative bodies, mayors and municipalities.

“provider” or **“technology developer”** means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge[10].

“user” or **“deployer”** means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity[11].

[7] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21.4.2021 COM (2021) 206 final 2021/0106 (COD)

[8] Committee on Artificial Intelligence (CAI) (2023), Revised Zero Draft Framework (Convention) on Artificial Intelligence, Human Rights, Democracy and the Rule of Law; AI HLEG (2020), Assessment List for Trustworthy Artificial Intelligence (ALTAI)

[9] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

[10] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21.4.2021 COM (2021) 206 final 2021/0106 (COD)

[11] Ibid. and European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts

1 Introduction

The core vision of the popAI project is to enhance and promote trust in the application of Artificial Intelligence (AI) in the security domain. To meet its vision, the project follows a cross-disciplinary approach and aims at increased awareness, ongoing social engagement and the consolidation of diverse spheres of knowledge offering a unified European view across Law Enforcement Agencies (LEAs) and specialised knowledge outputs, including recommendations, best practices and roadmaps[12].

Due to the role and position of LEAs in the society and the significant degree of power imbalance between LEAs and citizens, it is critical that AI technologies are designed, developed and used in a way that will not only facilitate the work of LEAs but will also -most importantly- prioritise fundamental rights and foster the trust of citizens.

In that context, WP4 'The pandect of recommendations for the ethical use of AI by LEAs' is a Work Package of the popAI project that, having considered the main actors involved in the AI lifecycle and the potential impact of law enforcement AI on fundamental rights and freedoms, consists of:

- T4.1 'Recommendations for and from policymakers and LEAs', principally focused on and addressed to LEAs as deployers of AI systems and to legislators and other policymakers (relevant submitted deliverable D4.1 "White Paper for LEAs");
- T4.2 'Recommendations for and from the Civil Society', principally focused on and addressed to the persons affected by the AI applications (relevant submitted deliverable D4.2 "White Paper for Civil Society");
- T4.3 'Recommendations for and from Technology Developers', principally focused on and addressed to the providers of AI systems (relevant submitted deliverable D4.3 "White Paper for Technology Developers") and
- T4.4 'Cross-disciplinary interchange of best practices' which collects, examines and evaluates the recommendations of the previous tasks to produce the best multidisciplinary practices for the ethical use of AI in law enforcement (relevant deliverable D4.4 "Synthesis: a collection of the best multidisciplinary practices").

For more perspectives to be represented and for the outcomes to be comprehensive, all tasks followed a multi-stakeholder and multidisciplinary approach involving LEAs, policymakers, ethics and legal experts and technology developers within and outside of the popAI Consortium, as well as citizens and other interested stakeholders. All sources that were utilised for the production of recommendations have been examined and filtered on the basis of the applicable laws surrounding the design, development and use of AI systems, including also the ethical and legal framework on AI as it has been formed so far.

[12] A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights (pop AI) Grant Agreement 101022001

1.1 Purpose and Scope

Although T4.1, T4.2 and T4.3 and the respective deliverables D4.1, D4.2 and D4.3 are orientated towards different groups, they share the same purpose: to ultimately indicate what the best practices are for the ethically and legally compliant use of AI in law enforcement.

It is the role of T4.4 and of the present deliverable to collect, examine and evaluate the recommendations included in the previous work of WP4 and present the emerging best multidisciplinary practices. The emerging best practices have been filtered in order to be compliant with the existing applicable ethical and legal framework and to complement the draft EU legislation on AI (mainly the Draft AI Act) wherever vague points or gaps have been identified considering that at this stage of the popAI project the AI Act is still in progress[13].

To this end, D4.4 is addressed to four groups involved and affected during the AI lifecycle:

1) **LEAs (and entities acting on their behalf)** that are planning to deploy or have already started deploying AI systems in order to carry out activities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security,
2) **policymakers** since the dynamics and the impact of AI on the society and the environment necessitate the existence of harmonised legal rules that will establish appropriate procedures and mechanisms to smoothly incorporate AI in the society by efficiently mitigating relevant risks,
3) **citizens** that constitute the individuals affected or potentially affected by the use of AI in law enforcement and
4) **technology developers** that are designing and developing AI systems that will be used for law enforcement purposes.

In this way, LEAs will obtain an overall picture of the steps and procedures to be followed prior and during the deployment of an AI system for law enforcement purposes and will leverage this knowledge to make ethical and lawful use of AI.

2 Approach for Work Package and Relation to other Work Packages and Deliverables

WP4 is a pop-AI Work Package that, due to its nature, needs to receive input from previous work done as part of the popAI project. Specifically, the dependence of T4.4 and, consequently, of this deliverable on other WPs, Tasks and Deliverables can be briefly outlined as follows:

D4.4 receives input from:

WP1:

- D1.4 “Ethics and Gender diversity Report”
- D1.6 “Policy briefs - 1st year”

[13] For the finalisation and adoption of the AI Act, a trilogue among the Council, the European Parliament and the European Commission is required which constitutes the last phase of the negotiations before the law is passed.

WP2:

- D2.1 “Functionality taxonomy and emerging practices and trends”
- D2.2 “Legal casework taxonomy: emerging trends and scenarios”
- D2.4 “Ethical frameworks for the use of AI by LEAs”
- D2.5 “Practical ethics toolbox for the use of AI by LEAs”
- D2.6 “AI meets organisational cultures: Human-machine interaction at the police station”

WP3:

- D3.1 “Map of AI in policing innovation ecosystem and stakeholders”
- D3.3 “Citizen produced priorities and recommendations for addressing AI in the security domain”
- D3.4 “Stakeholder attitudes, priorities, and recommendations for addressing AI in the security domain in practice”
- D3.5 “Foresight Scenarios for AI in Policing”

WP4:

- D4.1 “White Paper for LEAs”
- D4.2 “White Paper for Civil Society”
- D4.3 “White Paper for Technology Developers”

D4.4 provides output to:

WP1:

- D1.7 “Policy briefs - 2nd year”

WP5:

- D5.2 “Final community building and ecosystem engagement activities plan”
- D5.6 “Communication & Dissemination plan – final”
- D5.7 “Sustainability and exploitation plan”
- D5.8 “popAI roadmaps”

3 Structure and methodology

3.1 Structure of the deliverable

The introductory part, the scope and objectives of this deliverable as well as its relation to other popAI tasks and deliverables were presented above. The rest of the deliverable is structured as follows:

Chapter 3 presents the structure of the deliverable and the methodological approach adopted for the production and delivery of multidisciplinary best practices for the ethical and lawful use of AI by LEAs, including the overall procedure followed, the guidelines and criteria set as well as the sources of information.

Chapter 4 lists and analyses the recommendations that have been produced and constitute emerging best practices for LEAs, in order to ensure that AI will be used in law enforcement in an ethically and legally compliant manner.

Chapter 5 lists and analyses the recommendations that have been produced and constitute emerging best practices for policymakers, in order to ensure that AI applications in law enforcement will be smoothly incorporated in society through legislation.

Chapter 6 lists and analyses the recommendations that have been produced and constitute emerging best practices for citizens, in order to foster civil society's acceptance and trust towards AI applications in law enforcement.

Chapter 7 lists and analyses the recommendations that have been produced and constitute emerging best practices for technology developers, in order to ensure the design and development of trustworthy AI applications.

Chapter 8 concludes the deliverable.

3.2 Methodology

The emerging best practices are of multi-stakeholder and multidisciplinary origin seeking to cover the needs and expectations of all groups of interest. In particular, the present deliverable takes advantage of the knowledge obtained from the results of WP1, the literature review of WP2, the empirical research of WP3 with the broader ecosystem, and mainly the concluding results of the other three WP4 tasks. The recommendations were enhanced and finalised by taking into consideration the opinions of ethics experts from the popAI Ethics Advisory Board (EAB), the opinions of the members of the popAI Stakeholder Advisory Board (SAB) and the results of the sibling projects ALIGNER and STARLIGHT.

The recommendations emerge from the popAI stakeholder community, involving LEAs, policymakers, civil society representatives, legal and ethics experts, technology developers (bottom-up recommendations), but also by the popAI researchers based on their background (top-down recommendations).

Objectives

The overall procedure defined, adopted, and followed towards the production and delivery of the emerging best practices is based on a methodology which seeks to achieve the following goals:

From a methodological standpoint:

- To remain compliant with the Grant Agreement (GA) and the milestones set therein.
- To follow a multi-stakeholder and multidisciplinary approach seeking to cover the needs and expectations of all groups of interest.
- To consider and include the outputs of all associated popAI tasks, deliverables, meetings, as well as the outputs from other sibling projects, and thus satisfy all the appropriate interdependencies related to the content of the present deliverable.

- To filter out the findings based on the applicable legal and ethical framework and classify them as potential recommendations.
- To cross-check the results produced within the WP4 ecosystem (D4.1 for LEAs and policymakers with D4.2 for citizens and D4.3 for technology developers), to ensure their validity from different perspectives and according to the needs of LEAs and the target groups of interest.
- To effectively capture and elicit the target groups' input and resolve potential contradictory answers / feedback received.
- To consider the feedback provided by the SAB which consists also of members from the sibling projects ALIGNER and STARLIGHT.
- To consider the feedback provided by the EAB.

From a substantial standpoint:

- To ensure that the produced results represent the needs and expectations of LEAs.
- To ensure that the produced results represent the needs and expectations of the persons affected by law enforcement AI.
- To ensure that the produced results have considered the respective ethics principles and the applicable legal framework[14], such as the principles set by the High-Level Expert Group on AI for a trustworthy AI[15], the Charter of Fundamental Rights of the European Union, the EU data protection legislation (GDPR[16], LED[17]), the current legal framework on AI (Draft AI Act, Proposal for an AI Liability Directive[18], CoE Draft Framework Convention[19]), and societal as well as environmental values and needs.
- To ensure that as many fields and cases as possible have been covered by taking into consideration the perspectives of all groups of interest.

From a dissemination standpoint:

[14] Extended presentation of the ethical and legal framework is made in popAI D4.1 "White Paper for LEAs".

[15] AI HLEG (2019), Ethics Guidelines for Trustworthy AI, available at https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai and AI HLEG (2020), Assessment List for Trustworthy Artificial Intelligence (ALTAI), available at https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

[16] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

[17] 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

[18] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final

[19] Committee on Artificial Intelligence (CAI), Consolidated Working Draft of the Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law (7 July 2023)

- To ensure that the results of this deliverable are valid, helpful and of practical use to LEAs, policymakers, citizens and providers of AI system but also to the whole ecosystem of interested stakeholders,
- To present and disseminate the produced emerging best practices appropriately so that they are informative and clear and also communicated to the targeted audiences in collaboration with D1.7 and WP5 "Dissemination, Communications and Sustainable Community Engagement".

Methodological approach

WP4 applies a combination of doctrinal and empirical research in order to answer the question of what the emerging best practices or recommendations for the ethical use of AI by LEAs would be. D4.4, in particular, makes a synthesis of the results produced in the previously submitted WP4 deliverables (D4.1, D4.2, D4.3) and concludes to the emerging best multidisciplinary practices for LEAs, policymakers, citizens and technology developers that are complementary to each other and collectively aim to the ethical use of AI in law enforcement.

The present deliverable draws the theoretical framework from WP2 'Security AI in the next 20 years: trends, practices and risks', as revised based on the latest legislative developments at European level (related to the Draft AI Act, the proposed AI Liability Directive and the CoE Draft Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law) to ensure that it stays up-to-date due to the numerous and essential latest changes in the forthcoming legal landscape. Furthermore, it makes use of the WP3 'Empirical Knowledge Collection and Management Framework' results, with a focus on the Policy Labs of Task 3.4 in which stakeholders including LEAs and policymakers, civil society representatives, ethics experts and technology developers participated[20] and on the Crowdsourcing Platform of Task 3.3 through which feedback of citizens was obtained[21]. In addition, auxiliary sources from the popAI project were utilised to enhance the recommendations, such as D1.6[22] and minutes of the popAI plenary meetings and workshops[23].

The aforementioned sources were used in order to create the initial "entries" of recommendations that fed D4.1, D4.2 and D4.3. According to these entries, the main trends were identified, and a set of recommendations, categorised according to their thematic areas, was produced. The existing and applicable ethical and legal framework was the benchmark to filter out the popAI findings, given that compliance with the ethics requirements and the applicable laws was the main criterion according to which the entries were considered as emerging best practices/recommendations or not. As for the

[20] See popAI D3.4 "Stakeholder attitudes, priorities, and recommendations for addressing AI in the security domain in practice" and D4.1 "White Paper for LEAs", Annex A

[21] See popAI D3.3 "Citizen produced priorities and recommendations for addressing AI in the security domain"and its results in the form of recommendations in popAI D4.2 "White Paper for Civil Society".

[22] popAI D1.6 "Policy briefs - 1st year"

[23] Including also the panel discussions during the "popAI Final Event", Brussels, 19 September 2023. The panels consisted, among others, of LEA representatives from the popAI Consortium, four (4) popAI SAB members (including members of STARLIGHT and ALIGNER Consortia) and the EAB Chair.

draft EU legislation on AI (e.g., Draft AI Act, CoE Draft Convention on AI, Proposal for an AI Liability Directive), it was carefully studied for us to keep up with the latest developments.

Furthermore, as an additional step to evaluate the findings, T4.1 and T4.3 questionnaires were developed under WP4 based on the WP2 and WP3 taxonomies, functionalities, and controversies. The T4.1 questionnaire was addressed to LEAs and policymakers within and out of the popAI Consortium[24], while the T4.3 questionnaire was addressed to technological partners within and out of the popAI Consortium[25] and were used in WP4 as an assistant tool, to support, update, crosscheck and evaluate the recommendations for the ethical use of AI in law enforcement. Lastly, D4.4 takes into consideration the feedback of the SAB[26] and the EAB[27] to enhance the recommendations as well as the sibling projects' (ALIGNER and STARLIGHT) relevant results, opinions and suggestions[28].

The justification behind the combination of theoretical and empirical research is based on the GA, according to which WP2 provides the theoretical framework, WP3 conducts the empirical research, while WP4 draws conclusions based on the findings of the previous WPs, in quest of best practices that will ensure the ethical use of AI in law enforcement.

Taking into account the nature of the terms "recommendations" and "emerging best practices", their purpose in the present deliverable (as in the other WP4 deliverables) is to illuminate the existing concerns around AI in law enforcement, specify the obligations of its providers and deployers, make further propositions to ensure compliance with the said obligations, complement the applicable ethical and legal framework and identify vague points or gaps in the draft AI legislation that may need

[24] popAI D4.1 "White Paper for LEAs", Annex B (template) and section 3.3 (analysis and results). The questionnaire was sent to LEAs and policymakers within and outside of the popAI Consortium. Ultimately, it was completed by police officers of the Hellenic Police (4), the University of Applied Science - Police Affairs, in short BayHfoeD, (3) and Madrid Municipal Police (1) that belong to the popAI Consortium and police officers of the Vilnius Municipal Police (2), Krakow Municipal Police (2) and Valencia Local Police (3) that are external to the popAI Consortium, as well as it was completed by the city of Turin, in short PLTO, (1) that is a member of the popAI Consortium.

[25] popAI D4.3 "White Paper for Technology Developers", Annex B (template) and section 4.2. The questionnaire was sent to technology developers within and outside of the popAI Consortium. Ultimately, it was completed by the Head of Software Development Department of Hellenic Police (1), an NGO officer of ECAS (1), a technology developer of TRI (1), a post-doc researcher and two technology developers of CERTH (3), as well as an external data scientist of TRI London (1).

[26] The opinions of the popAI SAB members and other external experts as expressed during their participation in popAI plenary meetings (including primarily.the popAI plenary meeting in Rome and the popAI Final Event in Brussels) were taken into consideration. The popAI SAB also completed a dedicated T4.4 questionnaire to provide feedback on the recommendations presented in D4.1, D4.2 and D4.3.

[27] The opinions of the EAB members as expressed during their participation in bilateral meetings, as well as popAI plenary meetings(including primarily the popAI plenary meeting in Rome and the popAI Final Event in Brussels) were taken into consideration. The EAB chair also reviewed D4.1, D4.2 and D4.3 and completed a dedicated T4.4 questionnaire to provide feedback on the recommendations presented in D4.1, D4.2 and D4.3.

[28] ALIGNER "D2.3 Policy recommendations"; ALIGNER "D5.5 First Update of the Research Roadmap for AI in Support of Law Enforcement and Policing"; ALIGNER "D5.5 First Update of the Research Roadmap for AI in Support of Law Enforcement and Policing"; ALIGNER, popAI, STARLIGHT, AP4AI projects, Joint Workshop: "Ethical and Legal Aspects of AI for Law Enforcement", January 25th and 26th 2023, CEA premises in Brussels, Press release: https://www.pop-ai.eu/wp-content/uploads/2023/02/Ethical-and-legal-aspects-of-AI-for-law-enforcement-Conclusive-Statement.pdf; 5thALIGNER Public Workshop, June 2023

revision by the EU legislator. The emerging best practices, as listed and analysed below, aim to ultimately serve as a practical guide that will help all actors involved in the AI lifecycle, and primarily LEAs, ensure the ethical use of AI in law enforcement.

Sources

The methodology can be divided into three main phases: (1) collect existing data, (2) analyse new data/input, (3) produce new recommendations and update or discard existing recommendations.

Towards the direction of those steps, outcomes from the following sources were utilised to conclude to the best multidisciplinary practices for the ethical use of AI in law enforcement:

- popAI deliverables (WP1, WP2, WP3, WP4),
- popAI T3.4 Policy Labs Draft Reports,
- popAI Consortium meetings (e.g., plenary meetings) and workshops,
- literature, bibliography,
- AI HLEG ethics guidelines on trustworthy AI,
- applicable legal framework and draft EU legislation on AI,
- ALIGNER and STARLIGHT deliverables and workshops,
- T4.1 and T4.3 questionnaires,
- EAB and SAB feedback.

4 Emerging best practices for LEAs

This chapter aims at helping LEAs benefit from AI while using AI-enabled technologies in conformity with the ethical and legal framework so that fundamental rights are prioritised and respected and trust of the affected persons is fostered.

Extended reference to our sources and the recommendations that have been produced for LEAs is made in D4.1[29]. This chapter summarises the emerging best practices and presents them in the form of guidelines.

Ethics, privacy and security by design

As a prerequisite for the ethical and lawful use of high-risk AI in law enforcement, AI systems must have been designed and developed in line with the ethical and legal framework (for more information see below chapter 7 and also popAI D4.1 section 3.1.2.3 on the obligations of providers of high-risk AI systems according to the Draft AI Act[30]).

Therefore, from the deployers' perspective:

➔ LEAs and entities acting on their behalf should have the necessary knowledge on what to ask for and what to expect by the providers before they deploy an AI system.

[29] popAI D4.1 "White Paper for LEAs", chapters 3 and 4

[30] Ibid

- ➔ LEAs and entities acting on their behalf should be properly skilled or trained in order to be able to implement human oversight and ensure effective supervision of the AI system.
- ➔ LEAs and entities acting on their behalf should be properly skilled or trained in order to be able to monitor the operation of such systems on the basis of the instructions of use, to monitor the effectiveness of robustness and cybersecurity measures and to adjust or update the implemented measures if needed.
- ➔ LEAs and entities acting on their behalf should have the contact details of the providers and without undue delay get in contact with them (as well as with the distributors and the competent national supervisory authorities) when they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk or in cases of a serious incident or malfunctioning and interrupt or suspend the use of the system.

AI literacy

To the extent deployers exercise control over a high-risk AI system, they shall ensure that the natural persons assigned to ensure human oversight of the high-risk AI systems are competent, properly qualified and trained, and have the necessary resources in order to ensure the effective supervision of the AI system[31].

Important steps to achieve this goal are the following:

- ➔ LEAs and entities acting on their behalf should have ethical and legal education and training, i.e., participate in educational programmes (webinars, seminars and workshops, written guidelines) and training/skilling/reskilling courses, either organised by or indicated for LEAs, aiming to offer theoretical and practical knowledge on the ethical and legal considerations and risks that may derive from the use of AI by LEAs (e.g., on fundamental rights, on admissibility of evidence at court), the ethical rules, the applicable legal framework and the obligations, limitations and prohibitions stipulated by law and, soon, on issues clarified, revised and regulated through case law.
- ➔ LEAs and entities acting on their behalf should have technical education and training, i.e., participate in educational programmes (webinars, seminars and workshops, written guidelines) and training/skilling/reskilling courses, either organised by or indicated for LEAs, aiming to offer theoretical and practical technical knowledge on AI algorithms and best practices for data collection, data preparation and model training in general and specifically with respect to the deployment of a specific AI system by LEAs. In the latter case, the training courses should provide information about that AI system's purposes and technicalities including its capabilities and limitations of performance, predetermined changes, human oversight measures, potential bias, accuracy metrics, expected lifetime along with any necessary maintenance and care measures.

[31] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Article 29 par.1a(ii)

- ➔ Such educational and training programmes should take place both before and during the use of an AI system on a regular basis depending on the gaps and needs identified in each deployer's police department, the potential modification of an AI system in use or of its purpose, the introduction of new AI systems in a police department, or the pace of the AI advancements and of the legislative and case-law developments.

- ➔ For all aspects to be covered, the educators and trainers need to have different backgrounds and act collaboratively, i.e., ethics and legal experts and policymakers, technology developers, representatives of the civil society, LEAs (also from different police departments)[32].

- ➔ The educational and training programmes could be first provided to dedicated police officers that will be responsible to train later officers of their department based on a "train-the-trainers" scheme[33].

- ➔ At EU level, AI educational and training programmes could be coordinated by competent widely recognised EU Agencies[34]. EU handbooks on the use of AI in law enforcement would be highly beneficial[35]. Also, highly recommended is the participation of LEAs in EU-funded research projects that aim to the design and development of AI systems planned to be used in law enforcement.

- ➔ At national level, educational and training programmes on AI could be an initiative of LEAs in collaboration with the national competent authorities (e.g., ministries). The addition of relevant courses to the police academies' curriculum for the preparation of future police officers is also strongly recommended.

- ➔ Proposed example is the popAI Ethics Toolbox for the use of AI by LEAs. It is part of the objective of the popAI project for the creation of an EU AI innovation hub for LEAs and the broader community and consists of educational videos on AI and ethics, technology ethics briefs and interactive visualisation of AI and LEAs ethics taxonomies[36].

Impact assessments

Risks related to AI systems can result not only from the way such systems are designed, but also from the way such AI systems are used. Therefore, deployers of high-risk AI systems play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the providers during the AI development phase. To this end, in order to effectively ensure that

[32] Representatives of other law enforcement agencies that are using AI could provide their valuable insights and share their experience on the procedures that they are following in order to implement and be in line with the AI Act.

[33] SAB feedback received through the T4.4 questionnaire.

[34] Such as the European Union Agency for Law Enforcement Training (CEPOL) or the European Agency for Fundamental Rights (FRA).

[35] E.g., European Agency for Fundamental Rights, 'Preventing unlawful profiling today and in the future: a guide' (2018) available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

[36] For more information about the Ethics Toolbox see popAI D2.5 "Practical ethics toolbox for the use of AI by LEAs" and for more information about the EU AI Innovation hub see popAI D5.7 "Sustainability and exploitation plan".

fundamental rights are protected, the deployers of high-risk AI systems should conduct a fundamental rights impact assessment prior to putting such systems into use[37].

Important remarks for LEAs to conduct a thorough impact assessment are the following:

- ➔ The fundamental rights impact assessment (FRIA) should include a detailed plan describing the measures or tools that will help minimising the relevant risks identified at the latest from the time of putting the high-risk AI systems into use, otherwise the deployers should refrain from their utilisation[38].
- ➔ When performing a FRIA, the LEAs or entities acting on their behalf should notify the national supervisory authority and, to the best extent possible, relevant stakeholders as well as representatives of groups of persons likely to be affected by the AI systems in order to collect relevant necessary information[39].
- ➔ The summary of the FRIA should be made publicly available on the LEA's official website[40].
- ➔ Where applicable, LEAs shall use the information provided under Article 13 of the AI Act[41] to comply with their obligation to carry out a data protection impact assessment (DPIA) under Article 27 of Directive (EU) 2016/680 or Article 35 of Regulation (EU) 2016/679[42].
- ➔ The process of impact assessment and evaluation needs to include an ethical and social impact assessment (ESIA) in order to ensure that the affected persons' opinions, including their expectations, fears or objections are taken into account.
- ➔ All types of impact assessments must be reviewed on a regular basis and updated whenever needed (e.g., when something new is added to the AI system, or the initially intended purpose changes).
- ➔ Carrying out impact assessments by LEAs is highly recommended even in cases where this is not obligatory by law.

[37] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Recital 58a and Article 29a

[38] Ibid.

[39] Ibid.

[40] Ibid.

[41] Article 13 is about transparency and provision of information by the providers to the users of AI systems.

[42] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21.4.2021, Article 29 par.6; The EP also added the following to the said Article "[…] a summary of which (i.e., DPIA) shall be published, having regard to the specific use and the specific context in which the AI system is intended to operate. Deployers may revert in part to those data protection impact assessments for fulfilling some of the obligations set out in this article, insofar as the data protection impact assessment fulfils those obligations".

- ➔ Proposed templates are the ALIGNER FRIA[43] that is specifically prepared for and exclusively addressed to LEAs, HUDERIA[44] and HRESIA[45].

Inclusion of the civil society

Trustworthy AI means that the AI systems are designed and developed in a way that makes them understood, accepted and valued by the users and the affected persons as well as that they are used in a way that makes them understood, accepted and valued by the affected persons. Especially, in the case of law enforcement, the LEA actions that involve certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter. Therefore, stronger effort is required to achieve citizens' understanding and acceptance, mitigate their concerns and foster their trust towards law enforcement AI.

Important steps to this direction are the following:

- ➔ Equality, diversity and non-discrimination must be prioritised by including all members of the civil society and, most importantly, vulnerable individuals or groups affected by AI by also ensuring proper gender and age balance.
- ➔ Information including, at least, the AI systems being used (and, ideally, also systems planned to be used, e.g., at the procurement stage) in law enforcement, their purposes and expected outcomes should be provided by LEAs or entities acting on their behalf to the potentially affected persons.
- ➔ Information including, at least, the datasets used, the way in which the AI outcomes are produced and the role of LEAs in decision-making should be provided by LEAs or entities acting on their behalf to the affected persons to prove that proper human oversight is implemented, no discrimination or stigmatisation is made against them and their rights to presumption of innocence, defence, fair trial, effective remedy and personal data protection are not violated.
- ➔ Information about the rights of the AI subjects according to the AI Act along with contact details of a contact person or description of a mechanism that enables them to exercise their rights should be provided to the affected persons.
- ➔ Feedback mechanisms should be established in order to collect input on how to improve the AI system directly from those potentially affected thereby[46].

[43] https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/

[44] HUDERIA template included in The Alan Turing Institute, Human Rights, Democracy, and the Rule of Law Assurance Framework for AI Systems: A proposal prepared for the Council of Europe's Ad hoc Committee on Artificial Intelligence, available at https://rm.coe.int/huderaf-coe-final-1-2752-6741-5300-v-1/1680a3f688, p.247-271

[45] A. Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment', available at https://www.sciencedirect.com/science/article/pii/S0267364918302012

[46] Ad Hoc Committee on Artificial Intelligence (CAHAI), Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law, 3 December 2021, p.12 https://rm.coe.int/cahai-2021-09rev-elements/1680a6d90d

- ➔ Accountability and redress mechanisms should be established to support the AI subjects when they use existing legal avenues to seek resolution in case of misuse or harm caused by an AI system. It is also worth pointing out that cooperation with the national competent authorities[47] should be sought in order to remedy the infringement and mitigate its possible adverse effects to the biggest extent possible.
- ➔ Awareness raising and transparency tactics may vary depending on who needs to provide the information (e.g., provider, deployer), what are the most common means of communications which citizens are familiar with and what the target audience is.
- ➔ Some examples of awareness-raising tactics are:
  - organisation of events (physical, online or hybrid) to engage AI subjects in an open dialogue,
  - visits and talks at schools or universities to also involve young people,
  - creation of educational videos and campaigns.
- ➔ Some examples of tactics for building transparency and fostering public trust are:
  - Drafting protocols and codes of conduct governing the use of AI tools in law enforcement and making them publicly available through the official website of the LEA. Among others, procedures that ensure accountability such as keeping records of processing activities, logging, annual reporting, conducting impact assessments, prior consultations with supervisory authorities, establishment of internal whistleblowing mechanisms for reporting misconduct should be part of the protocols and codes of conduct governing the use of AI by LEAs[48].
  - Using a public register and/or the official website of the LEA to inform citizens about the AI systems being used in law enforcement, their main characteristics, intended purposes and expected outcomes.
  - Conducting a FRIA prior to the deployment (or public procurement) of an AI system by LEAs and prior to any changes made to that system or to its purposes and making it publicly available through a public register and/or the official website of the LEA.
  - Conducting an ESIA prior to the deployment (or public procurement) of an AI system by LEAs and prior to any changes made to that system or to its purposes to actively involve citizens in the impact assessment process.
  - Establishing communication channels, feedback mechanisms and redress mechanisms to inform the AI subjects about their rights according to the AI Act and enable them to interact with LEAs, provide feedback, ask questions, express concerns, raise objections about the use of AI tools and to exercise their rights according to the AI Act.

[47] Article 59 of the Draft AI Act stipulates the requirement of each Member State to designate a national supervisory authority responsible to ensure the application and implementation of the AI Act.

[48] SAB feedback received through the T4.4 questionnaire.

Establishment of multidisciplinary teams

To understand new disruptive technologies, their functioning, benefits, risks, and impact on society and the environment and to achieve the ethical and secure design, development and deployment of trustworthy AI, the active participation of persons with different backgrounds is imperative. Therefore, for the realisation of all aforementioned emerging best practices it is highly recommended to adopt a multidisciplinary approach during the entire lifecycle of AI through the establishment of a multidisciplinary and diverse team of people that have knowledge and expertise on AI-enabled technologies, ethics and law and care for inclusion, diversity and social benefit.

Important features and activities of such teams are the following:

- ➔ The recommended multidisciplinary team could have the form of a dedicated AI body/committee/department within each LEA.
- ➔ The team needs to be composed of LEAs, independent ethics and legal experts and technology developers that will exclusively deal with the use of AI-based technologies in law enforcement.
- ➔ Prior to and during the deployment of AI systems for law enforcement purposes, the team will have regular meetings to examine and constantly monitor the functioning of AI, its value and impact in the context of real cases.
- ➔ The team will draft protocols and codes of conduct governing the use of AI in law enforcement as well as periodical reports that include information on the number and types of AI systems used, their purposes, their expected outcomes and the actual outcomes of their use.
- ➔ The team will provide consultation to LEAs on AI matters and organise educational and training courses to police officers on the responsible use of AI by LEAs.
- ➔ The team will be responsible for conducting impact assessments (FRIA and ESIA) prior to the procurement or deployment of an AI system for law enforcement purposes. It will also review and update the impact assessments whenever changes to the system or to its purposes occur.
- ➔ The team will closely collaborate with the Data Protection Officer (DPO) designated within the LEA to ensure higher levels of conformity of the AI systems with the key requirement of data protection and governance and to co-draft DPIAs if so required or indicated according to Article 27 LED.
- ➔ The team will inform the affected persons about their rights according to the AI Act (incl. their right to explanation) and interact with the affected persons via established communication channels, feedback and redress mechanisms to enable them to exercise their rights. It will also be responsible for handling the AI-related information in the public register and/or the official website of the LEA[49].

[49] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Recital 58a. See also a relevant reference in the Ad Hoc Committee on Artificial Intelligence (CAHAI), Possible elements of a legal framework on artificial intelligence,

- ➔ The team will be in close cooperation with the national supervisory authority stipulated in Article 59 of the Draft AI Act (following the example of the GDPR and the role of the DPO[50]).
- ➔ Proposed example is this of the popAI Policy Labs that have been established as part of T3.4 of the popAI project. Extended information about the structure of the Policy Labs, the meetings, the discussions and the key outcomes can be found in D3.4[51] and D4.1[52].

5 Emerging best practices for policymakers

This chapter aims at helping policymakers ensure that AI will be deployed responsibly by LEAs as well as it will be smoothly incorporated in society. The emerging best practices for policymakers mainly depend on the findings of D4.1, D4.2 and D4.3. Considering that at this stage of the popAI project the finalisation of the EU legislation on AI is in progress, most of the proposed emerging best practices aim to complement mainly the Draft AI Act wherever vague points or gaps have been identified.

Extended reference to our sources and the recommendations that have been produced for policymakers is made in D4.1[53]. This chapter summarises the emerging best practices and presents them in the form of guidelines.

Introductory remarks about the need for harmonisation

The harmonisation of laws regulating AI, primarily at EU level, is critical to avoid fragmentation and different levels of minimum protection to citizens at national level.

- ➔ **Level of harmonisation:** On the one hand, the EU legislator should leave as little space as possible to the national legislator, while only limited and clearly specified derogations should be envisaged. On the other hand, attention should be paid to the preservation of and respect to Member States' national identity and cultural heritage as well as to the different levels of AI technological development and use among Member States.
- ➔ **Relationship of law and technology:** The EU legislator needs to have great knowledge of the available state-of-the-art technology and its capabilities, while constantly monitoring the technological changes. Since AI systems seek optimality, the conditions on which the systems will be improved and/or updated and necessary limitations or restrictions should be defined by law in advance, especially as regards AI applications in law enforcement, by always following a human-rights oriented approach in accordance with the Charter. Furthermore, it is highly recommended that the EU legislator uses terminology or wording which allows for a

based on the Council of Europe's standards on human rights, democracy and the rule of law, 3 December 2021, p.12: "The CAHAI considers that the establishment of public registers listing AI systems used in the public sector, containing essential information about the system such as, its purpose, actors involved in its development and deployment, basic information about the model, and performance metrics, where appropriate, and the result of a HUDERIA, should be addressed in the context of a legally binding or non-legally binding instrument on AI in the public sector"

[50] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Article 39

[51] popAI "D3.4 Stakeholder attitudes, priorities, and recommendations for addressing AI in the security domain in practice"

[52] popAI D4.1 "White Paper for LEAs", Annex A

[53] popAI D4.1 "White Paper for LEAs", chapters 3 and 5

level of flexibility and adaptability to the technological advancements, in order to cover existing and future cases to the extent that they do not compromise the notion of legal certainty.

- **Complementary legal acts:** Legislative acts (delegated acts, implementing acts) and non-legislative acts (recommendations, opinions, resolutions) need to be issued by competent EU institutions in complementarity to the AI Act for specific obligations, procedures or measures stipulated in the AI Act to be further defined and clarified and for conditions to be set that ensure that EU laws are applied uniformly. Handbooks and guidelines need to be issued by competent EU Agencies (such as the AI Office) or other EU bodies (such as the EDPB for personal data-related aspects of AI) for guidance to be provided on matters related to the implementation of the AI Act. This is of high importance especially in the absence of relevant case law at this early stage. Wherever below we are referring to the "establishment of procedures", this could be also carried out in the form of complementary acts issued by the EU institutions or other competent EU Agencies and bodies to support the AI Act.
- **Data protection:** The EU regulatory framework on AI shall be complementary to the data protection legislation, with due respect to obligations stemming from GDPR and LED and shall not undermine the level of privacy and personal data protection as guaranteed by the Charter. Emphasis needs to be put on the protection of special categories of personal data to prevent discrimination and stigmatisation of the AI subjects. Furthermore, along with FRIAs, DPIAs must be conducted by LEAs using AI systems that involve processing of personal data that may result in high risks to the rights and freedoms of the AI subjects/data subjects[54] and appropriate safeguards including both technological and organisational measures must be implemented to minimise the risks. Therefore, it is strongly recommended that the relevant newly added by the EP Recitals and provisions[55] are retained by the EU legislator in the final AI Act.

Recommendations on the Draft AI Act

In this section the revision of some vague points and gaps that have been identified in the Draft AI Act is proposed. In the same spirit, some procedures need to be expressly and concretely established and even standardised in order to ensure that AI will be responsibly used by the deployers in full respect of fundamental rights.

- **AI subjects' rights**: Most of the provisions relating to the rights of the AI subjects constitute new additions made by the EP. The relevant provisions can be found scattered in the Draft AI Act[56]. It is strongly recommended that the additions are retained and that the rights are listed

[54] According to Article 27 LED or Article 35 GDPR.

[55] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Recitals 2a, 2b, 45a, Article 29 par.6, Article 29a par.6

[56] Right to an explanation (Recital 84b, Article 68c), right to object against the application of AI systems (Article 52 par.1), right to seek judicial redress against decisions taken by or harm caused by AI systems (Article 52 par.1), right to lodge a complaint with a national supervisory authority (Article 68a), right to an effective judicial remedy against a legally binding decision of a national supervisory authority concerning them (Recital 84a, Article 68b), right to lodge a complaint against the providers or deployers of AI systems (Recital 84a)

collectively in a dedicated section of the AI Act (a) for the affected persons to have a clear view and the exercise of their rights to be facilitated and (b) for the providers and deployers to have a clear view of their obligations.

- ➔ **Transparency obligation:** According to the Draft AI Act, as regards the transparency obligation of the deployers (that consequently enables the AI subjects to exercise their right to object against the application of AI systems to the AI subjects and to seek judicial redress against decisions taken by or harm caused by AI systems, including their right to seek an explanation), this shall not apply to AI authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence[57]. It is strongly recommended a broader field of application (applicable also to LEAs), considering the severity of the potential harm caused to the AI subjects by AI systems used in law enforcement. Such a transparency obligation of LEAs could be limited[58]; however, an explicit complete exemption would justifiably raise major concerns and doubts in civil society. The AI subjects' rights to an explanation and to seek judicial redress should be respected at all costs.

- ➔ **AI literacy:** The requirement of AI literacy was added by the EP through its proposed amendments to the Draft AI Act. It is strongly recommended that after the trilogue the EU legislator retains this requirement in the final AI Act and also expressly defines what a "sufficient level of AI literacy"[59] is by also establishing specific training and reskilling procedures in order for all actors involved in the AI lifecycle to be equally prepared and compliant with their obligations.
- ➔ **Fundamental Rights Impact Assessment:** According to the amendments to the Draft AI Act proposed by the EP, it is mandatory that a FRIA is conducted by deployers of high-risk AI systems prior to putting such systems into use. It is strongly recommended that the EU legislator retains this obligation in the final AI Act and also encourages deployers to conduct a FRIA even in cases where this is not mandatory by law.

  Other significant recommendations to the EU legislator related to the FRIA procedure are as follows:

  - **FRIA template:** It is of high importance for the deployers that the legislator provides them with a standard template[60]. In this way, all deployers of high-risk AI systems will

[57] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Article 52 par.1

[58] Limitations to the AI subjects' rights and freedoms should be allowed as long as they are prescribed by law, respect the essence of the rights or freedoms, are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others in accordance with the Charter and by analogy with the LED.

[59] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Article 4d par.1

[60] Recently, a relevant appeal was launched by the VUB Brussels Privacy Hub. The appeal has surpassed 110 signatures among distinguished academics who have signed up. For more information see:

be equally prepared and compliant with their obligations. Furthermore, considering the role of LEAs in society and the severity of potential adverse impact of AI systems used by LEAs on fundamental rights and freedoms, a standard template of a FRIA specifically for the use of AI by LEAs is also highly recommended[61].

- **Ethical and Social Impact Assessment:** To actively involve the potentially affected persons in the process, be informed of their expectations, as well as any concerns and objections, it is strongly recommended that the FRIA template either includes or is accompanied by an ESIA.
- **FRIA and availability to the public:** The EP added that deployers of high-risk AI systems are encouraged to make the summary of their fundamental rights impact assessment publicly available on their website. The use of the word "encourage" does not indicate obligation, hence, it leaves space for derogations and consequent infringement of the requirements for transparency and accountability towards the AI subjects. It is strongly recommended that the EU legislator emphasises on the obligation of the FRIA's summary to be made publicly available. Whether this will be done via the official website of the public authority or via a public register is something that also needs to be clarified.
- **FRIA by the providers:** Based on the addition made by the EP, the obligation to conduct a FRIA is addressed only to deployers of high-risk systems. Considering the crucial role of the providers of such systems and their obligation to create trustworthy AI, it is highly recommended that a FRIA (including an ESIA) is carried out by the providers prior to the design and development of high-risk AI systems.

➔ **Feedback and redress mechanisms:** To enable the AI subjects to exercise their rights, the development and establishment of an easy-to-follow, yet well-defined procedure is highly recommended. In this way, the AI subjects will be able to communicate with the deployers, provide feedback and object against unjust decisions made by the AI system.

➔ **Procurement:** The procurement stage is one of the most critical phases for public authorities (incl. LEAs) to select an AI system by assessing its suitability to achieve the intended purposes. At that time, prior to an AI system's deployment, it is important to seek social acceptance. Therefore, a relevant reference in the AI Act to this stage of the AI lifecycle as well as the establishment of a procedure with necessary steps to be taken before and during the procurement of AI systems are recommended[62]. Those steps should include the mandatory conducting by the public authority, ideally in collaboration with the provider, of a fundamental rights impact assessment in case of high-risk AI systems by also assessing the

https://brusselsprivacyhub.com/2023/09/12/brussels-privacy-hub-and-other-academic-institutions-ask-to-approve-a-fundamental-rights-impact-assessment-in-the-eu-artificial-intelligence-act/

[61] See above in chapter 5 the ALIGNER FRIA that has been exclusively prepared for LEAs deploying AI systems for law enforcement purposes.

[62] See for example the EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 1.0 (12 May 2022), p.29-33 https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf, p.29

social impact through the involvement of the potentially affected persons (e.g., FRIA and ESIA)[63]. Prior to the deployment, the FRIA should be reviewed and updated in case of changes.

- ➔ **Multidisciplinary teams:** Elaborating upon the principle of human oversight, close to a human-over-the-loop approach, the active collaboration between LEAs, ethics and legal experts, policymakers, technology developers and civil society representatives, throughout the AI lifecycle, from its design and development to its testing, validation, implementation, and improvement is proposed. This can be achieved through the requirement for establishment of dedicated multidisciplinary bodies/committees/departments within the provider or the deployer (for more details see above the relevant emerging best practice addressed to LEAs).
- ➔ **Oversight EU bodies:** The EP added specific provisions about the establishment of an independent oversight body at EU level, namely the AI Office (or, in case this is not sufficient, of an AI Agency) to ensure an efficient and harmonised implementation of the AI Act and to achieve a high level of trustworthiness and protection of fundamental rights. Stakeholders should formally participate in the work of the AI Office through an advisory forum that should ensure varied and balanced stakeholder representation and should advise the AI Office on AI-related matters[64]. Therefore, it is strongly recommended that the relevant provisions are retained by the EU legislator in the final AI Act. Moreover, it is suggested that such an oversight body actively involves through its advisory forum, amongst other stakeholders, civil society representatives including representatives of vulnerable groups.
- ➔ **Explicit agreement of the AI subjects as an additional safeguard:** As stipulated in the LED, consent cannot itself constitute a legal ground for processing of personal data by competent authorities[65]. However, in certain cases of a particularly intrusive processing of personal data as in Recitals 35 and 37 LED, Member States could stipulate by national law the explicit agreement of the data subject not as a legal basis for the processing but as an additional safeguard to the processing. By analogy, the additional safeguard of requesting the explicit agreement of the AI subject could also be provided for in the AI Act and national laws supplementing the AI Act. In any case, this should be the exemption, as the explicit agreement of the AI subject may not be considered to be freely given.

The risk-based approach followed by the EU legislator can be considered a safeguard per se since some AI practices of particularly intrusive nature have already been prohibited in the Draft AI Act due to the unacceptable risks that they are posing to the rights and freedoms of the affected persons.

[63] See also the initiative taken by the City of Amsterdam developing a set of contractual clauses for the procurement of AI to create a framework for the information that suppliers need to provide about the used algorithms to ensure transparency and consequently citizens' trust in these services: AI Procurement, Develop EU standard contractual clauses for the procurement of ethical AI https://living-in.eu/groups/solutions/ai-procurement

[64] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Recital 76

[65] 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, Recitals 35,37

- ➔ **Protection of children:** When AI systems are deployed for law enforcement purposes, special attention shall be paid to whether the affected persons are adults or children. The providers of high-risk AI systems shall consider whether such systems are likely to adversely impact vulnerable groups of people or children[66]. In the same spirit, it needs to be highlighted by law that also the deployers of high-risk AI systems, especially if they are LEAs, shall pay special attention to this issue and take all necessary measures to mitigate any risks posed to childrens' rights prior to the deployment of an AI system.
- ➔ **Administrative penalties:** The law should set the strictest standards possible for public authorities (incl. LEAs) when they deploy AI technologies considering their role in society and the power imbalance between them and the affected persons. Member States' discretion to regulate the amount of the penalties for AI Regulation's infringement raises some concerns, as it enables national legislators to be less strict towards the public sector's infringements, such as infringements by LEAs. For that reason, it is recommended that the AI Act also sets the respective minimum limits for administrative penalties on public authorities.
- ➔ **Certification Bodies and mechanisms:** Certification bodies and mechanisms should be established to ensure that the AI system and related software planning to be used by LEAs are designed and developed in compliance with the applicable legal, ethical and security requirements.

Other proposed practices

Since the use of AI applications in law enforcement is still at a very early and therefore immature stage, the following practices are also recommended:

- ➔ **EU funding:** Additional funding is necessary for the LEAs to cope with the extra efforts required for the use of AI. To this end, it is recommended that the EU and the Member States provide dedicated financial resources to LEAs and competent authorities responsible for their supervision for their technological upgrade, especially considering that the Member States do not share the same level of technology development in the field of AI, as well as for reaching a sufficient level of AI literacy (through regular education and training). Furthermore, dedicated financial resources need to be provided for research and development, taking also into account the importance of regulatory sandboxes for the development of trustworthy AI and the need for LEAs to familiarise themselves with AI systems in controlled environments prior to their deployment in the real environment.
- ➔ **EU cooperation among stakeholders:** Exchanging lessons learnt and knowledge across the LEAs and the broader community of interested stakeholders is also of high importance. The establishment of a platform to interchange best practices, encouraging the usage of ethical and secure-by-design AI tools has been provided in popAI in the so-called AI Hub[67]. The AI Hub is a platform that gathers in one place the findings of the popAI project and can be updated to include future results under a continuous learning approach model. Such a platform or similar procedure could be established to support cooperation among Member States' LEAs and the broader community.

[66] Ibid., Article 9 par.8

[67] popAI D5.7 "Sustainability and exploitation plan"

6 Emerging best practices for citizens

This chapter is addressed to civil society and summarises the emerging best practices relating to the ethical use of AI by LEAs which, among others, necessitates the inclusion of citizens (affected persons) in the AI lifecycle (see also relevant sections in chapters 4, 5 and 7). It needs to be clarified that, the preposition "for" is not used to express that the recommendations are restrictively addressed to the civil society given that in certain cases the State, or the competent authorities (including the policymakers or LEAs) should be responsible for their implementation, but that they have an informative character and are formulated to serve the citizens' interests as interpreted by representatives of the civil society and NGOs, citizens and the rest of the stakeholders who participated in the popAI research activities. Therefore, this chapter provides for a citizen-centric point of view regarding the ethical use of AI by LEAs, but is addressed to *all readers* regardless of their background.

Extended reference to our sources and the recommendations that have been produced for civil society is made in D4.2[68].

Education and training[69]

- ➔ The need for accessible education, to increase citizens' understanding of AI tools, their benefits and risks when deployed by LEAs, under the general AI literacy notion, is urgent. Similarly, as stipulated by the EP in the draft Amendments to the AIA Proposal, Member States and all relevant stakeholders shall promote a sufficient level of AI literacy in all sectors of society[70].
- ➔ Citizens with relatively low engagement with or access to technology or relatively low technology literacy should also be able to have access to education regarding the use of AI by LEAs.

Academic Research[71]

- ➔ Academic research regarding, among others, the purpose, the justification, the narratives, and the social impact of AI used by LEAs should be encouraged. Conducting research in the field would provide a deeper understanding of the issues related to the use of AI by LEAs and even pose new questions within the concept of academic freedom.
- ➔ It is highly recommended that the research findings are available to the public, so that they can further serve as a basis for collective reflection towards the introduction of AI for law enforcement purposes.

[68] popAI D4.2 "White Paper for Civil Society"

[69] Ibid., SAB feedback received through the T4.4 questionnaire

[70] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Article 4d par.1

[71] popAI D4.2 "White Paper for Civil Society"

Awareness-raising[72]

- ➔ Educational campaigns to inform and draw the attention of citizens to the benefits and risks of AI systems including their potential impact on fundamental rights should be conducted.
- ➔ Particular focus shall be paid to raising awareness towards sensitive issues, such as the processing of personal data via AI systems for purposes of biometric identification.
- ➔ Further on, information about potential unlawful interference with the citizens' rights, would prerequire the provision of information on their existing rights and guidance on how to exercise them in clear and concrete steps.
- ➔ Such campaigns could be governmental or non-governmental.

Communication with the AI subjects[73]

- ➔ **General information to be made available to the public:**

  In general, information about the introduction of an AI system, the purposes for which it is going to be used, its necessity, its specifications, capabilities, limitations, drawbacks and safeguards implemented by the LEAs should be communicated or made available to the potentially affected community. Information regarding the design of AI systems to be deployed, including the adoption of an ethics-by-design approach, shall also be part of the information package. Specific emphasis shall be paid to the provision of such information to the citizens, regarding tools which can be potentially used for biometric identification, if and to the extent it is not prohibited by law. The potential for unlawful interference with the citizens' fundamental rights and freedoms shall also be disclosed to them in a simple and understandable language, regardless of the level of their technological literacy. The above information could be provided for instance via the regular publication of reports by the competent national authorities (LEAs and their supervisory Ministries or other), in public registries or in their website. It is suggested that such information shall be provided via official channels of the competent authorities, and additionally independent/non-governmental ones for reasons of pluralism[74].

- ➔ **Information to be provided to the AI subject:**

  Further on, information (by the AI system itself, by the provider/ or by the LEAs) should be provided to the person(s) exposed to or affected by an AI system used for law enforcement purposes, that they are subject to it, and additionally, about its purpose, the humans responsible for making the decision, the decision-making process, the adherence to the ALTAI principles and about their rights. [75] Limitations to the AI subjects' rights and freedoms, should be allowed as long as they are prescribed by law, respect the essence of the rights or

[72] popAI D4.2 "White Paper for Civil Society"; D4.1 "White Paper for LEAs"

[73] popAI D4.2 "White Paper for Civil Society"; D4.1 "White Paper for LEAs"; popAI D4.3 White Paper for Technology Developers"; SAB feedback received through the T4.4 questionnaire

[74] popAI D4.3 "White Paper for Technology Developers"

[75] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Article 52 par.1
This suggests a broader field of application of Article 52 par.1, however without prejudice to legitimate limitations to the AI subjects rights

freedoms, are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others in accordance with the Charter and by analogy with the LED[76]. Such information could be provided to the AI subject, automatically via electronic means, among others.

Information regarding personal data processing provided by the LEAs[77]

In accordance with the applicable data protection framework, Member States shall provide by law for the LEAs as data controllers, to make available a minimum amount of information to the data subjects as in Article 13 (1) LED[78].

In accordance with Article 13 (2) LED, Member States shall also provide by law that, in specific cases,[79] LEAs ensure that, in addition to the above information, further information[80] is given to the data subjects, in the sense that it reaches the data subject and is not published in a website,[81] in order to facilitate the exercise of their rights. That would be the case for example, if personal data is collected without the knowledge of the data subject, when the decision-making is conducted solely based on facial recognition technologies, when personal data is further processed within an international criminal cooperation procedure or in the case of personal data processing under covert operations as stipulated in national law[82].

➔ Not exclusively but especially as regards the provision of information under LED 13(2) to the data subjects in "specific cases", it is recommended that, among others, a procedure is in place to **automatically** via electronic means provide the information as required by law to the data subjects, and that the data subjects can similarly directly review the details, request further information in order to exercise their rights, or exercise their rights towards the data controller via the Supervisory Authority when applicable. This would be of particular importance in cases of usage of biometric identification tools by LEAs,[83] which has been

[76] Charter of Fundamental Rights of the European Union, Article 52 - Scope and interpretation; LED CHAPTER III Rights of the data subject

[77] popAI D4.2 "White Paper for Civil Society"

[78]LED, Article 13 par.1 "(a) the identity and the contact details of the controller; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended; (d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority; (e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject."

[79] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 1.0 Adopted on 12 May 2022, para 86-87

[80] LED, Article 13 par.2: "(a) the legal basis for the processing; (b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period (c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations; (d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject".

[81] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 1.0 Adopted on 12 May 2022, para 88

[82] Ibid. par. 86-87

[83] One of the citizen-centric concerns raised during popAI research activities was the processing of social media users' personal data found online for biometric identification by LEAs. When assessing whether processing of special categories of personal data is allowed as relating to data which are manifestly made public by the data subject, it is clarified that, for informative to the citizens purposes, that according to the EDPB Guidelines on the use of FRT in the area of law enforcement:

identified as an issue of concern for citizens during popAI research activities, if and to the extent they are not prohibited.

- ➔ As LEAs, under Article 13 (2) a LED shall disclose the legal basis for processing, a good practice would be that not only they refer to the respective LED provision, but also to the national legislative provision allowing the personal data processing[84].

Explicit agreement as an additional safeguard under Recital 35 and 37 LED[85]

As stipulated by LED, consent cannot itself constitute a legal ground for processing of personal data by competent authorities.[86] This shall not inhibit Member States from providing by law, that the data subject may, in addition to the existing legal basis, explicitly agree to the processing of their personal data, in cases of DNA tests in criminal investigations or the monitoring of their location with electronic tags for the execution of criminal penalties.[87] Similarly, processing of particularly sensitive in nature, data, in relation to fundamental rights and freedoms, should be allowed by law when the data subject has, additionally to the legal basis authorising the data processing, explicitly agreed to it[88].

- ➔ In certain cases of a particularly intrusive processing of personal data as in Recitals 35 and 37 LED, Member States could provide by law for the explicit agreement of the data subject, not as a legal basis for the processing, but as an additional safeguard to the processing. By analogy, in specified and limited cases of particularly intrusive technologies, the additional (to the legal basis authorising the usage of such technologies) safeguard of requesting the explicit agreement of the AI subject, could also be provided for in the AI Act and national laws.
- ➔ In any case, the explicit agreement of the AI subject may not be considered to be freely given due to the power imbalance between the parties. Resorting to the additional request of an explicit agreement should therefore be the exception. It is therefore suggested that the EU legislator retains an AI framework on certain prohibited AI practices taking into account the interests of the affected persons.

- ● A photograph itself is not considered to be falling under the category of biometric data;
- ● The photograph being manifestly made public by the data subject does not imply that the associated biometric data which can be potentially extracted via technical means, have been made public as well;
- ● The data subject must have explicitly made freely accessible and public via an open source the biometric data and not a facial image, so as biometric data to be considered as manifestly made public by them;
- ● In the case of social networks images, the EDPB considers that the data subject not choosing specific privacy features, or the case of absence of choice due to default settings, does not mean that the data subject's data are manifestly made public and can be further processed for biometric identification.

In addition, as envisioned in Recital 26 (b) of the latest AIA Draft Amendments: "The indiscriminate and untargeted scraping of biometric data from social media or CCTV footage to create or expand facial recognition databases add to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy. The use of AI systems with this intended purpose should therefore be prohibited."

[84] SAB feedback received through the T4.4 questionnaire.

[85] popAI D4.2 "White Paper for Civil Society"

[86] LED Recital 35,37

[87] LED Recital 35

[88] LED Recital 37

Inclusion, involvement and participation of the Civil Society[89]

The civil society in general and the affected persons specifically, could make good use of the following mechanisms and initiatives:

➔ **Feedback and Redress Mechanisms**[90]

The establishment of the following mechanisms, as introduced in previous chapters, could be essential for the affected communities and persons to provide their feedback and exercise their right to redress as AI subjects:

- The establishment of an easy-to-follow, yet well-defined procedure (for example via, among others, an online platform) to receive and incorporate evaluation comments of the people potentially affected by the AI system should be a valuable tool in the hands of the civil society for direct communication with the LEAs and indirectly with other stakeholders (for instance with technology developers/providers when they are communicating a technical issue) and vice versa.
- The establishment of a user-friendly redress mechanism (for example via, among others, an online platform, in cooperation with the national competent authorities) which would enable citizens to lodge a complaint against AI-assisted decisions, would be of paramount importance for the AI subjects in order to exercise their right to an effective remedy.

➔ **Involvement of the civil society in the Impact Assessment procedures**[91]

- The concerns and expectations of the affected persons should be expressed through their inclusion and participation in the impact assessment procedure[92]. More information regarding the impact assessment procedure is provided in the relevant section of chapter 4 of the present deliverable.

➔ **Participation of the civil society in collective movements**[93]

- Overall, the participation of citizens in collective movements, such as grassroot organizations, Civil Society Organisations and trade unions, is an important step towards amplifying their voices, holding authorities accountable, and advocating for responsible, transparent, and just use of AI tools in LEAs practices.
- The civil society could, in addition to initiatives of the national competent authorities, provide for guidance and concrete steps towards the AI subjects as regards the exercise of their rights.

[89] popAI D4.1 “White Paper for LEAs”, popAI D4.2 “White Paper for Civil Society”, popAI D4.3 “White Paper for Technology Developers”

[90] popAI D4.1 “White Paper for LEAs”, popAI D4.2 “White Paper for Civil Society”, popAI D4.3 “White Paper for Technology Developers”

[91] popAI D4.1 “White Paper for LEAs”, popAI D4.2 “White Paper for Civil Society”

[92] VUB, Brussels Privacy Hub, Sep 12 23 News, available at : https://brusselsprivacyhub.com/2023/09/12/brussels-privacy-hub-and-other-academic-institutions-ask-to-approve-a-fundamental-rights-impact-assessment-in-the-eu-artificial-intelligence-act/

[93] SAB feedback received through the T4.4 questionnaire.

7 Emerging best practices for technology developers

This chapter is addressed to providers of AI systems that will be used in law enforcement. For LEAs to be able to use an AI system in an ethically and legally compliant manner, it must be first ensured and demonstrated by the providers of such systems that they are trustworthy, i.e. that they have been designed and developed in full respect of fundamental human rights and in compliance with the applicable ethical and legal framework.

Extended reference to the recommendations that have been produced for technology developers is made in D4.3[94]. This chapter indicatively refers to certain emerging best practices and presents them in the form of guidelines. It is clarified herein that this is an indicative and non-exhaustive list.

Definition of the intended purpose of the AI system [95]

The intended purpose for which the AI system is designed should be clearly defined and detailed from the design stage. This would entail that:

- ➔ The problem along with the solution to which the AI system is intended to assist shall be defined from the outset.
- ➔ The specific law enforcement purpose (s) and functionalities, the context and conditions under which the AI system is designed should be defined from the outset.

Ethics-by-design: ethics self-assessment [96]

As a requirement for the ethical use of AI in law enforcement, AI systems ought to have been designed and developed in line with the ethical framework, as prescribed by the ALTAI principles. To build technologies that are ethical by design, the designer and developer team *should*:

- ➔ Integrate ethical principles to the very foundation of the AI system.
- ➔ Identify ethical issues and address ethical considerations from the outset; embed safeguards and mitigation measures, and monitor compliance throughout the entire development lifecycle.
- ➔ Implement checkpoints to ensure that every step is compliant with the applicable ethics framework.

Ethical and legal training and awareness-raising for technology developers[97]

- ➔ Under the general AI literacy notion, it is strongly recommended that the designers/ developers of AI systems receive training regarding ethical and lawful AI.

[94] popAI D4.3 “White Paper for Technology Developers”

[95] popAI D4.1 “White Paper for LEAs”, popAI D4.2 “White Paper for Civil Society”, popAI D4.3 “White Paper for Technology Developers"

[96] popAI D4.1 “White Paper for LEAs”, popAI D4.2 “White Paper for Civil Society”, popAI D4.3 “White Paper for Technology Developers"

[97] popAI D4.1 “White Paper for LEAs”

Cooperation among stakeholders [98]

- ➔ The establishment of multidisciplinary teams, in the design and development stage, consisting of people with technical, legal and ethical background should be promoted.
- ➔ In addition, the inclusion of users and affected persons and, namely, law enforcement officers and representatives of the civil society in the design and development of ethical AI for LEAs is strongly suggested, as below.

Human-centric design: inclusion of LEAs and citizens in the design stage

- ➔ **Involvement of LEAs**: The LEAs should be included throughout the design stages, via collecting the user requirements (needs, preferences, capabilities) and translating them into technical specifications.
- ➔ **Involvement of citizens:** The potentially affected community's feedback shall be also taken into consideration when designing AI systems to ensure the solutions provided are socially acceptable.

Data protection by design and by default: deliberate choice of technical and organisational measures [99]

The implementation of data protection principles (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability) via technological means must be ensured[100]. To this end, technical and organisational measures must be in place from the design stage to allow for lawful data processing activities.

- ➔ As regards technical measures, a deliberate choice between anonymisation, pseudonymisation, encryption or processing of raw personal data shall be made. That depends, among others, on the purpose and context of the processing, which in the current case, would be related with law enforcement purposes and competencies.
- ➔ When data anonymisation or pseudonymisation is preferable but not feasible, there shall be a justification, explaining why it was not possible to ensure data anonymisation and how privacy for the data subjects is safeguarded or how limitations are justified in a democratic society.
- ➔ The exact methods and techniques applied towards achieving anonymisation or pseudonymisation or implementing other technical measures should be documented.

[98] popAI D4.1 "White Paper for LEAs", popAI D4.2 "White Paper for Civil Society", popAI D4.3 "White Paper for Technology Developers"

[99] Ibid, SAB feedback received through the T4.4 questionnaire.

[100] GDPR Article 25, LED Article 20

Diversity, non-discrimination and fairness by design: inclusion, thresholds and checks[101]

It is possible that the AI system, tool and related product (to be) developed could potentially reinforce bias or discrimination against individuals or groups of individuals based on their protected characteristics. As prescribed by the ALTAI principles, this must be avoided.

Suggested steps towards the realisation of this scope include:

- ➔ The involvement of people who may be potentially adversely affected based on their protected characteristics is recommended to ensure that their needs and experiences are considered in the design phase, resulting in more inclusive and effective solutions.
- ➔ Certain statistical limits could be hardcoded into the algorithm as thresholds, monitored throughout the evolution of the algorithm and checked against previously or latterly generated results. When such thresholds are reached, then checks, reviews and audits of data and the algorithm against bias shall take place.

Risk management by design: Impact Assessments[102]

Planning the implementation and continuous update of a risk management system throughout the whole lifecycle of the AI systems, tools and related products is required for high-risk AI systems, according to the latest AIA draft**[103]**. The foreseen risk management system includes, among others, the following components: the identification, estimation, and evaluation of the known and reasonably foreseeable risks to health, safety, fundamental rights, democracy, the rule of law and the environment based on the intended purpose of the AI system; the involvement of experts and external stakeholders, when relevant; the evaluation of the impact on the groups affected with a strong emphasis on vulnerable groups or children; the outline of concrete and adequate mitigation measures or justification for any limitations[104]. Therefore, the following should be considered:

- ➔ The quest for the identification, assessment and mitigation of the AI systems' impact on potentially affected persons, their fundamental rights, on society, democracy and the environment, but also the human-centric design proposed previously, with the inclusion of users' and affected groups' needs and concerns, calls for the performance of a holistic impact assessment, before the development stage. In cases where the AI systems may pose risks to fundamental rights, it is suggested that a fundamental human rights impact assessment is performed prior to the development of such an AI system.[105] Such an impact assessment could also include an ethics and societal impact assessment (ESIA), to ensure that the affected

[101] popAI D4.3 "White Paper for Technology Developers", popAI D1.4 "Ethics and Gender diversity Report"

[102] popAI D4.1 "White Paper for LEAs", popAI D4.2 "White Paper for Civil Society", popAI D4.3 "White Paper for Technology Developers"

[103]European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Recital 42,43

[104] Ibid, Recitals 42,43 , Article 9

[105]See also: AI High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 8 April 2019, page 15

persons' feedback is taken into account. This can be achieved through the public consultation to take place in the context of algorithmic impact assessment, as proposed in the Draft Convention on AI by the Council of Europe. In this sense, the HRESIA (Human Rights, Ethical and Social Impact Assessment) and the SIA (Social Impact Assessment) models are of great value as self-assessment tools which take into consideration the public participation and have an interest in societal core values[106].

- ➔ The above should be performed without prejudice to the obligations set by law for conducting a DPIA[107].

Development of AI systems in sandboxes prior to operational use by LEAs [108]

The establishment of regulatory sandboxes, and specifically at least one national regulatory AI sandbox per Member State, is prescribed by the Draft AI Act,[109] so that development, testing and validation of innovative AI systems is conducted under oversight before these systems are put into the market or into service.

- ➔ The development of AI to be used for law enforcement purposes, in controlled and protected environments prior to putting the products in operational use by LEAs, is encouraged.
- ➔ The developers could progressively expose these systems to real-world conditions, so as to approach the actual conditions in the operational environments of interest.
- ➔ Examples of such sandboxes could be testing innovative AI systems under national or European research programmes.

Human oversight: control and monitoring mechanisms models in cooperation with LEAs

According to the ALTAI principles, human oversight of the AI systems shall be ensured.

- ➔ The inclusion of control and monitoring mechanisms should be planned from the design phase. The decision over a human-in-the-loop (HITL), human-on-the-loop (HOTL), or human-in-command (HIC) model in cooperation with the LEAs who are going to deploy it, is recommended. There is a suggestion for strong control and oversight mechanisms.
- ➔ The modification of control and monitoring mechanisms (additions, removals, replacements, modifications) in communication with the LEAs, is suggested.

[106] popAI D4.2 "White Paper for Civil Society"; Elsevier, Computer Law & Security Review, Volume 34, Issue 4, August 2018, Pages 754-772, Alessandro Mantelero, AI and Big Data: A blueprint for a human rights, social and ethical impact assessment

[107] GDPR Article 35 , LED Article 27

[108] popAI D4.1 "White Paper for LEAs", popAI D4.2 "White Paper for Civil Society", popAI D4.3 "White Paper for Technology Developers"

[109] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Recital 71

Reporting of events capabilities in accordance with the applicable for LEAs

- ➔ It is advised that the AI systems to be used by LEAs possess reporting of events (error codes, signals, warnings, alerts) capabilities in line with the reporting procedures of the LEAs. This may refer, among others, to the format of the reports and the persons to which they are addressed. As part of the procedure, the following should be also considered:
  - In principle, the LEAs need to report their findings to their chain of command.
  - For any evidence to be admissible before a court of law, specific conditions set by the applicable laws must be met.

AI system explainability regarding outcomes via the indication to the LEAs of key parameters

According to the ALTAI principles, the AI system's explainability regarding, among others, its outcomes needs to be guaranteed.

- ➔ It is essential that the system can indicate the key parameters used, regarding a specific result / outcome. The LEAs should be aware of the values of the key parameters, so that they can be aware of how the system outputs specific results. Moreover, even if it is not easy to correlate the outputs / results with the specific inputs, this can be done or found later, as long as the values of the parameters of interest have been stored, together with the values of the associated outputs / results. Therefore, the need for logging and storing a number of important parameter values, in general, is also recommended.

Provision of point of contact details and their assigned responsibilities by the provider to the LEAs

- ➔ Under the principle of transparency and communication, the provider of an AI system should provide to the LEAs the name and contact details of the point of contact, along with the technical aspect for which they are responsible, so that the LEAs can contact / consult them if necessary.

Instructions and restrictions to be made available by the provider to the LEAs

- ➔ Instructions regarding the use of the AI system, tool and related product along with information on the risks, limitations and restrictions regarding its use should be made available by the provider to the LEAs with the support of associated documents.

Information, Feedback and Redress Mechanisms[110]

- ➔ Information mechanisms to enable the LEAs to comply with their transparency obligations should be established, via-among others- technical means.

[110] popAI D4.1 "White Paper for LEAs"

- ➔ Feedback mechanisms should be established via -among others- technical means in order to collect input on how to improve the AI system directly from those potentially affected thereby.
- ➔ Redress mechanisms should be established via -among others- technical means which would enable citizens to lodge a complaint against AI-assisted decisions and have access to an effective remedy.

Certification of the AI system with regards to safety and security, ethics and compliance with the applicable laws [111]

- ➔ Provided that the respective certification bodies and mechanisms are in place, the AI system and related software (to be) used by LEAs should be certified with respect to their technical characteristics in relation to security, safety, ethics, and compliance with the applicable laws.

Other proposed practices

More recommendations regarding the design and development of AI systems to be used by LEAs with a focus on **logging actions, authorised access to LEAs, frequent technical support and backups, audits, checks and reviews** of the AI systems internally but also by **independent third parties** are presented in more detail in D4.3.

[111] Ibid

8 Conclusions

Considering that the advancements in the field of AI as well as the number and variety of its applications keep increasing at a rapid pace and that it can be foreseen that LEAs will start deploying more and more AI applications to assist them in carrying out law enforcement activities and meeting the demanding needs of their job, it has to be ensured that AI systems will be used in law enforcement in a way that will not only facilitate the work of LEAs but will also prioritise fundamental rights and foster the trust of citizens.

The present deliverable collected, examined and evaluated the recommendations included in the previous work of WP4, namely deliverables D4.1, D4.2 and D4.3. The recommended practices were addressed to four groups involved and affected during the AI lifecycle: LEAs (and entities acting on their behalf) as deployers of high-risk AI systems (D4.1), policymakers as the ones responsible for smoothly incorporating AI in the society through legal rules (D4.1), citizens as potential AI subjects (D4.2) and technology developers as the ones responsible for providing trustworthy AI systems (D4.3).

On that basis, the emerging best multidisciplinary practices were selected and presented in this deliverable in the form of guidelines. Although the emerging best practices are addressed to different groups, they share the same purpose: to ensure that the use of AI applications in law enforcement will take place in an ethically and legally compliant manner after having taken into consideration the opinions, needs and expectations of all groups of interest.

Through D4.4, we aim to give LEAs an overall picture of the steps and procedures that either need or must be followed prior and during the deployment of an AI system and to provide them guidance and assistance in order to responsibly deploy AI-enabled technologies and tools for law enforcement purposes by prioritising fundamental rights and fostering the trust of civil society.

9 References

A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights (pop AI) Grant Agreement 101022001

A. Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment', available at: https://www.sciencedirect.com/science/article/pii/S0267364918302012

Ad Hoc Committee on Artificial Intelligence (CAHAI), Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law, 3 December 2021, available at: https://rm.coe.int/cahai-2021-09rev-elements/1680a6d90d

AI HLEG (2019), Ethics Guidelines for Trustworthy AI, available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

AI HLEG (2020), Assessment List for Trustworthy Artificial Intelligence (ALTAI), available at: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

ALIGNER "D2.3 Policy recommendations"

ALIGNER "D5.5 First Update of the Research Roadmap for AI in Support of Law Enforcement and Policing"

ALIGNER Fifth (5th) Public Workshop, June 2023

ALIGNER FRIA available at : https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/

ALIGNER, popAI, STARLIGHT, AP4AI projects, Joint Workshop: "Ethical and Legal Aspects of AI for Law Enforcement", January 25th and 26th 2023, CEA premises in Brussels, Press release: https://www.pop-ai.eu/wp-content/uploads/2023/02/Ethical-and-legal-aspects-of-AI-for-law-enforcement-Conclusive-Statement.pdf

City of Amsterdam, AI Procurement: Develop EU standard contractual clauses for the procurement of ethical AI available at: https://living-in.eu/groups/solutions/ai-procurement

Committee on Artificial Intelligence (CAI) (2023), Revised Zero Draft Framework (Convention) on Artificial Intelligence, Human Rights, Democracy and the Rule of Law

Committee on Artificial Intelligence (CAI), Consolidated Working Draft of the Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law (7 July 2023)

Council of Europe, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach, 25.11.2022

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.

EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 1.0 (12 May 2022), available at: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

European Agency for Fundamental Rights, 'Preventing unlawful profiling today and in the future: a guide' (2018) available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21.4.2021 COM (2021) 206 final 2021/0106 (COD)

European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts

popAI D1.6 “Policy briefs - 1st year”

popAI D2.5 “Practical ethics toolbox for the use of AI by LEAs”

popAI D3.3 “Citizen produced priorities and recommendations for addressing AI in the security domain”

popAI D3.4 “Stakeholder attitudes, priorities, and recommendations for addressing AI in the security domain in practice”

popAI D4.1 “White Paper for LEAs”

popAI D4.2 “White Paper for Civil Society”

popAI D4.3 White Paper for Technology Developers”

popAI D5.7 “Sustainability and exploitation plan”

popAI Final Event, Brussels, 19 September 2023

Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final

SAB feedback, T4.4 Questionnaire answers

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

The Alan Turing Institute, Human Rights, Democracy, and the Rule of Law Assurance Framework for AI Systems: A proposal prepared for the Council of Europe’s Ad hoc Committee on Artificial Intelligence, available at https://rm.coe.int/huderaf-coe-final-1-2752-6741-5300-v-1/1680a3f688

VUB Brussels Privacy Hub, Appeal , Sep 12 23 News, available at : https://brusselsprivacyhub.com/2023/09/12/brussels-privacy-hub-and-other-academic-institutions-ask-to-approve-a-fundamental-rights-impact-assessment-in-the-eu-artificial-intelligence-act/