ALIGNER

ALIGNER D2.5

Policy Recommendations:

Final Iteration, September 30th 2024

Deliverable No.	D2.5
Work Package	WP2
Dissemination Level	PU
Author(s)	Lindsay Clutterbuck (CBRNE)
Co-Author(s)	-
Contributor(s)	Donatella Casaburo (KUL)
Due date	2024-09-30
Actual submission date	2024-09-29
Status	Final
Revision	1.0
Reviewed by (if applicable)	Daniel Lückerath (Fraunhofer)

This document has been prepared in the framework of the European project ALIGNER – Artificial Intelligence Roadmap for Policing and Law Enforcement. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101020574.

Contact:

info@aligner-h2020.eu
www.aligner-h2020.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no. 101020574.

Executive Summary

"A technological singularity is a point where our old models must be discarded

and a new reality rules"[1]

Whether the recent technological development in AI systems becomes accepted or not as a "*technological singularity*" remains to be seen, but at this stage and from the perspective of policing and law enforcement in the European Union, a point has been reached where "*our old models must be discarded and a new reality rules*". This has now become a certainty for P&LEAs. It is driven not only by the rapid increase of AI systems in the public domain and the problematic uses to which they can now be put, but also by another direct consequence of the arrival of AI systems; the passage into law of the EU Artificial Intelligence Act.

Since the commencement of Project ALIGNER, AI systems in general have dramatically changed from being viewed as a frontier technology of most interest to its exponents, to being almost universally accessible to people globally through their computers and increasingly, their mobile phones. In the context of policing and law enforcement, this combination of technological innovation and the capabilities it brings has additionally led to a rapidly advancing wave of their malicious use and the creation of new crime and security threats. The irony of this is that it has in turn, contributed to the demand for P&LEAs to improve their own effectiveness and to do so by incorporating the capabilities of AI systems into their day-to-day operations.

The overall aim of Project ALIGNER (*'Artificial Intelligence Roadmap for Policing and Law Enforcement'*) was the *"...[bringing] together of European actors concerned with Artificial Intelligence (AI), Law Enforcement and Policing to collectively identify and discuss needs for paving the way for a more secure Europe in which Artificial Intelligence supports LEAs while simultaneously empowering, benefiting and protecting the public.*"

As one element in achieving this aim, a requirement was set for ALIGNER to create "*policy recommendations tailored to the operational needs of the law enforcement sector…supported by identified capability gaps…[and] provide an overview of them from a societal and ethical perspective".*

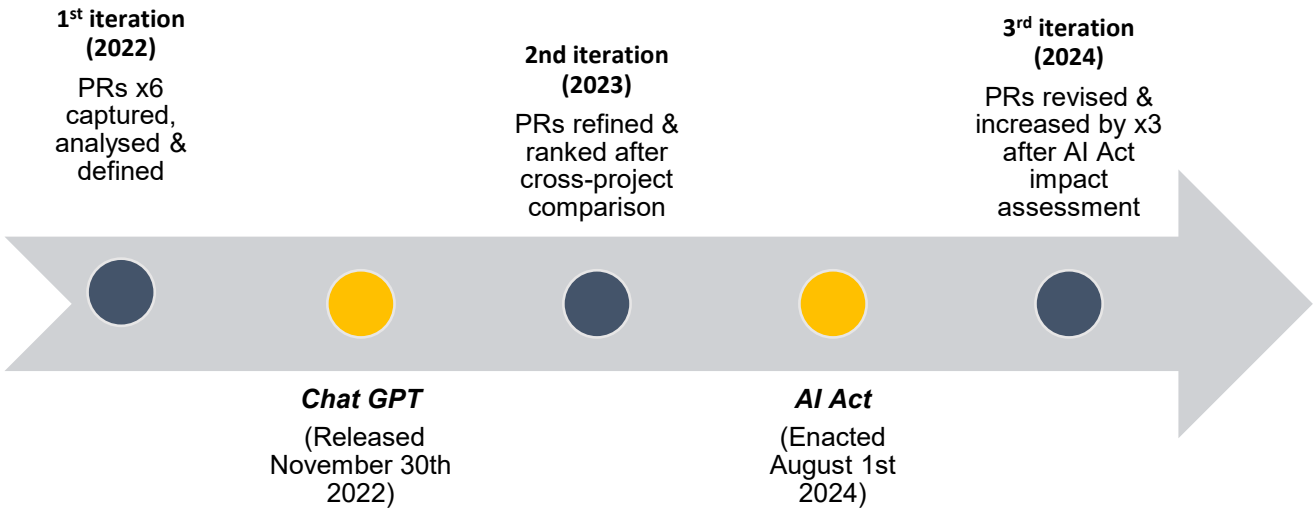
This document briefly describes how the ALIGNER policy recommendations were derived during the first year of the project and were published as Deliverable D2.3 in September 2022. In year two, they were then compared to assess their congruence with the policy recommendations put forward by two 'sister projects' from the Security Union (SU) AI Cluster (PopAI and STARLIGHT), plus another external set of policy recommendations from ENISA. They were then revised and ranked in priority order before being published as Deliverable D2.4 in September 2023.

During the final year of the project, the ALIGNER policy recommendations were again examined, this time to determine the impact on them of the Artificial Intelligence Act (AI Act) that ultimately came into force as EU legislation on August 1st 2024. For almost the entire three-year timescale of project ALIGNER, the proposed legislation had been in a process of internal debate and negotiation (and therefore subject to uncertainty and constant change), before the final version was arrived at and set the numerous prohibitions, obligations and requirements that EU P&LEAs must comply with.

[1] Vernor Vinge, Mathematician, Computer scientist & Science-fiction author (1944-2024)

The timing of the production of the three iterations of the ALIGNER policy recommendations and their relationship to two crucial real-world events mentioned above that occurred during the lifetime of the project are shown below in Figure 1.

Figure 1 – Chronology of the three Project ALIGNER policy recommendation iterations and two key external events



After a brief summary of the process employed by ALIGNER to develop its policy recommendations in years one and two, this latest and final iteration of the policy recommendations commences with an overview of the provisions of the AI Act that are of most relevance to EU P&LEAs. It then examines aspects of the Act that would seem likely to impact on each of the six ALIGNER policy recommendations as they stood by September 2023 in their second iteration. During work for the AI Act impact assessment, the need become apparent for three new ALIGNER policy recommendations to be formulated and these are presented here, along with an accompanying rationale and suggestions for implementation for each one. All nine of the final iteration of the ALIGNER policy recommendations are shown below:

Table 12 – The final set of the ALIGNER Policy Recommendations

ALIGNER POLICY RECOMMENDATIONS: FINAL ITERATION
ALIGNER - New Policy Recommendation (1) **(Created post-AI Act impact assessment, September 2024)**
The EU Commission, through its European Artificial Intelligence Office, should establish a constructive partnership with EU police and law enforcement agencies to ensure that compliance issues can be prevented or resolved, guidance and best practices can be identified, and lessons can be learned
ALIGNER - New Policy Recommendation (2) **(Created post-AI Act impact assessment, September 2024)**
The Artificial Intelligence Office should work with DG HOME and Europol to ensure that the meaning of the phrase in Article 5 referring to "a genuine and present or foreseeable threat of a terrorist attack" is clarified
ALIGNER - New Policy Recommendation (3) **(Created post-AI Act impact assessment, September 2024)**
The Artificial Intelligence Office should ensure the EU Database for High-Risk AI Systems established by Chapter VIII, Article 71 as a central pool of information containing details of the deployers of these AI systems can be utilized by EU P&LEAs, including who they can contact to discuss their experiences of its procurement, operations and other matters of mutual interest
ALIGNER: Policy Recommendation 1 **(Final iteration after AI Act impact assessment, September 2024)**
By utilising the provisions and requirements of the AI Act, the AI Office and DG HOME to ensure that the procurement, utilisation or in-service development of AI systems by P&LEAs is carried out in a consistent way that takes full account of their obligations towards fundamental human rights
ALIGNER: Policy Recommendation 2 **(Final iteration after AI Act impact assessment, September 2024)**
Building on the foundation of the AI Act, the European Commission should continue to develop its' legislative framework for AI systems so that the P&LEAs of Member States can utilise it to guide and support their selection, acquisition and use of AI systems
ALIGNER: Policy Recommendation 3 **(Final iteration after AI Act impact assessment, September 2024)**

The EU should guide and support the P&LEAs of Member States to incorporate into their technology base the lawful and appropriate AI systems that are currently available or are already foreseeable on the near horizon

ALIGNER: Policy Recommendation 4

(Final iteration after AI Act impact assessment, September 2024)

The EU to instigate a review of the EU data protection framework as it relates to the nexus between 'real-world' data and P&LEA functions and operations and their potential use of AI systems to access and process it. Currently, aspects of it are perceived as a potential barrier to the procurement and use of AI systems by P&LEAs

ALIGNER: Policy Recommendation 5

(Final iteration after AI Act impact assessment, September 2024)

DG HOME to work in conjunction with Europol and CEPOL to embed into EU police and law enforcement training and learning the concepts of 'AI Literacy' and a 'human-centric approach' to AI systems (Article 4 and Article 1 of the AI Act) and including their impacts, consequences and implications for P&LEAs

ALIGNER: Policy Recommendation 6

(Final iteration after AI Act impact assessment, September 2024)

To urge the EU to conduct and facilitate systematic and regular research into AI systems, both as solutions and as threats, that are tailored to the needs of P&LEAs and can be delivered within realistic timeframes

Table of Contents

List of Acronyms and Abbreviations

Abbreviation	Meaning
AI	Artificial Intelligence
ALIGNER	*'Artificial Intelligence Roadmap for Policing and Law Enforcement'*
CEPOL	European Agency for Law Enforcement Training
ENISA	European Union Agency for Cybersecurity
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulations
GPT	Generative Pretrained Transformer
GPAI	General Purpose Artificial Intelligence (a.k.a. 'Generative AI')
KPI	Key Performance Indicator
LEAAB	Law Enforcement Agency Advisory Board (ALIGNER)
LLM	Large Language Model
ML	Machine Learning
P&LEA	Police and Law Enforcement Agencies
popAI	*European Positive Approach towards Artificial Intelligence tools in support of Law Enforcement & Safeguarding Privacy & Fundamental Human Rights*
SIEAB	Scientific, Industrial and Ethical Advisory Board (ALIGNER)
SO	Specific Objective
STARLIGHT	*Enhancing the EU's strategic autonomy in field of Artificial Intelligence for LEAs*
SU	Security Union
WP	Work Package

1. Introduction

Project ALIGNER commenced in October 2021 and finished at the end of September, 2024. Its overall aim was to *"...[bring] together European actors concerned with Artificial Intelligence (AI), Law Enforcement and Policing to collectively identify and discuss needs for paving the way for a more secure Europe in which Artificial Intelligence supports LEAs while simultaneously empowering, benefiting and protecting the public.*"

To achieve this aim, ALIGNER was set a number of Specific Objectives (SO) and two of them related specifically to its policy recommendations. They were required to be *"…tailored to the operational needs of the law enforcement sector…supported by [identified] capability gaps…[and] provide an overview of them from a societal and ethical perspective".* They were to be set out in three sequential deliverables, one in each year of the project and entitled "*Policy Recommendations*" (D2.3, D2.4 and D2.5).[2] Other aspects of the ALIGNER policy recommendations were to be incorporated as necessary into a series of ALIGNER deliverables entitled "*Research roadmap for AI in support of law enforcement and policing*" (with D5.8 being its final iteration in September 2024).

Shortly after its instigation, ALIGNER began to operate as part of a cluster of projects related to varying aspects of AI system technology in the policing and law enforcement environment, known as the EC Security Union (SU) AI Cluster. It consisted mainly of collaboration and cooperation between ALIGNER and two other 'sister projects':

- ***PopAI*** *- European Positive Approach towards Artificial Intelligence tools in support of Law Enforcement & Safeguarding Privacy & Fundamental Human Rights*
- ***STARLIGHT*** *- Enhancing the EU's strategic autonomy in field of Artificial Intelligence for LEAs*

Project ALIGNER was conceived and commenced in a very different world to that of today and in particular, two key events relevant to AI systems in the context of policing and law enforcement occurred in the two years since ALIGNER published its initial policy recommendations at the end of September 2022. In terms of events and developments, there are two categories.

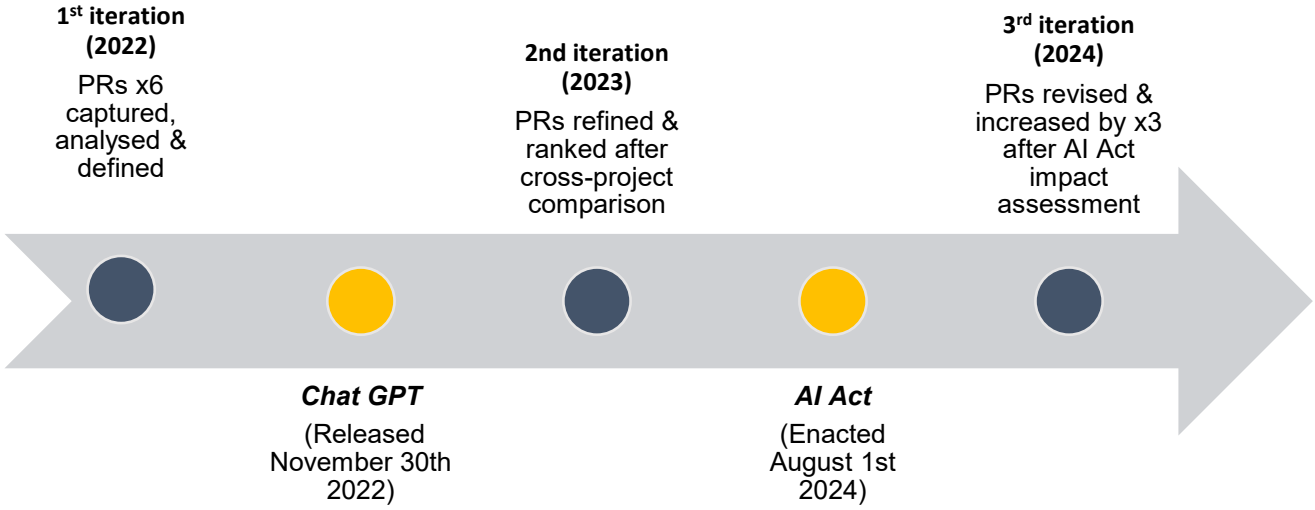
The first one concerned the process of turning the EU Proposal for an Artificial Intelligence Act into EU-wide law. Over this timescale, police and law enforcement agencies (P&LEAs) could only watch its glacier-like progress towards the statute book, knowing that there were many contentious issues that needed to be resolved between the Proposal of the European Commission, the 'general approach' to it of the Council of the EU and the 'negotiating position' of the European Parliament. As in all legislation in the field of criminal law, exact words and meanings matter and it was not until the AI Act became law on August 1st 2024 that they finally became set. However, despite this, much of the practical detail and processes entailed under the Act will remain unclear for some while yet.

In contrast to this is the second category relating to AI system technology itself and its use, plus the implications that have already arisen for police and law enforcement and those that are still coming to notice. A major catalyst for rapid change appeared in late November 2022 as a result of the release to the public by 'OpenAI' of their 'generative AI system' known as 'ChatGPT', closely followed by releases from other companies. In a very short space of time, AI systems based on Large Language Models (LLM) arrived and they quickly became of great interest to the public, the press and governments. Since

[2] ALIGNER Description of Work, Part B-4 and B-5

then, the expansion in the capabilities, scale, scope and public availability of 'general purpose AI systems' (GPAI) has expanded at great speed. When these two events occurred during the lifetime of project ALIGNER are shown below in Figure 1.

Figure 1 – Chronology of the three Project ALIGNER policy recommendation iterations and two key external events



Returning to the commencement of ALIGNER, before either of these developments had occurred, the first ALIGNER workshop was held in November 2021 and gave rise to the early insight that AI technology relevant in the context of policing and law enforcement has a dual nature. It consists of two interlinked dimensions, one where AI technology is a crime and security threat that P&LEAs must respond to and challenge when necessary, and one where P&LEAs can utilise AI technology in order to carry out their roles and functions. Over the course of the first three ALIGNER Workshops, it became clear that for EU police and law enforcement agencies (P&LEAs), AI technology was already having an impact within both of these different yet inter-connected dimensions.

In the 'crime and security threat' dimension, AI systems can be a threat if utilised by 'bad actors' to enable them to carry out acts hostile or detrimental to society and individuals within it. Here, the key aspect for P&LEAs is that they have no control over how or why the AI system is being used, nor (initially) over the 'bad actors' who seek to use it for their own illegal or illicit ends. This can create crime and security threats that Police and LEA's have to respond to in both the physical domain (to counter the criminals and their criminal actions) and in the digital domain (to counter the AI system(s) they may be utilising to carry out their criminal actions). In both of these domains, a prime need for P&LEAs is to secure evidence.

In the second of these dimensions, AI systems are utilised by P&LEAs to fulfil their roles and responsibilities to protect society i.e. AI systems are in the service of police and law enforcement agencies. Here, the key aspect is that as organisations, P&LEAs are in control of the AI systems they use, from its initial deployment to the objectives and circumstances of its use. Consequently, they can be proactive as to how it is controlled, directed and utilised.

Crucially therefore, P&LEAs are responsible and accountable for all aspects of how and why they employ it and ultimately, the impact and consequences its use may generate. A 'bad actor' using AI technology in pursuit of their criminal, hostile or malicious ends operates under no such constraints. As will be seen later, the arrival of the AI Act will have a huge impact on not only how, when and where P&LEAs can utilise AI systems, but also on what type of systems they can use and indeed, whether they are prohibited from using particular systems at all.

It became apparent early on in the project that ALIGNER had to adopt a broad approach to AI systems in the context of policing and law enforcement if it was to achieve relevant and useful results. If it did not and only focused on AI systems as a crime and security threat, a significant gap could occur as the second critical dimension of AI systems, how they can be utilised in the service of P&LEAs, could end up being given less attention than it deserves.

Nearly three years on from the commencement of ALIGNER, the EU Artificial Intelligence Act is now EU law and this dichotomy has been thrown into sharper focus. With the recent passing into law by the EU of the Artificial Intelligence Act, a new environment has begun to emerge in which P&LEAs will have to operate. Within it, the newly established 'EU Artificial Intelligence Office' can now start to carry out its function "*to contribute to the implementation, monitoring and supervision of AI systems…and AI governance*" and begin its task "*to encourage and facilitate the drawing up of codes of practices and codes of conduct at Union level…as well as monitoring the implementation and evaluation of codes of practices".*[3] It is clear that the AI Act compliance regime that will soon have to emerge will be a strong one and that P&LEAs will face many challenges to put into place and comply with the provisions of the Act that apply to them.

It may be a truism that '*policy is not made in a vacuum'*, but it also holds good for the ALIGNER policy recommendations. Consequently, the long-awaited enactment into law of the AI Act necessitated a review of its provisions where they were entirely applicable to P&LEAs, or those that will have the most consequence on P&LEA activities, to see where they might impact on each of the ALIGNER policy recommendations as they stood in their September 2023 iteration. It is important to note that the EU AI Act consists of thirteen Chapter titles, each of which contains its own set of Articles. In total, there are one hundred and thirteen Articles, plus an additional thirteen Annexes.[4] In the time available since the wording of the Act became final, it has not been possible to explore it to the depth that will eventually be necessary. It is also not yet possible to take into account the "Codes of Practice", "Guidance" or "implementing legislation" that the Act refers to, as none of it has yet been written or released.

However, working within these parameters led to the conclusion that the provisions of the AI Act will impact to some degree on all the ALIGNER policy recommendations but that it does not cause any policy recommendation to become superfluous or irrelevant. It was also clear a number of refinements to them could usefully be made and these revisions have been carried out.

This final ALIGNER deliverable also proposes three new policy recommendations that became apparent during the impact review and comparison, giving a final total of nine ALIGNER policy recommendations (see Section 4.2: Summary table of the final set of the ALIGNER Policy Recommendations).

[3] "*Commission Decision of 24.1.2024 establishing the European Artificial Intelligence Office*"
[4] See Annex A: EU Artificial Intelligence Act: A 'Table of Contents'

1.1 Gender Statement

ALIGNER partners actively safeguard gender equality and are aware of gender issues in science and technology (reference "Commission of the European Communities: Women and Science: Excellence and Innovation–Gender Equality in Science, SEC (2005) 370, available at https://data.consilium.europa.eu/doc/document/ST-7322-2005-INIT/en/pdf).

ALIGNER monitors gender equality addressing biases and constraints throughout all the stages of the project as listed in Gendered Innovations 2 (reference "European Commission: Gendered Innovation 2 How Inclusive Analysis Contributes to Research and Innovation, (2020) available at https://op.europa.eu/en/publication-detail/-/publication/33b4c99f-2e66-11eb-b27b-01aa75ed71a1/language-en).

Outreach activities, visual representations, events, modes of data gathering and analysis, and other research products related to D2.4 have been and will be gender proofed during the internal review process following the ALIGNER Gender policy (reference: ALIGNER D1.2 Project Handbook, section 8 '*Gender aspects in publications and research'*).

1.2 Structure of this report

After the 'Introduction' under Section 1 above, the remainder of this deliverable is structured as follows.

Section 2 provides a foundation by presenting an overview of how the initial ALIGNER policy recommendations were created, formalized and then presented in September 2022 in the deliverable, '*D2.3 - Policy Recommendations'*. The first part of this section recaps how the overall policy-related output of the first three ALIGNER workshops was gathered and analysed to identify and categorise into six potential policy issues "*tailored to the operational needs of the law enforcement sector"*. From this information, forty-four 'areas of concern' and capability gaps were identified where potentially, EU policy may be required to address them. These were analysed, assessed and finalised as the initial ALIGNER policy recommendations.

The final part of Section 2 describes the effort made during the second year of ALIGNER to ensure the ALIGNER policy recommendations continued to accurately reflect the needs of P&LEAs in a rapidly changing environment (policy and real world) by ascertaining if and how ALIGNER varied from, was in congruence with, or complemented related policy recommendations put forward by external sources.

To achieve this, a cross-project comparison was carried out to examine policy recommendations presented by external AI system related projects to see if they were in concordance with the ALIGNER policy recommendations and to assess what impact they may have on them. Each ALIGNER policy recommendation was compared to relevant policy recommendations produced by ALIGNER's two sister projects in the EC Security Union (SU) AI Cluster), namely *'popAI'* and *'STARLIGHT'*, whose focus was also on AI technology and law enforcement. In addition, the high-level findings of the ENISA 'Research and Innovation Recommendations' were also included in the comparison.

The overall results were then used to rank the ALIGNER policy recommendations into their order of congruence and finally, some of their wording was also revised to better reflect their applicability to the situation as it stood in September 2023 when their second iteration was published (see deliverable '*D2.3 - Policy Recommendations'*).

Section 3 examines the impact on the ALIGNER policy recommendations of the Artificial Intelligence Act that came into force as EU legislation on August 1st 2024. For almost the entire three-year timescale of project ALIGNER, the EU had been in a process of negotiation over the legislation, and therefore there was much uncertainty and constant change before the final version of the Act was arrived at, setting out the numerous prohibitions, obligations and requirements that EU P&LEAs must now begin to plan and prepare how they will comply with them.

This section commences with an overview of the provisions of the AI Act that are of most relevance to EU P&LEAs and from there, starts to examine what aspects of the Act would seem to impact on each of the six ALIGNER policy recommendations in their iteration from 2023. In addition to this, the coming into force of the Act has now generated a need for three new ALIGNER policy recommendations to be formulated. They are put forward here, along with their accompanying rationales and suggestions for their implementation.

Section 4 pulls together all the ALIGNER policy recommendations developed across the lifespan of the project into a final consolidated set, while Section 5 draws a number of broad conclusions.

Finally, there are three Annexes to this document, as listed below:

ANNEX A - EU Artificial Intelligence Act: A 'Table of Contents'

ANNEX B – Summary of the 'Over-arching categories' and 'Areas of Concern' arising from ALIGNER Workshops 1-3

ANNEX C – Summary of Policy Recommendations from 'popAI', 'STARLIGHT' and ENISA used in the cross-project comparison with the ALIGNER Policy Recommendations

2. How the ALIGNER Policy Recommendations were derived and validated

2.1 Deriving the first iteration of the ALIGNER Policy Recommendations

Methodology and approach

In early 2021, before the formal commencement of Project ALIGNER, the complexity surrounding AI technology and its use by Police and LEAs (P&LEAs) was recognised and that they "*are at the forefront of dealing with the dual challenge of maximising the benefits of AI … while simultaneously having to counter the tactics, techniques and procedures (TTPs) used to defeat the legitimate purposes of AI. To add even more complexity, the means by criminals to achieve objectives can range from legitimate, commercially available products to those that are malign and created solely for criminal purposes."*[5]

After working together with the participants at the Workshops, ALIGNER was able to explore and develop this initial perspective into an insight that has held strongly as a theme throughout the project, namely; there are two closely aligned facets relating to AI systems in the context of policing and law enforcement. In one, AI systems can pose a crime and/or security threat. In the other, AI systems can be utilised by Police and Law Enforcement Agencies to increase their operational capabilities and deliver improvements to their overall effectiveness.

The research undertaken by ALIGNER to develop policy recommendations designed to assist P&LEAs to operate in this environment utilised a variant of Grounded Theory and the use of data tables.[6] It provided an alternative means of analysing data other than the more traditional one built upon hypothesis, deductive theory and quantitative research. Instead, it relied on an inductive approach to the analysis of qualitative data, adapting and modifying its goal as new evidence emerged during the research process.[7]

During discussions and presentations during the first three ALIGNER Workshops, detailed information relevant to each of three key aspects of ALIGNER was gathered; AI technology as a crime and security threat, AI technology in the service of P&LEAs, and the existing and potential AI system capability needs of P&LEAs. The information was processed to produce a detailed summary of each point raised.

By applying an 'open coding' process to the summaries, a textual analysis of the workshop activities and discussions could be conducted. This process fragmented the summaries and enabled the identification of a number of 'areas of concern' where the development of future policy may be required. To distinguish where each of the 'areas of concern' had originated from, a code was attached to each one e.g., 'WS 1' for workshop one etc.

Once these steps had been completed, the Grounded Theory process of 'axial coding' was applied to the data. This re-assembled the data that had been 'fractured' during the process of 'open coding' and did so in a more meaningful and insightful way. All of the 'areas of concern' were then reviewed and

[5] See ALIGNER Description of Work, Part B-10
[6] Grounded Theory is a methodology that uses an inductive approach to qualitative data, enabling general conclusions to be drawn out of an assembled mass of specific data points. (See Strauss, A. & Corbin, J. (1994), Grounded Theory Methodology: An Overview. In N. Denzin & Y. Lincoln *Handbook of Qualitative Research. 1st ed.* (pp 273-284) and Warnes, R. (2009) Grounded Theory. In Ling, T. & Villalba van Dijk, L. *Performance Audit Handbook: Routes to Effective Evaluation.* Santa Monica, Rand Corporation)
[7] See Glaser, B. and Strauss, A. (1967) *The Discovery of Grounded Theory: Strategies for qualitative research.* London: Transaction.

where duplicates or overlapping aspects were found, these were amalgamated or amended to form more precise and complete summaries, each of them with an appropriate heading. Further information gathered by wider project research was also incorporated where appropriate.[8]

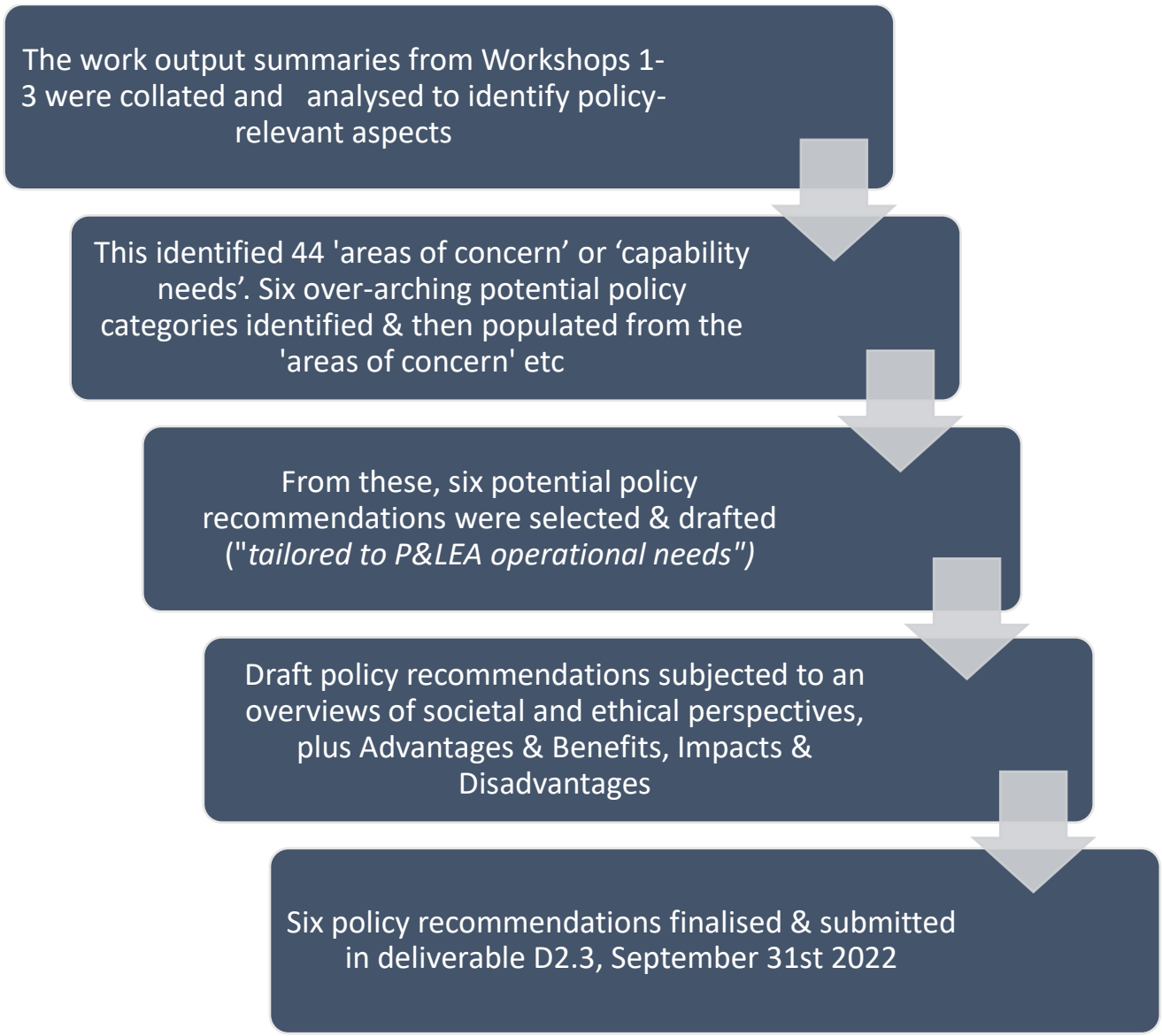
The forty-four 'areas of concern' also included potential P&LEA 'capability needs' and these were assessed and placed into six over-arching categories that had been identified where EU-led policy could have a beneficial effect in the context of policing and law enforcement. Each of them was assigned to one of the categories below:

- AI Technology: Research, development, and exploitation
- AI technology as a Crime and Security threat
- Legal and Judicial issues and considerations
- Ethical and Human Rights implications of P&LEA use of AI technology
- P&LEA utilisation of AI technology to enhance and increase P&LEA capabilities
- P&LEAs and AI technology: Internal governance and training issues

After taking into consideration all the information and categories that had been utilised, six draft policy recommendations were identified and articulated. As required by the ALIGNER description of work, each of them was then reviewed from a societal and ethical perspective, followed by an overview designed to explore their possible 'Advantages and benefits' and 'Impacts and disadvantages'. The overall process followed to arrive at this point is summarised in Figure 1 below:

[8] See ALIGNER deliverable D2.3, Annex B for full details of each 'area of concern' identified

Figure 1 – Summary of process used to derive the initial ALIGNER Policy Recommendations



The six topics identified by ALIGNER as being most suitable for the formulation of EU-led policy were finalised and became the first iteration of the ALIGNER policy recommendations that were published as ALIGNER deliverable D2.3 on September 30th, 2022. They are presented below in Table 1.

Table 1 - ALIGNER initial policy recommendations to address identified P&LEA needs & concerns at EU level (as first published, September 2022)

ALIGNER - Initial Policy Recommendation 1
Ensure the procurement, utilisation and in-service development of all AI technology by P&LEAs is carried out in a holistic way, with full cognizance of the adverse and beneficial impacts it may have on society
ALIGNER - Initial Policy Recommendation 2
Ensure there is always a competent and knowledgeable 'human in the loop' if AI technology is used to support and assist P&LEAs and criminal justice systems in critical decision-making processes
ALIGNER - Initial Policy Recommendation 3
Review the EU data protection framework on the use by AI technology of 'real-world' data as it appears to act as a barrier to the procurement and use by P&LEAs of AI technology
ALIGNER - Initial Policy Recommendation 4
Enable and support the P&LEAs of EU Member States to bridge gaps between their current levels of technology, the AI technology of today and AI technology already on the near horizon
ALIGNER - Initial Policy Recommendation 5
The EU to approach AI technology adoption in the context of P&LEAs and criminal justice systems by using a Directive, as used to counter terrorism from 2017 onwards
ALIGNER - Initial Policy Recommendation 6
Conduct further and regular research into P&LEA and criminal justice concerns and capability needs for AI technology in order to ensure EU policy makers are aware of new developments and on-going issues

Section 2.2 below shows how, during year two of ALIGNER in 2023, the initial policy recommendations were further developed in two ways, first, they were compared to assess their congruence with relevant policy recommendations from other related projects and organisations and second, their content and wording was revised and finally they were ranked by order of congruence.

2.2 Testing and validating the first iteration of the ALIGNER Policy Recommendations

2.2.1 Subjecting the ALIGNER Policy Recommendations to a cross-project comparison

It should be noted that over the second year of ALIGNER (2022 to 2023), both AI systems and their use, plus the new EU legislation of the Artificial Intelligence Act that was expected to regulate and control them, continued to develop. This period also included the first public release in November 2022 of a 'general purpose AI' system, in the form of 'ChatGPT'. This aspect of AI technology, its impact and consequences had not been foreseen in the AI Act legislation and this meant that further amendments had to be drafted and debated, resulting in continuing uncertainty over how, why and when the Act would affect the activities of P&LEAs in relation to AI systems.

Against this background, the opportunity was taken by ALIGNER to try and assess where its original policy recommendations sat in the wider AI policy landscape. In order to do this, it was decided to assess how congruent each one of them was when compared with the recommendations produced to date by ALIGNER's 'sister' projects in the EC Security Union AI cluster. There were two of these projects; 'PopAI' (*European Positive Approach towards Artificial Intelligence tools in support of Law Enforcement & Safeguarding Privacy & Fundamental Human Rights*) and Project STARLIGHT (*Enhancing the EU's strategic autonomy in field of Artificial Intelligence for LEAs*).

Similar to ALIGNER, both of the above projects had commenced their work in either 2020 (popAI) or 2021 (STARLIGHT) and with ALIGNER, all three were required by the Commission to work collaboratively and when possible, collectively. Each of them had been tasked to produce their own policy recommendations.[9] PopAI was completed as a project in September 2023, when their policy recommendations became final, while STARLIGHT had by then produced their first interim version. A third element in the comparison was added by selecting relevant recommendations and findings from a set of recommendations produced by the European Union Agency for Cybersecurity (ENISA), released in June 2023.

It is important to note that the assessment was not carried out on an exact 'word for word' comparison basis for each policy recommendation. This approach would not have been effective or useful due to the myriad of interpretations and differing contexts of many of the key words used by the projects e.g. "framework", "evaluation", "performance" or "standards". To mitigate this variability, the comparison was made by using a combination of the six ALIGNER policy recommendations from September 2022 plus, for each one, a more broadly worded 'Aim' specifically written to describe it.

An initial process of selection was undertaken to ensure that the other project policy recommendations used in the comparison were broadly compatible with the focus of the ALIGNER policy recommendations, even if they were not specifically *"…tailored to the operational needs of the law enforcement sector…".* A total of twenty-eight selected recommendations were then available to be assigned to what was judged to be the most appropriate ALIGNER policy recommendation.

In addition to the instances where an external policy recommendation was only comparable to a single ALIGNER policy recommendation, there were also four instances where external policy recommendations were considered as an appropriate 'fit' with two ALIGNER policy recommendations.

[9] A summary of all three sets of policy recommendations (Pop AI, STARLIGHT and ENISA) can be found at Annex C of this document

There were a further five instances when they were judged to be congruent with three ALIGNER policy recommendations. Overall, this meant that the six ALIGNER policy recommendations were able to be compared with forty-two external policy recommendations from the three different sources. A summary of the comparison findings are set out in Table 2 below.

Table 2 – External Project comparisons: Number of congruent Policy Recommendations from external projects assigned to each ALIGNER policy recommendation (n=42)

Project ALIGNER Policy Recommendation Nos. (PR)	Total Project popAI PRs congruent with ALIGNER	Total Project STARLIGHT PRs congruent with ALIGNER	Total ENISA PRs congruent with ALIGNER
ALIGNER PR 1	**9** (PRs.2,5,6,7,8,10,11,14,15)	**3** (PRs.2,3,5)	**2** (RG1, RG2)
ALIGNER PR 2	**1** (PR.9)	**Zero**	**1** (RG3)
ALIGNER PR 3	**2** (PRs.3,17)	**2** (PRs.1,2)	**2** (RN3, RN4)
ALIGNER PR 4	**5** (PRs.1,2,7,8,12)	**2** (PRs.3,4)	**1** (RN1)
ALIGNER PR 5	**6** (PRs.1,2,6,7,8,10)	**3** (PRs.2,3,5)	**1** (RN5)
ALIGNER PR 6	**1** (PR.13)	**Zero**	**1** (RN2)
Total	**24**	**10**	**8**

A number of insights were drawn from these results and are set out in the following section.

2.2.2 Assessing, revising and prioritising the ALIGNER Policy Recommendations

On examination from a high-level, cross-project perspective, the congruency assessment yielded a number of insights into the overall policy recommendation environment of the SU cluster participants. In essence, these insights were predominantly associated with the need to provide certainty for P&LEAs relating to how they can acquire and utilise trusted and safe AI systems and do so in a holistic way (from defining their capability needs to carrying out their procurement and deployment), and how they can do so within a regulatory and compliance environment that will both support and constrain P&LEA operations and functions. A second, smaller category of suggestions refers to specific requirements to enhance the functions and activities of P&LEAs when involved with AI systems.

The most important policy recommendations were aggregated and summarised as follows:

- The procurement, utilisation, in-service development and use of AI systems as tools by P&LEAs or on their behalf should be approached in a holistic way. This should be based on a common European understanding of AI systems and carried out by P&LEAs utilising common and harmonised EU legal directions and guidelines

- For P&LEAs to effectively engage with AI systems and their potential capabilities, there is a need for an EU-wide framework to enable, enhance and institutionalise how they do so. It should be designed for this purpose and utilise elements of primary legislation, statutory regulations, guidelines and protocols, systems and structures, processes and procedures

- The role of ethics in the P&LEA approach to AI technology and tools is seen to be of fundamental importance and should be governed by a clear and consistent 'ethical framework' of principles and practices

- AI systems as tools for P&LEAs in the EU should be legally compatible and functionally interoperable. To achieve this, they should be evaluated (for legality, ethical compliance and functional performance). Consequently, there is a need for agreed standards to enable them to be assessed and compared

- The establishment by the EU of a single body or organisation to act as a nexus between rapidly developing AI technologies and their impacts on P&LEA functions and responsibilities could bring many benefits. Two of its suggested functions were for it to act as an Observatory to monitor AI and cybersecurity threats (source ENISA) and as a central AI Systems Registry of each one used by P&LEAs across the EU (source STARLIGHT)[10]

  Other functions could also be envisaged for it, for example, as a source of impartial and accurate advice and guidance for P&LEAs on issues relating to AI systems. This type of approach would contribute to a common European understanding and enhance P&LEA cooperation and collaboration

- The congruency assessment could be used as a benchmark against which the ALIGNER policy recommendations can be compared in the future to enable them to be re-evaluated and revised as necessary.

Finally, it should be noted that if the policy recommendation insights are embraced as a whole, then the more likely they are to enhance the effectiveness of P&LEAs whilst at the same time safeguarding the rights and privacy of individuals and wider society. An alternative future dominated by unguided and unregulated deployment of AI technology by P&LEAs is highly unlikely to achieve any comparable situation.

[10] (See also new ALIGNER policy recommendation (3) on pp.54-55 which compliments the STARLIGHT recommendation)

Revisions to the ALIGNER policy recommendations in the light of the congruency assessment

The original set of ALIGNER policy recommendations were published in 2022 and were deliberately not ranked into any order of priority as it was felt that it was too early in the project for this to be determined in any meaningful way. Consequently, their numbering from 1 to 6 was done only to distinguish between them for reference purposes.

After the congruency assessment process, it then became possible to develop a ranked hierarchy of each ALIGNER policy recommendation according to its degree of congruence with the external projects. It ranged from the 'most congruent' (with fourteen external project policy recommendations) to the 'least congruent' (with two external project policy recommendations).

Once this was done, the ALIGNER policy recommendations were reordered and renumbered. This step is shown in detail in Table 3 below:

Table 3 - ALIGNER Policy Recommendations ranked in descending order of congruency compared to those of selected external projects

ALIGNER PR ranked in order of congruency	ALIGNER Policy Recommendation Nos.	popAI PRs congruent with each ALIGNER PR	STARLIGHT PRs congruent with each ALIGNER PR	ENISA PRs congruent with each ALIGNER PR	Total no. PRs congruent with each ALIGNER PR
First	**ALIGNER PR 1**	9	3	2	(14)
Second	**ALIGNER PR 5**	6	3	1	(10)
Third	**ALIGNER PR 4**	5	2	1	(8)
Fourth	**ALIGNER PR 3**	2	2	2	(6)
Fifth	**ALIGNER PR 2**	1	0	1	(2)
Sixth	**ALIGNER PR 6**	1	0	1	(2)
					[Total = 42]

After they had been ranked in order of concordance with comparable policy recommendations from the external projects, the opportunity was taken to reassess and revise the wording of the original ALIGNER policy recommendations in order to better reflect the overall aim of each one. The new versions of these, as published in D2.4 in September 2023, are shown in the following section.

2.3 The second iteration of the ALIGNER Policy Recommendations

The wording and overall relevance of the ALIGNER policy recommendations, as set out in Table 4 below, continued to be reviewed in year three of the project, with a view to producing a final iteration of them by its end in September 2024. The events that occurred and the circumstances that developed over this time-span that were of enough relevance to impact on ALIGNER, plus how and why its policy recommendations evolved from the form they were set out in Table 4, are dealt with in the following section.

Table 4 – ALIGNER policy recommendations, 2023, with updated wording and as ranked in order of congruency with selected external projects

ALIGNER Policy Recommendation 1 (As revised 2023)
The EU to ensure that the procurement, utilisation and in-service development of all AI technology, by or on behalf of P&LEAs, is carried out in a holistic and consistent way, taking full cognizance of both the adverse and beneficial impacts it may have on society
ALIGNER - Policy Recommendation 2 (As revised 2023)
The EU to provide as a matter of priority a tailored legislative framework designed specifically to guide and support the P&LEAs of Member States in their adoption, acquisition and use of AI technology
ALIGNER - Policy Recommendation 3 (As revised 2023)
The EU to assist and support the P&LEAs of Member States to bridge the gaps between their current level of technology and the AI technology that is already available and to transition towards the AI technology that is already foreseeable on the near horizon
ALIGNER - Policy Recommendation 4 (As revised 2023)
The EU to instigate a review of the EU data protection framework as it relates to the nexus between 'real-world' data and P&LEA functions and operations, and their potential use of AI technology to access and process it. Currently, it appears to act as a barrier to P&LEA procurement and use of AI technology
ALIGNER - Policy Recommendation 5 (As revised 2023)
The EU and Member States to ensure P&LEAs always have a trained, competent and knowledgeable 'human in the loop' when they utilise AI technology to assist in decision making processes
ALIGNER - Policy Recommendation 6 (As revised 2023)
To urge the EU to conduct and facilitate systematic and regular research into AI technology that may have potential ramifications (both as solutions and as threats) for the operational needs and capability requirements of P&LEAs

3. The impact of the EU Artificial Intelligence Act on the ALIGNER Policy Recommendations

3.1 Overview of the Artificial Intelligence Act in the context of policing and law enforcement

The AI Act aims to ensure that AI systems placed and used in the EU internal market are safe and respect fundamental rights. However, while the Act is now in force, none of its requirements apply as yet.[11] For the provisions that are relevant in a police and law enforcement context, this will occur over an already unfolding timeline of key dates between now and August 2nd 2026, when a substantial number (but not all) of its provisions come fully into force.

To achieve its objectives, the Commission pursued a horizontal regulatory approach as the Act is intended to provide a flexible and future-proof legal framework applicable to all 'AI systems' throughout their whole lifecycle in all sectors of the internal market. To assist in this, it defines AI systems both broadly and in a technologically-neutral way.

As it is 'horizontal legislation' applying to all AI systems in all sectors of the market, it is important to note that while the Act includes numerous provisions of direct relevance to the roles, responsibilities, functions and activities of police and law enforcement agencies, it does not have within it any cohesive or unifying framework, structure or approach to these aspects.

The complete provisions of the Act are contained in one hundred and thirteen Articles, grouped into thirteen thematic Chapters and supported by thirteen Annexes. Of these, the majority of provisions relating to police and law enforcement are found in:

- Chapter II: Prohibited Artificial Intelligence Practices
- Chapter III: High-Risk AI Systems
- Annex II: List of Criminal Offences
- Annex III: High-Risk AI Systems

However, in particular, a greater number of Articles also contain important information or requirements for P&LEAs to comply with e.g. Article 3: *Definitions* and Article 4: *AI literacy*.

The topics described in this overview as applicable to policing and law enforcement are the most obvious and relevant ones and are predominantly drawn from the Chapters and Annexes given above. Exact information and further relevant aspects should be obtained by the reader directly from the text of the legislation.

Broadly speaking, many of the provisions of the Act of concern to P&LEAs are designed to ensure that fundamental rights are enforced, with a focus around three questions:

- ❖ What type of AI system can or cannot be utilised by P&LEAs?
- ❖ What is the purpose, circumstances and justification for each use of an AI system?

[11] EU Artificial Intelligence Act, 19.4.2024, available at https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf

- What compliance regime measures must be taken by every P&LEA to ensure its use of an AI system is lawful under the AI Act?

For P&LEAs, the Act is designed primarily to regulate their use of AI systems by P&LEAs. It does not criminalise nor otherwise address AI systems that are lawfully on the market but are misused for unlawful purposes, nor does it cover instances where they are utilised by 'bad actors' for malicious or criminal purposes. Consequently, AI systems used for such malicious or criminal purposes must continue to be dealt with by the provisions of the relevant existing criminal law.

An early challenge to the 'future proof' intentions of the Act occurred when the Act was still under consideration as a Proposal, from 2021 to 2022, as its provisions did not anticipate the appearance of AI models with 'generative capabilities', nor their fast and widespread introduction into the public sphere as 'general purpose AI systems' (GPAI). Fortunately, as the Act was not yet law, it could be modified and improved in response to the appearance of the first one, ChatGPT, in November 2022. It was very quickly followed into the public domain by a plethora of other generative AI systems released by other technology companies.

The AI Act definition of AI systems

The final version of the Act is now enshrined in EU law and defines an 'AI system' as "*a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".* (Article 3(1). The definition accentuates the key characteristics distinguishing an AI system from other technology, such as the capability to operate according to explicit or implicit objectives, its autonomy and adaptiveness, as well as the capability to infer outputs from inputs or data.

The Act builds on this to also provide an explicit definition of a 'general purpose AI system' as "*an AI system which is based on a general-purpose AI model that has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems."* (Article 3 (44e)

Scope of application

The Act applies to two main categories of entities:

- An AI 'provider'; meaning "*a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge."* (Article 3 (3)

- An AI 'deployer'; meaning "*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." (Article 3 (4)*

Police and law enforcement agencies that use an AI system are, as 'public authorities', now considered to be 'deployers' of an AI system when they acquire and use it.

As for its geographical scope of application, the Act applies to both AI system providers and deployers established or located in the EU, and providers and deployers established in a third country when the

AI system is put into service in the EU or placed on the EU market or when the output produced by the AI system is used in the EU.

Article 2 (24) excludes from the scope of application of the Act "*systems for military, defence or national security purposes*". However, if an AI system developed or used for these purposes is used, temporarily or permanently, for other purposes "*for example, civilian or humanitarian purposes, law enforcement or public security purposes*", then the AI Act would apply to it.

Some considerations for 'providers' and P&LEAs as 'deployers'

The AI Act and 'General-purpose AI'

A 'general-purpose AI model' is an AI model that displays significant generality and is capable of competently performing a wide range of distinctive tasks regardless of the way the model is placed on the market and which can be integrated into a variety of downstream systems or applications. Examples are where generative AI creates new text, images, audio or videos.

In essence, GPAI models create obligations under the AI Act predominantly applicable to 'providers'. However, GPAI systems create obligations under the AI Act for both 'providers' and 'deployers' and consequently, these will apply to police and law enforcement agencies should they acquire or use an AI system designated as 'high risk' by the Act.

'General purpose AI systems': Obligations placed on their deployer

A 'general-purpose AI system' is an AI system which is based on a 'general-purpose AI model' that has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems. Examples are 'ChatGPT and 'Midjourney'. GPAI systems create obligations for both 'providers' and 'deployers' i.e. they will affect P&LEAs if they are the deployer of a GPAI system (by itself or as a component of other AI systems) and they can be of 'high risk'.

Deployers of general-purpose AI systems classified as high-risk AI systems when used in isolation or as components of other high-risk AI systems must comply with the obligations for high-risk AI systems established by the AI Act.

Moreover, deployers of general-purpose AI systems generating synthetic content need to comply with the transparency obligations established by the AI Act. If the AI system generates a deep fake or if it generates text with the purpose of informing the public on matters of public interest, then it must be labelled as artificially generated or manipulated.[12] However, there are exceptions in certain circumstances if the AI system is "…*authorised by law to detect, prevent, investigate or prosecute criminal offences…"*

[12] AI Act, Article 50: Transparency obligations for providers and deployers of certain AI systems

The AI Act requirement for 'AI Literacy': A new core concept for all police and law enforcement agencies

Before examining the provisions of the Act that relate explicitly to policing and law enforcement, note should be taken of the how the Act emphasises the centrality of human beings in operating and exercising oversight of AI systems in an environment where 'High Risk' AI systems are deployed.

This is set out in Article 14: '*Human oversight*' as "*High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use*."

Having set out this requirement, the Act reinforces it by introducing the concept of 'AI literacy' in Article 4: *AI Literacy.* The requirement here is for providers and deployers of AI systems "*to ensure to their best extent a sufficient level of AI literacy for their staff and other persons dealing with the operation and use of AI systems […]*"

The Act defines in detail AI literacy under Article 3(42)(bh) as the "*skills, knowledge and understanding that allows providers, users [deployers?] and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause.*"

P&LEAs who utilise AI systems are considered as 'deployers' of the system and consequently, the requirements of these three Articles are likely to have considerable implications for them in the near-future in terms of the selection, training and employment of their personnel who may interact with AI systems. It will include when they are involved in the selection, procurement and installation of the system or after its introduction, the officers and staff who will use it in the course of their work, and the officers and staff who will be responsible and accountable for implementing the AI Act compliance requirements.

THE RISK BASED REGULATORY APPROACH OF THE AI ACT

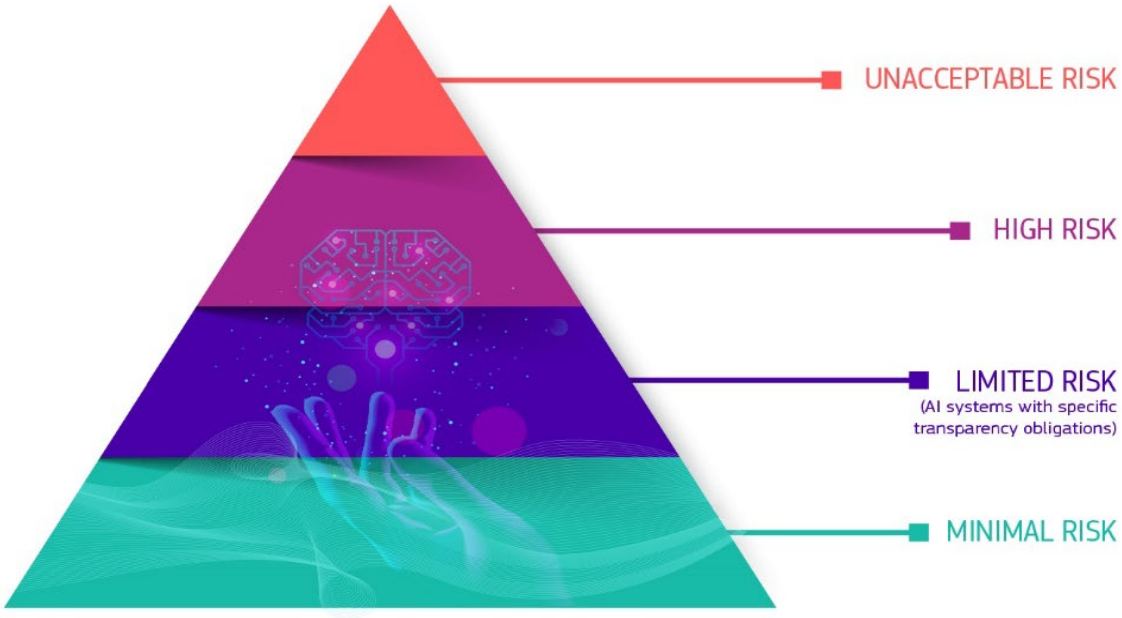
Starting from the assumption that the risks and harm potentially caused by AI systems differ depending on the circumstances and their use, the AI Act adopts a risk-based regulatory approach, where the 'risk of harm' is defined under Article 1(a) as;

> *"…the combination of the probability of an occurrence of harm and the severity of that harm"*

As shown in Figure 2 below, the Act distinguishes four levels of risk of harm with AI systems:

- Unacceptable risk
- High risk
- Low risk
- Minimal risk

Figure 2: AI 'risk of harm' levels *Source: European Commission*



UNACCEPTABLE RISK

The AI Act, under Article 5(1), prohibits the placing on the EU market or the use of any AI system deemed to create an unacceptable risk by contravening EU values and violating fundamental rights.[13] The prohibition covers eight AI practices:

- AI systems deploying subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, when they materially distort the behaviour of a person or group, causing them to take a decision they would have not taken and in a manner that is likely to cause significant harm.
- AI systems exploiting any of the vulnerabilities of a person or group due to their age, disability, social or economic situation, when they materially distort their behaviour and in a manner that is likely to cause significant harm.
- AI systems used to evaluate or classify a person or group over a certain period of time based on their social behaviour, personal or personality characteristics, when the score leads to detrimental or unfavourable treatment in an unrelated social context or detrimental or unfavourable treatment that is unjustified or disproportionate.
- AI systems to assess the risk of a person committing a criminal offence, based solely on their profiling or on their personality traits and characteristics, unless used to support human assessments after reasonable suspicions based on objective and verifiable facts linked to a criminal activity.
- AI systems creating or expanding facial recognition databases through the untargeted scraping of facial images from internet of CCTVs.
- AI systems used to infer emotions of a person in a workplace or education institutions.

[13] Artificial Intelligence Act, Article 5: Prohibited Artificial Intelligence Practices

- Biometric categorisation systems deducing or inferring a person's race, political opinion, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation, unless used to label or filter lawfully acquired biometric datasets.
- Real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes.

The section below examines three areas where the use of AI systems is prohibited and where it is of particular relevance for P&LEAs.

1. **Prohibited:** Real time remote biometric identification systems in publicly accessible spaces for law enforcement purposes (Article 5(1)(h)

Due to its prevalence and potential operational implications for P&LEAs, the prohibition under Article 5(1) (h) of the Act will be considered first. It prohibits P&LEAs from using remote biometric identification systems operating in 'real-time' in publicly accessible spaces for the purposes of law enforcement, except for the purpose of confirming the identity of a specifically targeted individual. Article 3 (42) defines such an AI system as:

> "*a remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, comprising not only instant identification, but also limited short delays in order to avoid circumvention"*

To become prohibited, these AI systems must fulfil an additional four conditions:

- The AI system needs to be designed for the purpose of identifying natural persons at a distance, by matching their biometric data with those contained in a reference database
- The identification process, from the moment of the collection of data to that of the identification in itself, needs to occur in real time, or without any significant delay
- The AI system needs to be deployed in any physical place which is accessible to the public.
- The AI system needs to be used for law enforcement purposes, that is; 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 safeguarding against and preventing threats to public security.

A distinction is drawn between this type of use and where remote systems are used for "post" identification. These are not prohibited as the risk from their use is considered as "high risk" rather than "unacceptable". A final point of note is that real time remote biometric identification systems are also allowed and treated as "high risk" if they are used for purposes other than law enforcement e.g. crowd control or public health. In these circumstances they are subject to the requirements established by the General Data Protection Regulations (GDPR).

> Exceptions enabling P&LEAs to the use real time remote biometric identification in publicly accessible spaces for the purpose of law enforcement (Article 5(1)

The prohibition of Article 5(1)(h) concerning the use of AI systems for real time remote biometric identification in publicly accessible spaces for the purpose of law enforcement is not an absolute one. Their use is allowed when it is strictly necessary to confirm the identity of a specifically targeted individual in the three following situations:

- Targeted search for specific victims of abduction, human trafficking or sexual exploitation, as well as for missing persons;

- Prevention of a specific, substantial, and imminent threat to the life of physical safety of persons or “a genuine and present or foreseeable threat of a terrorist attack”;
- Localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for the offences listed in Annex II to the AI Act and punishable in the Member State by a custodial sentence or a detention order for a maximum period of at least four years.

Before initiating the use, P&LEAs need to evaluate:

- The nature of the situation arising, in particular the seriousness, probability and scale of the harm that would be caused if the system was not used
- The consequences of its use for the rights and freedoms of all persons concerned

The evaluation must determine that the national laws relating to its necessary and proportionate safeguards and conditions have been complied with. Moreover, before initiating its use, P&LEAs must request an *ad hoc* authorisation from the competent judicial or administrative authority, unless there is a duly justified situation of urgency. If the authorisation is not granted, P&LEAs must stop using the system and delete the data and outputs.

The use can be authorised only if a Fundamental Rights Impact Assessment (FRIA) has been completed by the P&LEA, as provided for by Article 27. Finally, the AI system must be registered in the EU database according to Article 29 (in justified cases of urgency, the system can be used without being registered provided that registration is completed without undue delay).

The Act provides no clarification or definition of “public security services” or “national security purposes” and this may prove problematic in areas where the Act specifically mentions terrorism or terrorist acts e.g. in Article 5 (1)(h) dealing with the use of remote biometric identification for law enforcement purposes in publicly accessible spaces.

The final exceptions to the prohibition on P&LEAs using real time remote biometric identification systems in publicly accessible spaces for law enforcement purposes are listed by the Act in Annex II: *List of Criminal Offences Referred to in Article 5(1), First Subparagraph, Point (h)(iii).* The criminal offences previously listed in the original Proposal have now been extensively amended, with fifteen of them being dropped completely e.g. ‘computer-related crime’. The final list of seventeen offences is now as follows:

- Terrorism
- Trafficking in human beings
- Sexual exploitation of children and child pornography
- Illicit trafficking in narcotic drugs or psychotropic substances
- Illicit trafficking in weapons, munitions or explosives
- Murder
- Grievous bodily injury
- Illicit trade in human organs or tissue
- Illicit trafficking in nuclear or radioactive materials
- Kidnapping, illegal restraint or hostage-taking
- Crimes within the jurisdiction of the International Criminal Court
- Unlawful seizure of aircraft or ships
- Rape
- Environmental crime

- ❖ Organised or armed robbery
- ❖ Sabotage
- ❖ Participation in a criminal organisation involved in one or more of the offences listed above

2. **Prohibited:** Biometric categorisation and databases (Article 5(1)(g) and (e)

P&LEAs are prohibited from using AI systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. (Article 5(1)(g)

The only exception for P&LEAs is when they label or filter lawfully acquired biometric data or datasets, such as images, for the purpose of law enforcement e.g. sorting images according to hair or eye colour.

The use of AI systems by P&LEAs to create or expand facial recognition databases through the untargeted scraping of facial images from the internet or from CCTV footage is also prohibited (Article 5(1)(e)

3. **Prohibited**: Predictive policing (Profiling) (Article 5(1)(d)

P&LEAs are prohibited from using AI systems to make risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence based solely on the profiling of a natural person or, on assessing their personality traits and characteristics.
However, there is an exception to this where an AI system is used to support the human assessment of the involvement of a person in criminal activity which is already based on objective and verifiable facts directly linked to a criminal activity.

Certain predictive policing systems are not prohibited but they do fall into the category of 'high risk'. These are where:

- ❖ The risk assessment of the likelihood of a natural person offending is not solely based on profiling or on assessing the person's personality traits and characteristics e.g. based also on location;
- ❖ The risk assessment is of the likelihood of a natural person becoming the victim of a criminal offence;
- ❖ Profiling in general.

HIGH RISK

AI systems that pose significant risks to the health and safety or fundamental rights of persons are deemed to be of 'high risk' under Article 6 of the AI Act and are divided into two categories. In one, there are AI systems that are intended to be used as a 'safety component' of a product covered by the EU product safety legislation and required to undergo a third-party conformity assessment. Consequently, it may create high risks of harm to health and safety of individuals.

In the other category are the stand-alone AI systems that fall into the eight areas listed in the Act under 'Annex III: High risk systems'. In the latter case, the system is permitted but only if it complies with specific obligations and undergoes an ex-ante conformity assessment. However, they are not automatically classified as high risk and the onus is on the provider of an AI system to determine if it poses such a risk. In general, an AI system is not considered as creating high risk if it does not materially influence the outcome of the decision-making, e.g. by only performing a narrow procedural task, improving the results of a previously completed human activity, detecting decision-making patterns, or performing a preparatory task to an assessment.

P&LEA use of stand-alone AI systems as listed in Annex III: High-Risk AI Systems

Of the areas of application listed in Annex III, six of them are of relevance to P&LEAs (to varying degrees). They are:

- Law enforcement
- Migration
- Biometrics
- Employment
- Access to public services
- Justice and democracy

Within each of these areas, the AI Act sets out a number of provisions and obligations that P&LEAs must follow:

1. **Law enforcement (Annex III (6 (a-e)**
   If they are permitted by the confines of EU or national law, AI systems used for the following tasks or functions are considered as high risk:
   - Risk assessment of a person becoming the victim of a criminal offence
   - Polygraphs and similar tools
   - Evaluation of the reliability of evidence
   - Risk assessment of a person (re-)offending, not solely on the basis of profiling or assessment of personality traits and characteristics or past criminal behaviour
   - Profiling of persons

2. **Migration (Annex III (7) (a-d)**
   - Polygraphs and similar tools
   - Risk assessment of irregular migration or health risk posed by a person entering the territory of a Member State
   - Systems to assist with the examination of asylum, visa or residence permit applications
   - Systems used for detecting, recognising or identifying natural persons

3. **Biometrics (Annex III (1) (a-c)**
   - Remote biometric identification systems (where not prohibited e.g. post remote identification)
   - Biometric categorisation according to sensitive or protected attributes or characteristics (where not prohibited e.g. according to gender)

- Emotion recognition

4. **Employment and workers management (Annex III (4) (a-b)**
    - Systems used for the recruitment or selection of natural persons, to analyse and filter job applications and evaluate candidates
    - Systems used to make decisions on work-related relationships, promotion or termination of work contracts and systems to allocate tasks or monitor and evaluate employees based on their performance and behaviour

5. **Access to public services and benefits (Annex III (5) (d)**
    - AI systems used to classify and evaluate emergency calls by natural persons, or their use to dispatch or establish priority of emergency first response services, including by police

6. **Administration of justice and democracy (Annex III (8) (a)**
    - AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts or in alternative dispute resolution

All of the AI systems referenced above are categorised as 'high risk' as they operate in areas particularly associated with surveillance, arrest or have the potential for discrimination. Their use can also harm the exercise of other fundamental rights, such as the right to a fair trial or the presumption of innocence.

Obligations of deployers of high risk systems (i.e. includes P&LEAs)

Chapter III, section 3 (Article 27) sets out the obligation for 'deployers' of AI systems that are also "*bodies governed by public law*", which therefore includes P&LEAs, to carry out a Fundamental Rights Impact Assessment (FRIA) on their high-risk AI systems prior commencing their use. Such an assessment must consist of:

- A description of the processes in which the high-risk AI systems are used;
- A description of the periods of time they are used for, and frequency of use;
- Categories of natural persons and groups that are affected;
- Specific risks of harm likely to have an impact on the affected natural persons and groups;
- The human oversight measures to be implemented;
- Mitigation measures and complaint mechanisms.

LIMITED RISK

The third level of risk in the AI Act is 'limited risk' and it is applied to AI systems that are intended to interact directly with natural persons (e.g. chatbots) or to generate content. There are minimal transparency obligations associated with it, namely the requirement to inform the concerned person that they are interacting with an AI system (unless this is obvious) and for AI system generated content to be labelled as such.

The exception to the transparency obligation is when the AI system is authorised by law to detect, prevent, investigate or prosecute criminal offences (Article 50). This will benefit the uses P&LEAs can make of it.

MINIMAL RISK

The fourth and final level of risk is 'minimal risk'. AI systems creating minimal or no risks, such as AI-enabled videogames or spam filters will be unregulated and can be designed and used freely. It is worth bearing in mind that due to human ingenuity and inventiveness, the concept today of a 'no risk' AI system may not hold good in the technological, criminal or security environments of tomorrow.

Selected elements of the AI Act Article 113 implementation timeline and its main impacts on EU P&LEAs

- **August 1st 2024: AI Act enters into force**
  - None of the requirements of the AI Act currently apply (September 2024)
  - Application of the Act is from 24 months from its date of entry into force

    i.e. from **August 2nd 2026**

    N.B. There are numerous exceptions to this
- **December 2024/January 2025: Application of prohibitions**
  - LEAs to have reviewed by then the following AI systems to ensure that they do not fall within the prohibitions:
    - Real-time remote biometric identification systems
    - Biometric categorization systems and databases
    - Predictive policing systems
  - LEAs to have established procedures to request judiciary authorizations for the use of real-time remote biometric identification
  - LEAs to have conducted a fundamental rights impact assessment (FRIA) for each system
  - LEAs to have registered each system in the EU database
- **May 2nd 2025: Commission to have prepared Codes of Practice by this date**
- **August 2025: Application of rules for general purpose AI models & EU governance**
  - LEAs developing general purpose AI models need to implement the corresponding obligations and to notify the Commission if the model creates systemic risks
  - AI Act governance structures (AI Office and EU AI Board) become operative

❖ **August 2026: Application of rules for high-risk systems listed in Annex III**

- LEAs developing and using high-risk AI systems need to implement the corresponding obligations

❖ **August 2029: Commission delegated acts and guidelines**

- Definition of AI
- Prohibitions
- Criteria exempting from high-risk (by December 2025/January 2026)
- High-risk use cases (by December 2025/January 2026)
- High-risk provider requirements

A full implementation timeline of the requirements under the AI Act are contained in its Chapter XIII: Final Provisions, Article 113: *Entry into Force and Application*

Even at this early stage, it is quite apparent that the AI Act will become the single most important factor in the relationship between P&LEAs and AI Systems that it will take a considerable period of time before its full ramifications are understood, and that all the provisions it makes for ancillary structures and requirements are created and published. Despite this, by December 2024/January 2025, P&LEAs that currently deploy AI systems must have carried out in relation to them a number of specified reviews that will directly impact on whether their use can continue or whether it must cease.

Below this strategic level of what the AI calls for, lies the detail of what the words it uses to do so actually mean and what their impact will be. For example, there appears to be a complex area of ambiguity concerning the relationship and boundaries envisaged by the Act between what it states are "*public security purposes*" and "*public safety*", particularly where it involves considerations of terrorism or terrorist threats as these may also impinge on "*national security purposes*".

P&LEAs will also need to have a clear understanding of whether the use of an AI system for the "*prevention of [the] threat of a terrorist attack*" equates to "*safeguarding against and preventing threats to public security*", or are they considered to be different? A terrorist attack is very likely to be a threat both to public safety and to public security, but in addition it could also be a threat to "national security". EU Commission guidance will be needed.

A further example of this type of complexity arises under the wording of Article 5 that sets out a requirement for P&LEAs to demonstrate the necessity for them to utilise a real time remote biometric identification AI system for "*the prevention of… a genuine and present or genuine and foreseeable threat of a terrorist attack"*. They must also ensure all the other requirements of the Act for these circumstances are met.

The use in the AI Act of the words '*genuine*', '*present*' and '*foreseeable*' to describe the type of terrorist attack P&LEAs may be seeking to forestall are problematic. They are not clear, subjective and open to interpretation. For this reason, they are not usually found in the tried-and-tested lexicon of terrorist threat assessment methodologies, and therefore they are not appropriate criteria for P&LEAs to apply to demonstrate their compliance with the AI Act.[14]

[14] In the context of security threat assessments, 'likelihood' can be on a scale of risk from 'Rare', through 'Unlikely', 'Credible' and 'Likely' to 'Almost certain'. Each one has their own generally accepted definition in the context of terrorist threats and security responses.

If this argument is accepted, there is a need for clarification of their meaning so that P&LEAs can demonstrate they have complied with the Act and therefore, they can lawfully deploy this type of AI system in response to the threat of a terrorist attack. (Also see ALIGNER new Policy Recommendation (3) as set out below in Section 3.3, pp.51-52 where this issue is examined in more detail).

3.2 Impact of the EU Artificial Intelligence Act on the second iteration of the ALIGNER Policy Recommendations

The first formal proposal for a Regulation "laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)" was published by the European Commission on April 21st 2021.[15]Just over five months later, Project ALIGNER formally commenced, on October 1st 2021. The gestation period of the Act was a long one, stretching over almost three and a half years until its formal passage into law in July 2024 before coming into force on August 1st 2024.

The consequences of this for ALIGNER have been that, although the outlines and principles of the Act and how they will affect policing and law enforcement have slowly become clearer as the legislation has been revised and modified, what has been missing was the exactness and level of certainty that all Police and Law Enforcement Agencies must have from any legislation that impacts significantly on the how, when and where of performing their day-to-day duties and functions. None of the Act's provisions could be taken as a certainty until they became law very recently. However, this point was close to the end of the project and time to examine the impact of the AI Act on the ALIGNER policy recommendations has been limited.

Despite this time constraint, it is clear that the AI Act will undoubtedly impact on the ALIGNER policy recommendations. It is too fundamental in its provisions for it to be otherwise and simultaneously, the technological advances in AI systems and their ever-expanding commercial availability will also act to ensure that P&LEA must keep their policies, strategies and deployments relating to AI systems under constant review. Meanwhile, P&LEAs must also deal with the constant challenges posed by the threats posed by the use and abuse of AI systems by both 'bad actors' and the public at large.

Assessing the AI Act for areas of potential impact on the pre-existing ALIGNER policy recommendations from 2023

This Section sets out some observations drawn from a broad preliminary examination of the AI Act to discover aspects of it that could have the potential to impact on the ALIGNER policy recommendations. Each of these elements in the Act were assessed in the light of the ALIGNER Policy Recommendations as they stood from September 2023 i.e. after they had been subjected to a cross-project validation process and revised accordingly (as described previously in Section 2.2). Each of the six Policy Recommendations from September 2023 are set out below, along with the Chapters, Sections, Articles and Annexes of the AI Act that appear be of most relevance to each one of them.

For each policy recommendation, the overall assessed *impact* has been categorized as 'High', 'Medium' or 'Low'. When making this judgement, the overall *implications* of the Act for each policy recommendation and, in the wider perspective, for P&LEAs, were also considered. The Section concludes by presenting a number of observations and where appropriate, these have been taken up

[15] European Commission (2021). 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, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (accessed on 18 August 2023)

in the following Section of the report where the final iterations of the ALIGNER Policy Recommendations are presented.

ALIGNER Policy Recommendation 1: (As at September 2023)

Aim - To ensure there is consistency across all aspects of the involvement of P&LEAs with AI systems.

ALIGNER AI Act impact assessment category: **HIGH**

Table 5 - Selected aspects of the Artificial Intelligence Act potentially relevant to ALIGNER policy recommendation 1 (2023)

ALIGNER Policy Recommendation 1 (Revised 2023)
The EU to ensure that the procurement, utilisation and in-service development of all AI technology, by or on behalf of P&LEAs, is carried out in a holistic and consistent way, taking full cognizance of both the adverse and beneficial impacts it may have on society
Artificial Intelligence Act: Selected aspects relevant to ALIGNER PR 1
Chapter I: General Provisions
Article 2: ***Scope (Exemptions from the Act)***
Article 3: ***Definitions ("Artificial Intelligence Office" (42) and "AI Literacy (42)(bh)***
Article 4: ***AI Literacy***
Chapter II: Prohibited Artificial Intelligence Practices
Article 5: ***Prohibited AI practices***
Chapter III: High-Risk AI System
Section 1: Classification of AI systems as High-Risk
Article 6: ***Classification rules for High-Risk of AI systems***
Section 2: Requirements for High-Risk systems
Article 14: ***Human oversight***
Section 3: Obligations of Providers and Deployers of High-Risk systems
Article 26: ***Obligations of Deployer***
Article 27: ***Fundamental Rights Impact Assessment***
Chapter VII: Governance

Section 1: Governance at Union level

Article 64: *AI Office*

Article 67: *Advisory Forum*

Chapter VIII: EU Database for High-Risk AI Systems

Article 71: *AI Systems listed in Annex III*

Annex II: List of criminal offences

Annex III: High-Risk AI systems

ALIGNER Policy Recommendation 2:(As at September 2023)

Aim - To ensure the EU supports P&LEAs in their adoption and use of AI systems by providing a legislative framework designed to achieve this

ALIGNER AI Act impact assessment category: **MEDIUM**

Table 6 - Selected aspects of the Artificial Intelligence Act potentially relevant to ALIGNER policy recommendation 2 (2023)

ALIGNER Policy Recommendation 2 (Revised 2023)
The EU to provide as a matter of priority a tailored legislative framework designed specifically to guide and support the P&LEAs of Member States in their adoption, acquisition and use of AI technology
Artificial Intelligence Act: Selected aspects relevant to ALIGNER PR 2
In general and to varying degrees, the AI Act in its entirety is relevant…
There are also certain provisions of the AI Act relating to policing & law enforcement aspects of particular relevance, such as:
Chapter I: General Provisions
Article 1: *Subject matter,*
Article 2: *Scope (Exemptions from the Act)*
Chapter VII: Governance
Section 1: Governance at Union level
Article 64: *AI Office,*
Article 67: *Advisory Forum*
Section 2: National Competent Authorities & Single Point of Contact

Article 70: ***Designation of NCA & SPOC***

Section 3: Enforcement

Article 77: ***Powers of Authorities Protecting Fundamental Rights***

Chapter VIII: EU database for High-Risk AI systems listed in Annex III

Article 71: ***EU database***

Chapter X: Codes of Conduct and Guidelines

Article 96: ***Guidelines from the Commission on the Implementation of this Regulation***

Annex I: List of Union Harmonisation Legislation

Annex X: Union Legislation on Large-scale IT systems in the Area of Freedom, Security and Justice

[e.g. includes Schengen Information System, Eurodac and Interoperability]

ALIGNER Policy Recommendation 3: (As at September 2023)

Aim - To enable P&LEAs to undertake the transition into adopting and using effective, safe and lawful AI systems

ALIGNER AI Act impact assessment category: **HIGH**

Table 7 - Selected aspects of the Artificial Intelligence Act potentially relevant to ALIGNER policy recommendation 3 (2023)

ALIGNER Policy Recommendation 3 (Revised 2023)
The EU to assist and support the P&LEAs of Member States to bridge the gaps between their current level of technology and the AI technology that is already available and to transition towards the AI technology that is already foreseeable on the near horizon
Artificial Intelligence Act: Selected aspects relevant to ALIGNER PR 3
Chapter I: General Provisions
Article 2: ***Scope***
Article 3: ***Definitions***
Article 4: ***AI literacy***
Chapter II: Prohibited Artificial Intelligence Practices
Article 5: ***Prohibited AI practices***
Chapter III: High-Risk AI System

Section 1: Classification of AI systems as High-Risk

Article 6: *Classification rules for High-Risk of AI systems*

Section 2: Requirements for High-Risk systems

Article 14: *Human oversight*

Section 3: Obligations of Providers and Deployers of High-Risk systems

Article 26: *Obligations of Deployers*

Article 27: *Fundamental Rights Impact Assessment*

Chapter VII: Governance

Section 1: Governance at Union level

Article 64: *AI Office*

Article 67: *Advisory Forum*

Chapter XIII: Final Provisions

Article 111: *AI Systems already placed on the Market or put into Service*

Article 112: *Evaluation and Review*

Article 113: *Entry into Force and Application*

ALIGNER Policy Recommendation 4: (As at September 2023)

Aim - To remove barriers for P&LEA adoption of AI systems created by the lack of clarity in the EU data protection framework

ALIGNER AI Act impact assessment category: **LOW**

Table 8 - Selected aspects of the Artificial Intelligence Act potentially relevant to ALIGNER policy recommendation 4 (2023)

ALIGNER Policy Recommendation 4 (Revised 2023)
The EU to instigate a review of the EU data protection framework as it relates to the nexus between 'real-world' data and P&LEA functions and operations, and their potential use of AI technology to access and process it. Currently, it appears to act as a barrier to P&LEA procurement and use of AI technology

Artificial Intelligence Act: Selected aspects relevant to ALIGNER PR 4

Chapter I: General Provisions

Article 2: *Scope*

Chapter VI: Measures in support of innovation

Article 57: *Regulatory sandboxes*

Article 59: *Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox*

ALIGNER Policy Recommendation 5: (As at September 2023)

Aim – To ensure P&LEAs retain the primacy of the human factor when decisions are made based on information from AI systems.

ALIGNER AI Act impact assessment category: **HIGH**

Table 9 - Selected aspects of the Artificial Intelligence Act potentially relevant to ALIGNER policy recommendation 5 (2023)

ALIGNER Policy Recommendation 5 (Revised 2023)
The EU and Member States to ensure P&LEAs always have a trained, competent and knowledgeable 'human in the loop' when they utilise AI technology to assist in decision making processes

Artificial Intelligence Act: Selected aspects relevant to ALIGNER PR 5

Chapter I: General Provisions (*NB* - Article 3(42)(bh)*; Definitions,* Article 4*; AI literacy*)

Chapter III: High-Risk AI System

Section 2: Requirements for High-Risk systems

Article 14: *Human oversight*

Section 3: Obligations of Providers and Deployers of High-Risk systems

Article 26: *Obligations of Deployers*

Article 27: *Fundamental Rights Impact Assessment*

ALIGNER Policy Recommendation 6: (As at September 2023)

Aim - To encourage AI system-focused research whose results will be of practical use to P&LEAs within realistic timeframes

ALIGNER AI Act impact assessment category: **HIGH**

This policy recommendation is expanded and developed in the final iteration of ALIGNER deliverable D5.8, *'Research roadmap for AI in support of law enforcement and policing'*.

Table 10 - Selected aspects of the Artificial Intelligence Act potentially relevant to ALIGNER policy recommendation 6 (2023)

ALIGNER Policy Recommendation 6 (Revised 2023)
To urge the EU to conduct and facilitate systematic and regular research into AI technology that may have potential ramifications (both as solutions and as threats) for the operational needs and capability requirements of P&LEAs
Artificial Intelligence Act: Selected aspects relevant to ALIGNER PR 6
Chapter X: Codes of Conduct and Guidelines, **Article 96: *Guidelines from the Commission on the Implementation of this Regulation*** **Chapter VI: Measures in support of innovation** **Article 57: *Regulatory sandboxes***

Summary of the AI Act impact assessment on the ALIGNER policy recommendations

Following the review of the AI Act to discover the elements within it of the most relevance to P&LEAs, each of the provisions selected were considered in the light of each ALIGNER policy recommendation and its associated 'aim'. They were then assigned to what seemed to be the most appropriate one. Some provisions were assigned to more than one policy recommendation/aim. After this process, a number of insights emerged and they are summarised below as follows:

- The AI Act has impacts, at varying levels, on each one of the six pre-existing ALIGNER policy recommendations from September 2023

- Overall, the assessed categories of AI Act provisions were rated as being of 'HIGH' impact in four cases, of 'MEDIUM' impact in one case and of 'LOW' impact in one case (see Table 11 below for a summary)

Table 11 – Summary of the impact of the AI Act on initial ALIGNER policy recommendations from September 2023

ALIGNER PR number	Brief Aim of ALIGNER PR	Assessed degree of AI Act impact on ALIGNER PR
1.	*'Ensuring consistency of P&LEA involvement with AI technology'*	**HIGH**
2.	*'EC to support P&LEAs with tailored legislation'*	**MEDIUM**
3.	*'EC to enable P&LEAs to transition to the use of AI systems'*	**HIGH**
4.	*'EC to clarify & harmonise the operation of the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) regarding P&LEA use of AI systems'*	**LOW**
5.	*'Retaining the human factor when P&LEAs utilise AI systems'*	**HIGH**
6.	*'Reflecting the need for P&LEA-focused research'*	**HIGH**

- The most clear-cut impact of the Act is on ALIGNER Policy Recommendation 5 (assessed as '**HIGH**') and where the focus is on retaining the human factor in the P&LEA use of AI systems. Through the provisions set out in the Act, it reinforces a strongly held requirement expressed on numerous occasions within the ALIGNER project that, from the perspective of policing and law enforcement, human beings should be central to any decision-making process based on the output of an AI system

  - In the four Articles below, the Act sets out how this 'human-centric' perspective will be achieved:

    Article 6: '*Rules for High Risk AI systems*'; "*…As a pre-requisite, AI should be a human-centric technology. It should serve as a tool for people, with the ultimate aim of increasing human well-being.*"

    Article 14: '*Human oversight*'**;** "*High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use."*

    Article 4: '*AI Literacy*'; "*Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf.*"

Article 3(42)(bh): '*AI literacy*'; "…*refers to skills, knowledge and understanding that allows providers, users and affected persons …to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause.*"[16]

- It was felt that retaining this ALIGNER Policy Recommendation would be beneficial as the requirements of the Act regarding 'AI literacy' will have many consequences and implications for P&LEAs. They extend from P&LEA processes for selecting and recruiting staff to their training, working practices, management and accountability

❖ On the other hand, it appears the Act could have the least impact on ALIGNER Policy Recommendation 4 (assessed as '**Low'**), which calls for a review of the barriers to P&LEA adoption of AI systems created by the lack of clarity in the requirements placed on them of the EU data protection framework. In essence, the General Data Protection Regulation (GDPRs) and the Law Enforcement Directive (LED) regarding P&LEA use of AI systems appear to be open to interpretation.

- Not unsurprisingly, the Act does not impact on this issue directly, but in the wider context of P&LEA adoption of AI systems, the issue has continued to be raised on a number of occasions within ALIGNER (but see the final bullet point below for a possible approach). It should therefore be retained as an ALIGNER policy recommendation

❖ The three remaining ALIGNER PRs will also undoubtedly be impacted upon by the AI Act and it has been categorized as having a '**HIGH**' impact on each one of them.

Policy Recommendation 1 (Assessed AI Act Impact category: **HIGH**)

Aim - 'Ensuring consistency of P&LEA involvement with AI technology'

Policy Recommendation 2 (Assessed AI Act Impact category: **HIGH**)

Aim - 'EC to support P&LEAs with tailored legislation'

Policy Recommendation 3 (Assessed AI Act Impact category: **HIGH**)

Aim - 'EC to enable P&LEAs to transition to the use of AI systems'

- How exactly the Act will impact is not yet clear as the important questions of how, when and with what consequences the Act will have on them, need to be explored and understood and studied carefully before accurate and detailed answers begin to emerge.

❖ Initially, further uncertainty for P&LEAs will be caused by the role of the 'AI Office', established in anticipation of the Act and with one of its functions being to "*contribute*

[16] It is assumed that the word 'users' equates to 'deployers'

to the implementation, monitoring and supervision of AI systems'. To achieve this, the AI Office is required to introduce specific Codes of Practice and Guidelines.

- The Codes of Practice and Guidelines are, as of now, yet-to-be devised, never mind implemented. Exactly what they will contain is not known and while the deadline for their production and approval by the Commission is set by Article 113 of the Act for May 2nd 2025, this will not occur until well after the completion of ALIGNER and should be taken up by Project STARLIGHT

- The existence and use of regulatory sandboxes to explore the impact and consequences of using AI systems in a closed environment that replicates the real world may well be helpful and supportive of ALIGNER policy recommendation 4 (Exploring EU data protection framework perceived barriers to AI system use by P&LEAs)

- Regulatory sandboxes used for these purposes could also impact on ALIGNER policy recommendation 6 (Reflecting the need for P&LEA-focused research). The ALIGNER deliverable D5.8 '*Research roadmap for AI in support of law enforcement and policing*' considers this issue in some detail. The aspect of guidance on what is and is not relevant for regulatory sandboxes should be discussed by P&LEAs with the AI Office

To conclude, the AI Act will impact, to a greater or lesser degree, on all of the existing ALIGNER policy recommendations. Similarly, these policy recommendations generally appear congruent with many of the provisions of the Act, and as ALIGNER has consistently tried to ensure that the policy recommendations that it has generated closely reflected the operational needs of P&LEAs, it is encouraging to see that there is no gaping chasm between them and this new key stone legislation.

It will be some time before the full ramifications of the Act are fully understood in the context of policing and law enforcement but it is already apparent from the initial ALIGNER impact assessment review that three new ALIGNER policy recommendations are required as a matter of priority. They are proposed, examined and explained in the following section.

3.3 Three new ALIGNER Policy Recommendations generated by the EU AI Act

The previous section focused on the sections of the AI Act that are of most relevance to policing and law enforcement and assessed their potential impact on each one of the ALIGNER Policy Recommendations. As a result of this assessment, all of the ALIGNER Policy Recommendations were re-formulated and re-written to take its results into account.

This next section arose as a direct result of carrying out the impact assessment described above as, in the course of carrying it out, it became clear that the introduction of new structures to implement, oversee and enforce the AI Act will have other, fundamental impacts on policing and law enforcement. Consequently, it was appropriate for ALIGNER to put forward new Policy Recommendations to reflect this fundamental shift. As with the original set of policy recommendations, the new policy recommendations have also been, as far as possible,*"…tailored to the operational needs of the law enforcement section…"* and are "*supported by [identified] capability gaps…"* [17]

The AI Act itself is one of a number of measures proposed by the Commission aimed at promoting the uptake of AI and addressing the risks associated with its use. It is designed to do this by "…*laying down harmonised rules on artificial intelligence…to foster the development, use and uptake of AI in the internal market*."[18] From a police and law enforcement perspective, there is a close focus in the Act on what types of AI systems they can or cannot use, depending on the risk category of the system and on the obligations and conditions that the Act dictates they must abide by if they are to lawfully deploy a permissible AI system.

In order to create the new policy recommendations, it was necessary to consider not just the EU AI Act itself but also a key piece of enabling legislation that preceded it, the "*Commission Decision of 24.1.2024 establishing the European Artificial Intelligence Office*". It was here that the first step was taken to establish the "European Artificial Intelligence Office" as part of the European Commission Directorate-General for Communication Networks, Content and Technology (DG CNECT).[19]

Article 3(42) of the AI Act itself defines the words "Artificial Intelligence Office" to mean "…the Commission's function of contributing to the implementation, monitoring and supervision of AI systems, general purpose AI models and AI governance." The AI Office will inevitably evolve over time and, for P&LEAs, it should become the nexus between policing and law enforcement issues arising at the operational and tactical levels concerning the use (and potential misuse) of AI systems, and the higher-level strategic issues of concern to the new "AI Board" that also impact on or are of relevance to P&LEAs. Consequently, it will come to have an important role to play from the perspective of the Commissions requirement for the ALIGNER policy recommendations to be "…tailored to the needs of the law enforcement sector".

The Commission Decision set out a number of tasks the AI Office will need to accomplish "*for the purposes of implementing and enforcing [the AI Act]*" (Article 2). The tasks of the AI Office of most importance from the perspective of policing and law enforcement are laid out in Article 3, where it states it will act in "*assisting the Commission in the preparation of guidance and guidelines to support the practical implementation of the forthcoming Regulation, as well as developing supportive tools, such as*

[17] Ibid. – ALIGNER Description of Work
[18] *Commission Decision* para 2.
[19] "*Commission Decision of 24.1.2024 establishing the European Artificial Intelligence Office*"

standardised protocols and best practices, in consultation with relevant Commission services and bodies, offices and agencies of the Union"[20] Additionally, it will "*coordinate the establishment of an effective governance system, including by preparing the set-up of advisory bodies at Union level…*" and in "*Encouraging and facilitating the drawing up of codes of practices and codes of conducts at Union level…[and] monitoring the implementation and evaluation of codes of practices.*"[21]

Article 4 requires the AI Office to cooperate with "*stakeholders*" and to consult with them regularly "*to collect input for the performance of its tasks under Article 3 (2)*", while Article 6 states that when pursuing its tasks, the AI Office "*shall establish the appropriate forms of cooperation with bodies, offices and agencies of the Union*." An important role for the AI Office that ensures that it sits at the crucial nexus between policy, strategy and operations in relation to the use of AI systems in the EU arises from its requirement to "*act as the Secretariat for the AI Board and its subgroups, providing administrative support to the advisory forum and scientific panel of independent experts, including organising meetings and preparing relevant documents.*"[22]

There is no doubt that the AI Office will benefit in its role by the establishment of a dynamic and on-going relationship with EU policing and law enforcement, and that it should begin as soon as possible. Each of the new ALIGNER policy recommendations presented below, along with its aim, rationale and some suggestions on how it could be achieved, is designed and put forward make a contribution to this.

THE NEW ALIGNER POLICY RECOMMENDATIONS

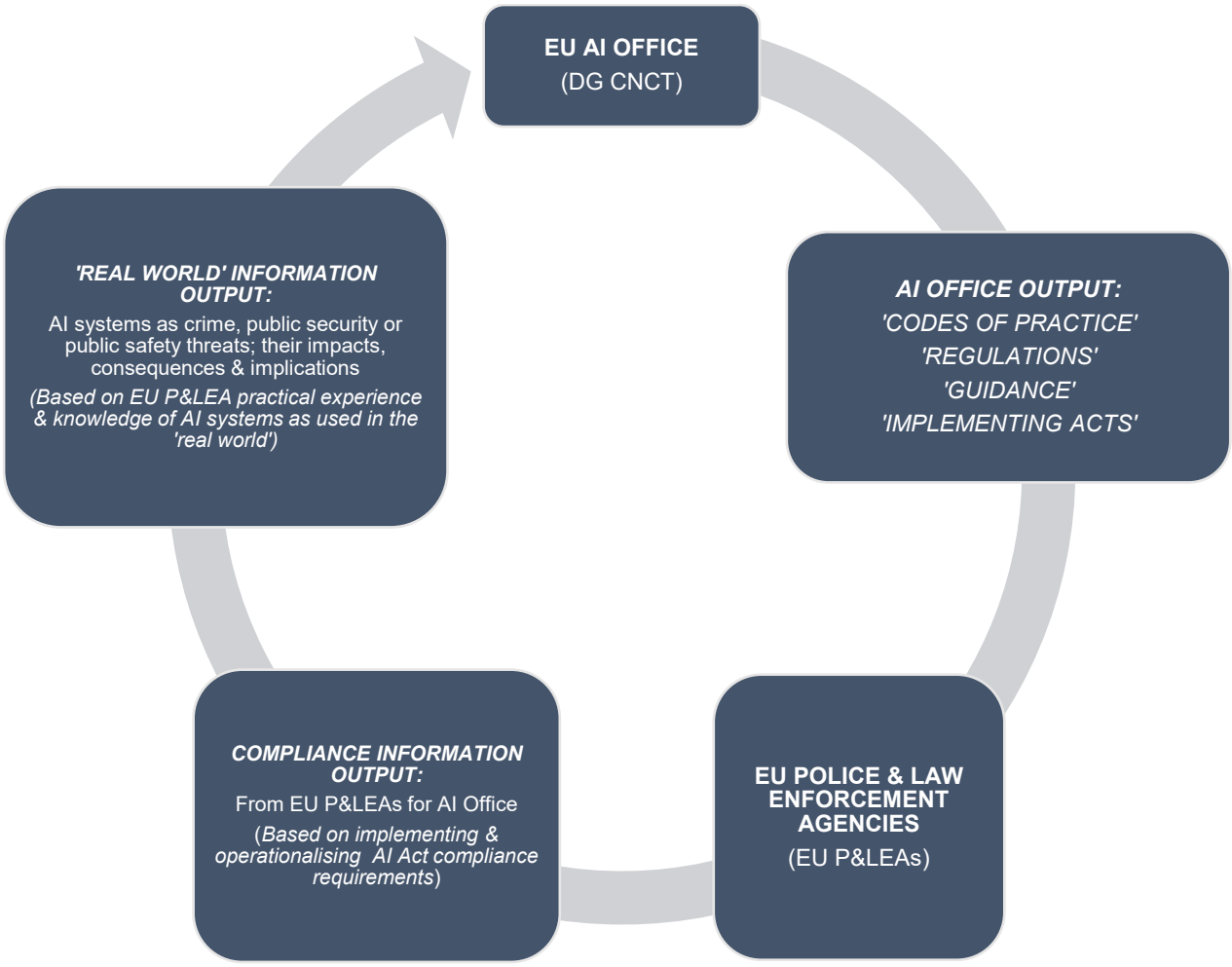
NEW ALIGNER POLICY RECOMMENDATION (1): CONCEPT

This first new policy recommendation is directly and specifically connected to the role of the AI Office, as it is set out by the Commission Decision and the AI Act. It relates to the desirability for EU police and law enforcement to have a regular means of input into the AI Office as it draws up the Codes of Practice, guidance and further implementing legislation (see Figure 3 below). It will require the setting up a mechanism for EU policing and law enforcement to communicate with the AI Office to discuss relevant issues on two levels; first, relating to regulatory compliance and technical issues under the AI Act, as they begin arise as EU P&LEAs start to plan for and then implement its provisions.

Second, EU P&LEAs communications with the AI Office should also encompass a broader output from them of knowledge and experience they have gained from operating in the real-world where AI systems are already being used to generate crime and public security threats. This kind of information on AI systems will enable the AI Office to put into context and better consider the implications of any legislation-specific issues it may have under consideration as a result of its role to monitor and regulate the implementation of the AI Act. This two-level approach to the gathering and communicating of information relating to AI systems, plus the ways they are used and abused to create crime and security threats, will be of mutual benefit of both parties.

[20] Commission Directive Article 3, 2(c)
[21] Commission Directive Article 3, 2(g) and 2(i)
[22] Commission Directive Article 3, 2(h)

Figure 3 – Suggested strategic communication concept to apply between the EU AI Office and EU Police and Law Enforcement Agencies



NEW ALIGNER POLICY RECOMMENDATION (1)

ALIGNER - New Policy Recommendation (1): (Created post-AI Act, September 2024)
The EU Commission, through its European Artificial Intelligence Office, should establish a constructive partnership with EU police and law enforcement agencies to ensure that compliance issues can be prevented or resolved, guidance and best practices can be identified, and lessons can be learned

*This new PR should be treated as a **HIGH PRIORITY** due to the short time remaining for P&LEAs to input into the first Code of Practice (required by Article 113 of the Act to be ready by May 2025)*

Aim of new Policy Recommendation (1)

To ensure the AI Office recognizes and engages with the 'EU policing and law enforcement' community as a *'stakeholder'* under Article 4 of the Decision in order to both integrate the P&LEA community into the governance system of the AI Act and to create a clear path for communication over and above the reporting channels required by the compliance regime for 'high-risk' AI systems under the AI Act

Rationale for new Policy Recommendation (1)

- The AI Act calls for the Commission to "*develop guidelines on the practical implementation of this Act*" and, at the request of the Member States or the AI Office, or on its own initiative, "*…the Commission shall update guidelines previously adopted when deemed necessary.*"[23] Among the functions of the AI Office are those that aim at "*assisting the Commission in the preparation of guidance and guidelines to support the practical implementation of the forthcoming Regulation, as well as developing supportive tools, such as standardised protocols and best practices, in consultation with relevant Commission services and bodies, offices and agencies of the Union*"[24]
- Moreover, a task of the AI Office is to "*encourage and facilitate the drawing up of codes of practices and codes of conduct at Union level, taking into account international approaches, as well as monitoring the implementation and evaluation of codes of practices."*[25]
- The AI Act states that the AI Office can invite other bodies to contribute to the drawing up of the Codes and who will act to support the AI Office. They could include in support of the process "*Civil society organisations, industry academia and other relevant stakeholders such as downstream providers and independent experts*"[26]
- Article 4 of the Commission Decision states that the AI Office shall cooperate with stakeholders, by "*conducting regular consultation of stakeholder, including experts from the scientific community and the education sector, citizens, civil society and social partners, where relevant, to collect input for the performance of its tasks*"[27]
- As part of its task of "*assisting the Commission in the preparation of guidance and guidelines to support the practical implementation of the [AI Act]",* the AI Office would benefit if was regularly updated on the collective experiences and knowledge of EU police and law enforcement agencies relating to the impact that the new compliance regimes under the AI Act are having 'on the ground'.[28]
- The role of the AI Office relating to the Codes of Practice states "*The Commission may give general EU validity to a code of practice through implementing acts*", or "*it may provide common rules for implementation through implementing acts.*" The drafting of implementing acts is another element where consultation between the AI Office and EU police and law enforcement would be desirable in order to advise the Commission. This is likely to be a continuous function under the Act and not just confined to the initial implementation period of the Act.[29]
- In the light of these requirements and their implications, a strong case can be argued for the AI Office to put in place arrangements to consult with P&LEAs regularly and consistently. It can be

[23] AI Act, Article 96: *Guidelines from the Commission on the Implementation of this Regulation*
[24] Commission Decision Article 3(2)(c))
[25] Commission Decision Article 3, 2(i)
[26] AI Act, Article 56: Codes of Practice, para. 3
[27] Commission Decision of 24.1.2024
[28] Commission Decision Article 3, 2(c)
[29] AI Act, Article 56: Codes of Practice

envisaged that the need for information to flow from EU police and law enforcement to the AI Office and beyond will be a long-standing and continuous one in order to keep pace with new developments under the AI Act, and the external use and abuse of AI systems that will undoubtedly continue to evolve

How could new Policy Recommendation (1) be implemented?

- Now that the EU AI Office has been established, the AI Office task of creating the Codes of Practice for AI systems, as required under Article 56 of the EU AI Act, should now be underway as they are scheduled to come into effect by of August 2nd 2025.[30]
- EU police and law enforcement should be asked to contribute to the process of drawing up the new Codes of Practice, particularly where they will impact on their duties and responsibilities
- Consultation at an early stage between the AI Office and police and law enforcement agency representatives over implementation issues, legislation, guidance, best practices and the Codes of Practice would be beneficial from both their perspectives
- The AI Office should designate the EU police and law enforcement community as a '*stakeholder*' under the AI Act system of governance, followed by consultation at an early stage between representatives over the Codes of Practice and other potential guidance and implementing acts
- Given the circumstances outlined above and taking into account the short timescale for the AI Office to prepare the Codes of Practice, the EU Innovation Hub at Europol could become the initial point of contact and act as a conduit between the AI Office and the national police and law enforcement agencies of each Member State, unless and until other arrangements are put in place.
- While Frontex (for Border guards), Eurojust (for public prosecutors) and CEPOL (for law enforcement training) participate in the Innovation hub, individual arrangements with each of them could also be explored.
- The AI Office is tasked to act to "*conduct evaluations and reviews on and preparing reports related to [the AI Act]*"[31]
- Moreover, the AI Office is tasked to establish a governance framework for the AI Act that would "*coordinate the establishment of an effective governance system, including by preparing the set-up of advisory bodies at Union level…*"[32]
- The AI Act makes provisions to establish an AI Board consisting of representatives from the Member States (which the AI Office will attend and also act as its Secretariat); a Scientific Panel to integrate the scientific community and; an Advisory Forum to contribute stakeholder input to the implementation of the Act at Union and national level.[33]
- An argument can be made that there is a need to establish a dynamic 'stakeholder' relationship between the AI Office and the EU police and law enforcement community, as the insights and guidance they can offer can be channelled through it to provide inputs and advice to the Advisory Board, Advisory Forum and relevant sub-groups that may be created. The information would be qualitatively different to that required under the Codes of Practice or compliance requirements.
- By doing this, the Commission would benefit from the insights gained from the practical experience of EU police and law enforcement agencies when applying the provisions of the AI Act to AI systems in use in the real world.

[30] As set out in the AI Act, Article 113: Entry into force and Application
[31] Commission Directive Article 3, 2(f)
[32] Commission Directive Article 3, 2(g)
[33] AI Act, Article 65: Establishment structure of the European Artificial Intelligence Board and Article 67: Advisory Forum

NEW ALIGNER POLICY RECOMMENDATION (2)

The second new ALIGNER policy recommendation arises from the specific wording of the AI Act under Article 5. In their current form, it would be very challenging for any P&LEA to justify in a clear and accurate way why the operational circumstances they are dealing with in response to the threat of a terrorist attack creates the necessity for them to deploy a remote biometric identification AI system. This issue should be rectified as a matter of importance, and certainly in advance of this provision of Article 5 being applied to real-world situations.

ALIGNER - New Policy Recommendation (2): (Created post-AI Act, September 2024)

The Artificial Intelligence Office should work with DG HOME and Europol to ensure that the meaning of the phrase in Article 5 referring to "a genuine and present or foreseeable threat of a terrorist attack" is clarified

Aim of new Policy Recommendation (2)

To ensure that the AI Office works with DG HOME and Europol to provide further guidance and standardise the practical criteria of 'credibility' and 'likelihood' that P&LEAs need to work with when assessing the threat of a terrorist attack so that P&LEAs can utilise a real time remote biometric identification AI system in response to it

Rationale for new Policy Recommendation (2)

- The wording of Article 5 sets out a requirement for P&LEAs to demonstrate the necessity for them to utilise a real time remote biometric identification system for "*the prevention of… a genuine and present or genuine and foreseeable threat of a terrorist attack"*. They must also ensure they meet all the other requirements of the Act, as described previously on p.28.
- The use in the AI Act of the words '*genuine*', '*present*' and '*foreseeable*' to describe the type of terrorist attack P&LEAs may be seeking to forestall is problematic. They are too unspecific, too subjective and are open to interpretation. It is for this reason that they are not found in any tried-and-tested lexicon of terrorist threat assessment methodologies and therefore, they are not the appropriate criteria for P&LEAs to apply to demonstrate their compliance with the AI Act in these circumstances.
- The aim of any assessment of the threat of a terrorist attack is to aid in determining what the risk of the attack may be and consequently, what actions may be required to prevent it from happening. Therefore, the threat assessment it is based on any relevant information that can be gathered and evaluated prior to the attack being launched.
- Any information gathered must first be evaluated in two ways, by grading the reliability of its source and by grading the reliability of the information itself. For example, source grades can range from 'Reliable' (Grade A), to 'Cannot be judged' (Grade F) while information grades range from 'Confirmed' (Grade 1), to 'Cannot be judged' (Grade 6).[34]
- Once the reliability of the information has been quantified, the assessment of the specific threat of a terrorist attack requires the careful examination of two critical factors;
    - Whether the threat of the terrorist attack is credible or not, and;
    - If the threat of the terrorist attack is a credible one, what is the probability of it occurring?

[34] Each of the grades will have its own definition as a means to assist in the grading process

- ❖ In the context of security threat assessments;
  - A 'credible' threat is where an adversary is assessed as having both the intent and the capability to carry out the threat. If either of these two factors is absent, then the threat may still be present but at a reduced level.
  - The 'probability' (likelihood) of a threat can be plotted onto a scale, generally spanning from 'Rare or remote', through 'Unlikely', 'Credible' and 'Likely', to 'Almost certain'. Each one can have its own accepted definition in the context of terrorist threats and security responses.[35]
- ❖ If need for the use of criteria such as described above is accepted by the AI Office as the right approach for P&LEAs to take, there is then a need for standardisation of the degrees of 'credibility' and 'probability' that P&LEAs must demonstrate in order to be able to use this type of AI system in any response to the threat of a terrorist attack. This should be achieved as soon as possible.

NEW ALIGNER POLICY RECOMMENDATION (3): CONCEPT

The third new ALIGNER policy recommendation focuses on a specific opportunity, generated by the AI Act itself, to put into place a mechanism that ensures EU P&LEAs have access to current and accurate information relating to any other P&LEA deployers of 'High Risk' AI systems. This information will already be part of the database established under the Act, *Chapter VIII: EU database for High-Risk AI systems listed in Annex III (Article 71)*, which is designed to enable the EU Commission to keep track of the implementation of the AI Act and to enforce compliance with it through fines if necessary.

For example, by using it in the way envisaged, an EU P&LEA wishing to explore the option of procuring an AI system for law enforcement purposes can easily discover what types of 'High Risk' AI systems are already being utilised in the EU for law enforcement purposes, in which Member State they are located, what particular organization is deploying them and for what purpose, plus and who in the organisation is the official EU Commission point of contact to deal with AI system issues.

Article 71(4) states that "*the information registered in accordance with Article 60 shall be accessible only to market surveillance authorities and the Commission, unless the prospective provider or provider has given consent for also making the information accessible the public*." However, an argument can be made for the Commission to set up a specific section or access to the Register allowing EU P&LEAs to voluntarily share this information with other EU P&LEAs. If this was put into place, it would facilitate communications and information sharing between EU P&LEAs on their experiences during the procurement, management and operations of 'high risk' AI systems.

[35] As an example, the UK intelligence assessment community uses a 'Probability Yardstick', originally devised by 'Defence Intelligence', and based on a scale of probability using a "shared vocabulary of likelihood". It commences with a 'Remote chance', then to 'Highly unlikely', 'Unlikely' 'Realistic possibility', 'Likely or probable', 'Highly likely' and ending with 'Almost certain'. Percentages and ratios are also assigned to each category for use if required.
https://www.gov.uk/government/news/defence-intelligence-communicating-probability
(Accessed 4.9.24)

NEW ALIGNER POLICY RECOMMENDATION (3)

ALIGNER - New Policy Recommendation (3): (Created post-AI Act, September 2024)

The Artificial Intelligence Office should ensure the EU Database for High-Risk AI Systems, designed to contain detailed information on all EU P&LEAs deploying these AI systems, can be utilised also by EU P&LEAs to discover what EU P&LEAs are operating what system and where, plus who they can contact directly to discuss relevant issues, exchange knowledge and share experiences of AI system procurement and operation

Aim of new Policy Recommendation (3)

To ensure the AI Office facilitates the exchange of relevant experiences and information on 'high risk' AI systems by enabling the EU P&LEA community to identify and contact the appropriate representative of any other EU P&LEA that already are deployers of the same type of AI system

Rationale for new Policy Recommendation (3)

- ALIGNER have already identified there is a need for EU support to EU P&LEAs in this area and have encapsulated it into one of its original Policy Recommendations (see below):

  ALIGNER Policy Recommendation 1 (Final iteration post-AI Act, September 2024)

  > *"By utilising the provisions and requirements of the AI Act, the AI Office and DG HOME to ensure that the procurement, utilisation or in-service development of AI systems by P&LEAs is carried out in a consistent way that takes full account of their obligations towards fundamental human rights"*

- The AI Act contains provisions that build a solid legislative foundation on which this new policy recommendation can be achieved and maintained into the future
- Article 71: *EU Database for High-Risk AI Systems Listed in Annex III* states "…*the Commission shall, in collaboration with the Member States, set up and maintain an EU database containing information … concerning high-risk AI systems.*"
- Annex VIII: *Information to be Submitted upon the Registration of High-Risk AI Systems* states *"The data listed in Section C of Annex VIII shall be entered into the EU database by the deployer who is…a public authority, agency or body"* and that *"For high-risk AI systems …in the areas of law enforcement, migration, asylum and border control management, the registration …shall be in a secure non-public section of the EU database referred to in Article 71"*

How could new Policy Recommendation (3) be implemented?

- The AI Act has a provision under Chapter VIII, Article 71 for the creation of an EU database of 'High-Risk' AI systems that are listed under Annex III of the Act. The types of system listed of most relevance to EU P&LEAs are those used for:
  - Law enforcement

    - Migration
    - Biometrics
    - Employment
    - Access to public services
    - Justice and democracy
- Annex VIII, Section C – Information to be submitted by deployers of high-risk AI systems in accordance with Article 49(3), requires the deployer to provide and keep updated the following information:
    - ❖ The name, address and contact details of the deployer
    - ❖ The name, address and contact details of the person submitting information on behalf of the deployer
    - ❖ The URL of the entry of the AI system in the EU database by its provider
    - ❖ A summary of the findings of the fundamental rights impact assessment conducted in accordance with Article 27
    - ❖ A summary of the data protection impact assessment carried out in accordance with Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680 as specified in Article 26(8) of this Regulation, where applicable
- A mechanism should be established to enable the information detailed above to be released to an appropriate employee of a police or law enforcement agency for purposes of researching their organisations capability needs, potential procurement process, development or operational issues relating to high-risk AI systems

To conclude this section on the three newly generated ALIGNER policy recommendations, now that the AI Act has become a significant feature of the laws that European police and law enforcement agencies must comply with and operate AI system under, it is clear that the Act only addresses one dimension of the dual nature of AI systems considered during ALIGNER; where they are used in the service of P&LEAs. While the scope of the AI Act does not include countering the malicious use of AI systems, it does take cogniscance of some AI system misuse in the real world e.g. it defines 'deepfake' under Article 3, (60).

In addition, AI system capabilities have now expanded to encompass audio 'deepfakes' of human voices and image 'deepfakes' of human faces and bodies that can be presented as photographs or film footage from 'real life'. Consequently, and perhaps inevitably, AI system-produced deep fakes are now widely-used used as an integral part of creating misinformation, disinformation and malicious deceptions.

AI systems are already being used in criminal or malicious ways, generating adverse impacts and unforeseen consequences for individuals, communities and societies and consequently, they already present a continuing series of challenges for policing, law enforcement and criminal justice systems.

Examples of how this occurs range from AI systems being used to facilitate acts of fraud and deception (as outlined in some of the scenarios explored by ALIGNER) and in at least one known case, the generation and proliferation of Child Sexual Abuse Material (CSAM) that became included as an integral part of an open-source database of images that was used to train a number of AI systems.[36]

[36] 'Can AI image generators be policed to prevent explicit deepfakes of children?' Alex Hern, 23.4.24, *Guardian* https://www.theguardian.com/technology/2024/apr/23/can-ai-image-generators-be-policed-to-prevent-explicit-deepfakes-of-children Accessed: 19.7.24

The scale of public availability of AI systems has increased enormously since ChatGPT first appeared in November 2023. The complexity and scale of problems generated by public use of AI systems are already apparent and surely the new AI Office will require an awareness of issues of this type. This is where EU police and law enforcement can support them with information, facts and evidence. Issues such as those outlined were considered when assessing the impact of the AI Act on the ALIGNER Policy Recommendations and in the subsequent decision to add three new ones to them.

4. The third and final iteration of the ALIGNER Policy Recommendations

4.1 The third iteration of the ALIGNER Policy Recommendations (Final set)

The ALIGNER Policy Recommendations have evolved systematically over the full timescale of Project ALIGNER, with the first iteration of them published as deliverable D2.3 on September 30th 2022. The second iteration, D2.4, was published on September 30th 2023 after they had all been subjected to a cross-project comparison and been revised in consequence. Shortly afterwards, on November 30th 2023, an AI-technology advance equivalent of the astronomical "Big Bang" occurred when ChatGPT was first released to the public.

Since that date, many events and circumstances of great relevance to policing and law enforcement as it relates to their involvement with AI systems have occurred. They included the technological advancements of AI system technology itself, as 'generative AI' (now known as 'General purpose AI'), became the 'new normal'. Very quickly, the numbers of companies who became providers of these systems increased dramatically and, in some cases, they released AI systems to the public as 'open-source' versions that purchasers could be adapt and modify as they wished.

However, this was not all. This event rapidly led both to the current wide-spread use (and the beginnings of the abuse) of publicly available AI systems and to the attempts made internationally to introduce effective methods of governance and to develop suitable 'guard-rails' for AI technology. The EU contributed to setting these governance measures and brought to fruition its' long-awaited Artificial Intelligence Act, coming into force as European Union law as of August 1st 2024.

The role of the ALIGNER Advisory Boards in the Policy Recommendation process

As an integral part of ALIGNER, two expert Advisory Boards (ABs) were formed as soon as the project commenced; the Law Enforcement Agency Advisory Board (LEAAB) and the Scientific, Industrial and Ethical Advisory Board (SIEAB). These Advisory Boards provided a mechanism to access the experience and technical expertise held by their members. At each workshop, in addition to the Advisory Board participants were ALIGNER project consortium members and selected other participants invited to attend the workshops. Taken together, this arrangement helped to ensure that the policy recommendations were *"...tailored to the operational needs of the law enforcement sector..."*

Over the lifespan of the Project and as the Policy Recommendations were devised, refined and amended, the Advisory Boards were also used as a 'sounding board' for each of their iterations. The draft version of each iteration was presented for their comments and suggestions before it was published. On September 25th, 2024 Project ALIGNER held its Final Event/Workshop 8 in Brussels. Participants attended in person and on-line and included 26 members of the two Advisory Boards.

The consultation process with the Advisory Boards outlined above was followed as before, with an initial draft of all of Section 3 of this latest and last iteration of the Policy Recommendations being sent to just over 50 members of the two Advisory Boards for their thoughts and comments. Responses were made both in advance and during the session on the day dedicated to "ALIGNER's Research and policy recommendations".

The overall discussions and comments on the new and policy recommendations were positive and supportive and led to only a few minor changes, mainly presentational, to the final set of the ALIGNER policy recommendations contained in this document.

The final set of policy recommendations, plus the individual aim of each one, are listed here in two parts. The three new ALIGNER policy recommendations, created as a direct consequence of the AI Act legislation, are shown in Part One. They are followed in Part Two by the six policy recommendations that were amended and revised following the recent ALIGNER AI Act impact assessment. All nine of them are summarised below:

PART ONE - NEW ALIGNER POLICY RECOMMENDATIONS (As generated directly by the AI Act, September 2024)

ALIGNER new policy recommendation (1)

*This newPR should be considered a **HIGH PRIORITY** due to the short time remaining for inputs into the first Code of Practice (required by the AI Act to be ready by May 2025)*

ALIGNER - New Policy Recommendation (1): (Created post-AI Act, September 2024)

The EU Commission, through its European Artificial Intelligence Office, should establish a constructive partnership with EU police and law enforcement agencies to ensure that compliance issues can be prevented or resolved, guidance and best practices can be identified, and lessons can be learned

Aim of new Policy Recommendation (1)

To ensure the AI Office recognizes and engages with the 'EU policing and law enforcement' community as a *'stakeholder'* under Article 4 of the Decision in order to both integrate the P&LEA community into the governance system of the AI Act and to create a clear path for communication over and above the reporting channels required by the compliance regime for 'high-risk' AI systems under the AI Act

ALIGNER new policy recommendation (2)

ALIGNER - New Policy Recommendation (2): (Created post-AI Act, September 2024)

The Artificial Intelligence Office should work with DG HOME and Europol to ensure that the meaning of the phrase in Article 5 referring to "a genuine and present or foreseeable threat of a terrorist attack" is clarified

Aim of new Policy Recommendation (2)

To ensure that the AI Office works with DG HOME and Europol to provide further guidance and standardise the practical criteria of 'credibility' and 'likelihood' that P&LEAs need to work with when assessing the threat of a terrorist attack so that P&LEAs can utilise a real time remote biometric identification AI system in response to it

ALIGNER new policy recommendation (3)

ALIGNER - New Policy Recommendation (3): (Created post-AI Act, September 2024)
The Artificial Intelligence Office should ensure the EU Database for High-Risk AI Systems, designed to contain detailed information on all EU P&LEAs deploying these AI systems, can be utilised also by EU P&LEAs to discover what EU P&LEAs are operating what system and where, plus who they can contact directly to discuss relevant issues, exchange knowledge and share experiences of AI system procurement and operation

Aim of new Policy Recommendation (3)

To ensure the AI Office recognizes and works with the 'EU policing and law enforcement' community to ensure that EU P&LEAs who wish to adopt AI system technologies for use within their own organisations can be put into contact with appropriate representatives of other EU P&LEAs that already have become deployers of the same type of AI system in order to exchange relevant experiences and information

PART TWO – FINAL EXISTING ALIGNER POLICY RECOMMENDATIONS (As revised in the light of the AI Act, September 2024)

ALIGNER Policy Recommendation 1: Final iteration

ALIGNER: Policy Recommendation 1 (Final iteration post-AI Act, September 2024)
By utilising the provisions and requirements of the AI Act, the AI Office and DG HOME to ensure that the procurement, utilisation or in-service development of AI systems by P&LEAs is carried out in a consistent way that takes full account of their obligations towards fundamental human rights

Aim of revised Policy Recommendation 1

To ensure that consistent approaches will be taken by P&LEAs across all aspects of their involvement with AI systems.

ALIGNER Policy Recommendation 2: Final iteration

ALIGNER: Policy Recommendation 2 (Final iteration post-AI Act, September 2024)
Building on the foundation of the AI Act, the European Commission should continue to develop its' legislative framework for AI systems so that the P&LEAs of Member States can utilise it to guide and support their selection, acquisition and use of AI systems

Aim of revised Policy Recommendation 2

To ensure the EU supports P&LEAs in their selection and use of AI systems by continuing to develop a legislative framework designed to achieve this.

ALIGNER Policy Recommendation 3: Final iteration

ALIGNER: Policy Recommendation 3 (Final iteration post-AI Act, September 2024)
The EU should guide and support the P&LEAs of Member States to incorporate into their technology base the lawful and appropriate AI systems that are currently available or are already foreseeable on the near horizon

Aim of revised Policy Recommendation 3

To guide and support P&LEAs to make the transition into adopting and using effective, safe and lawful AI systems

ALIGNER Policy Recommendation 4: Final iteration

ALIGNER: Policy Recommendation 4 (Final iteration post-AI Act, September 2024)
The EU to instigate a review of the EU data protection framework as it relates to the nexus between 'real-world' data and P&LEA functions and operations and their potential use of AI systems to access and process it. Currently, aspects of it are perceived as a potential barrier to the procurement and use of AI systems by P&LEAs

Aim of revised Policy Recommendation 4

To see if there are barriers for P&LEAs to adopting and using AI systems that are created by the lack of clarity in the EU data protection framework and if so, suggest how they could be mitigated

ALIGNER Policy Recommendation 5: Final iteration

ALIGNER: Policy Recommendation 5 (Final iteration post-AI Act, September 2024)
DG HOME to work in conjunction with Europol and CEPOL to embed into EU police and law enforcement training and learning the concepts of 'AI Literacy' and a 'human-centric approach' to AI systems (Article 4 and Article 1 of the AI Act) and including their impacts, consequences and implications for P&LEAs

Aim of revised Policy Recommendation 5

To ensure EU P&LEAs are fully aware of the requirements generated by the concepts of 'AI literacy' and a 'human-centric approach' when utilising AI systems for the purposes of law enforcement

ALIGNER Policy Recommendation 6: Final iteration

ALIGNER: Policy Recommendation 6 (Final iteration post-AI Act, September 2024)
To urge the EU to conduct and facilitate systematic and regular research into AI systems, both as solutions and as threats, that are tailored to the needs of P&LEAs and can be delivered within realistic timeframes

Aim of revised Policy Recommendation 6

To encourage AI system-focused research whose results will be of practical use to P&LEAs and are deliverable within realistic timeframes

N.B. - It should be noted that ALIGNER deliverable D5.8 expands on and covers in more detail the Research Recommendations and suggestions of the project

4.2 ALIGNER Policy Recommendations: Summary table of the Final Set

The three new ALIGNER Policy Recommendations derived as a direct consequence of the impact assessment review of the AI Act in 2024 have been amalgamated with the third iteration of the six Policy Recommendations from 2024, after they had also been revised and updated after the impact review. All nine of the ALIGNER Policy Recommendations are shown in Table 12 below:

Table 12 – The final set of the ALIGNER Policy Recommendations

ALIGNER POLICY RECOMMENDATIONS: FINAL ITERATION
ALIGNER - New Policy Recommendation (1) **(Created post-AI Act impact assessment, September 2024)**
The EU Commission, through its European Artificial Intelligence Office, should establish a constructive partnership with EU police and law enforcement agencies to ensure that compliance issues can be prevented or resolved, guidance and best practices can be identified, and lessons can be learned
ALIGNER - New Policy Recommendation (2) **(Created post-AI Act impact assessment, September 2024)**
The Artificial Intelligence Office should work with DG HOME and Europol to ensure that the meaning of the phrase in Article 5 referring to "a genuine and present or foreseeable threat of a terrorist attack" is clarified
ALIGNER - New Policy Recommendation (3) **(Created post-AI Act impact assessment, September 2024)**
The Artificial Intelligence Office should ensure the EU Database for High-Risk AI Systems established by Chapter VIII, Article 71 as a central pool of information containing details of the deployers of these AI systems can be utilized by EU P&LEAs, including who they can contact to discuss their experiences of its procurement, operations and other matters of mutual interest
ALIGNER: Policy Recommendation 1 **(Final iteration after AI Act impact assessment, September 2024)**
By utilising the provisions and requirements of the AI Act, the AI Office and DG HOME to ensure that the procurement, utilisation or in-service development of AI systems by P&LEAs is carried out in a consistent way that takes full account of their obligations towards fundamental human rights
ALIGNER: Policy Recommendation 2 **(Final iteration after AI Act impact assessment, September 2024)**
Building on the foundation of the AI Act, the European Commission should continue to develop its' legislative framework for AI systems so that the P&LEAs of Member

States can utilise it to guide and support their selection, acquisition and use of AI systems

ALIGNER: Policy Recommendation 3

(Final iteration after AI Act impact assessment, September 2024)

The EU should guide and support the P&LEAs of Member States to incorporate into their technology base the lawful and appropriate AI systems that are currently available or are already foreseeable on the near horizon

ALIGNER: Policy Recommendation 4

(Final iteration after AI Act impact assessment, September 2024)

The EU to instigate a review of the EU data protection framework as it relates to the nexus between 'real-world' data and P&LEA functions and operations and their potential use of AI systems to access and process it. Currently, aspects of it are perceived as a potential barrier to the procurement and use of AI systems by P&LEAs

ALIGNER: Policy Recommendation 5

(Final iteration after AI Act impact assessment, September 2024)

DG HOME to work in conjunction with Europol and CEPOL to embed into EU police and law enforcement training and learning the concepts of 'AI Literacy' and a 'human-centric approach' to AI systems (Article 4 and Article 1 of the AI Act) and including their impacts, consequences and implications for P&LEAs

ALIGNER: Policy Recommendation 6

(Final iteration after AI Act impact assessment, September 2024)

To urge the EU to conduct and facilitate systematic and regular research into AI systems, both as solutions and as threats, that are tailored to the needs of P&LEAs and can be delivered within realistic timeframes

5. Conclusion

"A technological singularity is a point where our old models must be discarded and a new reality rules"[37]

Whether the recent technological development in AI systems becomes accepted or not as a "*technological singularity*" remains to be seen, but at this stage and from the perspective of policing and law enforcement in the European Union, a point has been reached where "*our old models must be discarded and a new reality rules*". This has now become a certainty for P&LEAs. It is driven not only by the rapid increase of AI systems in the public domain and the problematic uses to which they can now be put, but also by another direct consequence of the arrival of AI systems; the passage into law of the EU Artificial Intelligence Act.

Since the commencement of Project ALIGNER, AI systems in general have dramatically changed from being viewed as a frontier technology of most interest to its exponents, to being almost universally accessible to people globally through both computers and increasingly, mobile phones. In the context of policing and law enforcement, this combination of technological innovation and the capabilities it brings has additionally led to a rapidly advancing wave of their malicious use and the creation of new crime and security threats. The irony of this is that it has in turn, contributed to the demand for P&LEAs to improve their own effectiveness and to do so by incorporating the capabilities of AI systems into their day-to-day operations.

In the near future, the AI Act will start to govern how P&LEAs interact with and utilise AI systems to carry out their duties and responsibilities but in the meantime, there is a narrow window of opportunity for P&LEAs to work in conjunction with the new AI Office to make sure that the way the Act is interpreted and enforced strikes an acceptable balance between innovations that are "*tailored to the operational needs of P&LEAs*" in order to increase their effectiveness, and the obligations and conditions placed on P&LEAs to ensure that their use of AI systems is always in compliance with the Act.

Project ALIGNER has been in the fortunate position over the last three years of being able to devise, revise and validate a robust set of policy recommendations relating to AI systems that draw on contemporary knowledge, current events and circumstances to bring benefits to the challenges policing and law enforcement agencies face. They were initially shaped by examining the past and the present and trying to forsee the future, but now, more importantly, they can be put forward as a means to develop solutions oriented to both the present and the future.

Experience has now shown us that what the future may hold in terms of AI systems may often be uncertain until it arrives (think 'general purpose AI'), but when they come fully into operation from August 2025 onwards, the provisions of the AI Act will provide a good degree of certainty for EU P&LEAs to plan for and to work with.

What is also certain is that circumstances will almost inevitably change, and in turn, P&LEAs and legislators who are concerned with the use and impact of AI systems on society must change as well if the solutions that they need to continue to provide are to remain relevant and effective.

[37] Vernor Vinge, Mathematician, Computer scientist & Science-fiction author (1944-2024)

6. References

ALIGNER Description of Work, Annex 1 (part A) Coordination and support action, 06/04/2021

“Commission Decision of 24.1.2024 establishing the European Artificial Intelligence Office”

‘Can AI image generators be policed to prevent explicit deepfakes of children?’ Alex Hern, 23.4.24, Guardian, https://www.theguardian.com/technology/2024/apr/23/can-ai-image-generators-be-policed-to-prevent-explicit-deepfakes-of-children, Accessed: 19.7.24

EU Artificial Intelligence Act, 19.4.2024, available at https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf

European Commission (2021). 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, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 , Accessed 18.8.2023

Glaser, B. and Strauss, A. (1967) The Discovery of Grounded Theory: Strategies for qualitative research. London: Transaction.

Strauss, A. & Corbin, J. (1994), Grounded Theory Methodology: An Overview. In N. Denzin & Y. Lincoln Handbook of Qualitative Research. 1st ed. (pp 273-284)

UK intelligence ‘Probability Yardstick’ (Defence Intelligence), available at https://www.gov.uk/government/news/defence-intelligence-communicating-probability, Accessed 4.9.2024

Warnes, R. (2009) Grounded Theory. In Ling, T. & Villalba van Dijk, L. Performance Audit Handbook: Routes to Effective Evaluation. Santa Monica, Rand Corporation)

ANNEX A

EU Artificial Intelligence Act: A reference guide to its contents'

(Drawn from https://artificialintelligenceact.eu)

The EU AI Act consists of 13 Chapter titles, each of which contains its own set of Articles. There are 113 Articles in total and in addition, there are 13 additional Annexes. These have been compiled here into the form of a 'Table of Contents' as a guide to the Act It is not a format used in the Act itself.

Chapter I: General Provisions

Article 1: Subject Matter

Article 2: Scope

Article 3: Definitions

Article 4: AI literacy

Chapter II: Prohibited Artificial Intelligence Practices

Article 5: Prohibited Artificial Intelligence Practices

Chapter III: High-Risk AI System

Section 1: Classification of AI Systems as High-Risk

Article 6: Classification Rules for High-Risk AI Systems

Article 7: Amendments to Annex III

Section 2: Requirements for High-Risk AI Systems

Article 8: Compliance with the Requirements

Article 9: Risk Management System

Article 10: Data and Data Governance

Article 11: Technical Documentation

Article 12: Record-Keeping

Article 13: Transparency and Provision of Information to Deployers

Article 14: Human Oversight

Article 15: Accuracy, Robustness and Cybersecurity

Section 3: Obligations of Providers and Deployers of High-Risk AI Systems and Other Parties

Article 16: Obligations of Providers of High-Risk AI Systems

Article 17: Quality Management System

Article 18: Documentation Keeping

Article 19: Automatically Generated Logs

Annexes

ANNEX B – Summary of the 'Over-arching categories' and 'Areas of Concern' arising from ALIGNER Workshops 1-3

Below can be found the data derived from the Grounded Theory analysis of the summarised data drawn from each of the first three ALIGNER workshops (see deliverable D2.3, Section 3, 'Methodology and Approach' for details). The end result was forty-four 'areas of concern' and capability needs relating to AI technology in the context of policing and law enforcement. From these, six over-arching categories can be discerned. To ensure clarity, these six are shown below first, followed by the headings for all forty-four of the 'areas of concern' and capability needs. In only two cases here is the heading accompanied by its associated text summary. Each one of the 'areas of concern ' has been assigned to one of the six over-arching categories. The Workshop(s) where the topic arose or was discussed are indicated by a code e.g. WS 1 is Workshop 1 etc.

The six over-arching ALIGNER categories are:-

1. AI Technology: Research, development and exploitation
2. AI technology as a Crime and Security threat
3. Legal and Judicial issues and considerations
4. Ethical and Human Rights implications of P&LEA use of AI technology
5. P&LEA utilization of AI technology to enhance and increase P&LEA capabilities
6. P&LEAs and AI technology: Internal governance and training issues

The forty-four main 'areas of concern' are:

1. <u>AI Technology: Research, development and exploitation</u>

Maximise the benefits of previous, current and future EU AI technology research

(WS 1 & WS 2)

AI Technology gaps between P&LEA current capabilities and future needs (WS 1)

Certification of AI technology processes, trustworthiness and security (WS 3)

AI technology in P&LEA investigations vs. Problem of 'one size fits all' (WS 2)

Testing AI technology with real data and intelligence (W2)

P&LEAs to have secure ICT networks for effective AI technology use (WS 2)

2. <u>AI technology as a Crime and Security threat</u>

Crime & security threats posed by AI technology fall into four broad categories (WS1, WS 2)

When considering threat related policy recommendations in relation to P&LEA and AI technology, it will be important to consider them in conjunction with the four over-arching crime

and security threat categories that have emerged to date from the work of the first two ALIGNER Workshops. These are:

- AI technology; Vehicles, robots & drones
- AI technology; Crime & criminality in the digital domain
- AI technology; Disinformation & social manipulation
- AI technology; On-line cybercrime

A range of actors can be motivated to criminally exploit AI technology (WS 1)

Possible exploitation of AI technology for nefarious political purposes (WS 2)

AI technology as an element of Hybrid Threats (WS 1 & WS 3)

Detrimental impacts on businesses of 'ransomware' cyber attacks (WS 2)

AI technology use with 'Bots' to drive social manipulation (WS 2)

3. Legal and Judicial issues and considerations

Lack of high-level legal frameworks and instruments to underpin P&LEA acquisition and utilization of AI technology (WS 3)

Legal regulations relating to P&LEA use of AI technology for task automation (WS 2)

AI as 'dual use' technology: Need for appropriate legal & 'due diligence' checks (WS1 & WS2)

AI and the 'dual use' of 'Chatbots' (WS 2)

AI technology generated content could undermine the integrity of Judicial systems (WS 2)

Use of AI technology assisted transcription in Court cases (WS 3)

AI technology, digital forensics and digital evidence gathering (W2)

4. Ethical and Human Rights implications of P&LEA use of AI technology

Need for clear and transparent monitoring of P&LEA use of AI technology (WS 2)

AI technology and the use of the Impact Assessments (IA) to safeguard privacy and fundamental rights (WS 2)

AI technology in the Commercial and Business world: Need for checks and balances (WS 2)

Public Trust in AI technology generated data (WS 1)

5. P&LEA utilisation of AI technology to enhance P&LEA capabilities

The utilisation (or potential utilisation) of AI technology by P&LEAs falls into ten categories

(WS 1 & WS 2)

When considering potential policy relevant recommendations in relation to AI technology, the ten categories that have emerged from ALIGNER in relation to AI technology and its current and potential use by P&LEA should be noted. The first six cover broad areas of P&LEA activities and capabilities while the remaining four encapsulate more specific core functions that lie at the heart of many P&LEAs and where it was assessed that AI technology could be beneficially applied. They are:

- Recognition and identification of individuals
- Crime and threats; their detection and prevention
- Data and information handling processes
- Digital forensics
- Digital domain activity
- Autonomous vehicles, robots and drones

- Preventive and detection capabilities
- Reactive and response capabilities
- Investigative and prosecutorial capabilities
- Other ancillary P&LEA capabilities

Public acceptance of P&LEAs using AI technology in the virtual world (WS 3 and WS 1)

P&LEA use of AI technology to detect ‘hate speech’ and behavioural indicators (WS 2)

P&LEA use of AI technology in vehicles, robots and drones (W2)

P&LEA use of AI technology for predictive purposes (WS 2)

AI technology as an aid to operational decision making (WS 3)

Processing of multi-agency generated information and intelligence (WS 3)

6. P&LEAs and AI technology: Internal governance & training issues

P&LEA internal governance and training (WS 2 and WS 3)

Governance of P&LEA decision-making tools incorporating AI technology (WS 3)

Resource implications of AI technology to enhance P&LEA capabilities (WS 3)

ANNEX C – Summary of Policy Recommendations from 'popAI', 'STARLIGHT' and ENISA used in the cross-project comparison with the ALIGNER Policy Recommendations

C.1 – popAI Policy Recommendations (Drawn from their Second Policy Brief, Deliverable D1.7, September 30th 2023)

Policy Recommendation 1

"EU to provide a **legal framework for continuous AI training and educational programmes** under the AI Literacy notion for LEAs and civil society"

Policy Recommendation 2

"EU to establish **a common, harmonized European AI regulation for LEAs** that will govern the entire process from the design to the implementation and final use of AI systems by law enforcement authorities"

Policy Recommendation 3

"EU to develop clear **guidelines and standards for the collection, storage, restriction and use by LEAs of sensitive data, including biometric or other data**"

Policy Recommendation 4

"Carrying out **impact assessments** even in cases when this is not obligatory by law"

[NB - No close concordance assessed with ALIGNER PRs]

Policy Recommendation 5

"Establishment and standardization of a **holistic impact assessment process**"

Policy Recommendation 6

"Establishment of **lawfulness, transparency and accountability protocols for LEAs**"

Policy Recommendation 7

"EU to support the development of **guidelines designed especially for the use of AI systems by LEAs**"

Policy Recommendation 8

"Formulating a **general ethical framework for the use of AI tools**, taking into account that the AI Regulation can only regulate the basic legal framework for the use of AI"

Policy Recommendation 9

"EU to ensure that the **use of AI tools by police officers must be subject to multi-level control**"

Policy Recommendation 10

"To establish a procedure for the **evaluation of AI tools by LEAs**, from the ethical point of view"

Policy Recommendation 11

"EU Member States to support the **continuous monitoring of AI systems** in use, taking into account the perspective of civil society organisations"

Policy Recommendation 12

"Establish a European **AI Systems Registry** that will hold basic information about each AI system used by each LEA, by country and its records will be accessible to all EU citizens"

Policy Recommendation 13

"**EU funding investment for research and development** in order to explore the use of AI systems in LEAs"

Policy Recommendation 14

"Institutionalisation of **multidisciplinary collaboration**"

Policy Recommendation 15

"Establish **inclusive AI development standards**"

Policy Recommendation 16

"**Inclusion of Civil Society**"

[NB - No close concordance found with ALIGNER PRs)

Policy Recommendation 17

"EU to **empower people to lodge a complaint and seek redress** when their rights have been violated by the use of an AI system for law enforcement"

C.2 - STARLIGHT Interim Ethical and Legal focused Policy Recommendations (As of September 2023)

Policy recommendation 1

> "Foreseeable regulations and guidance concerning data protection in scientific research: need for greater legal clarity, and a pressing need for more guidance and legislation on scientific research using sensitive data in order to enable AI innovation"

Policy recommendation 2

> "Coherent & consistent regulations – Differences in each legal system can become a barrier when developing AL tools in a multinational consortium and employing them afterwards"

Policy recommendation 3

> "Coherent and consistent ethical approaches - Ethical principles should be developed in a manner to allow different parties to apply them consistently, homogenously; clear and practical guidance should be developed into the tools, based on a common European understanding"

Policy recommendation 4

> "Regulatory sandboxes – collaboration between technical, legal, ethical experts [and P&LEA users] in a dynamic setting"

Policy recommendation 5

> "Contextual feasibility and coherence for LEAs…The tools/approaches that will be developed need to consider differences of country, language, operational environment and software infrastructure and must work to ensure inter-operability"

C.3 – Selected ENISA Research and Innovation Recommendations in concordance with ALIGNER Policy Recommendations

(ENISA Research and Innovation Brief, Published June 7th 2023)

Research Gaps

Research Gap 1

> "Development of standardised data sets following these requirements in order to reliably reproduce and compare existing data sets"

Research Gap 2

> "The need for a standardised performance evaluation framework to enable reliable comparisons between solutions addressing the same or similar problems"

Research Gap 3

"Bringing 'humans into the loop' e.g. training practitioners using real-world scenarios"

Research Needs

Research Need 1

"Test beds to study and optimise the performance of ML-based tools and technologies used for cybersecurity"

Research Need 2

"Development of penetration testing tools based on AI and ML to find and exploit security vulnerabilities to assess the behaviour of attackers"

Research Need 3

"Development of standardised frameworks assessing the preservation of privacy and the confidentiality of information flows as well as the designed system"

Research Need 4

"Development of AI training models for practitioners using real-world scenarios"

Research Need 5

"Establishing an observatory for AI and cybersecurity threats"