Institut européen
European Institute

Executive Master in EU Studies

The EU AI Act: key impacts for the Public Sector

Supervised by Thomas Traguth

Daan VAN PINXTEREN

2024

Abstract

The rapid integration of Artificial Intelligence (AI) in the Public Sector presents significant opportunities to enhance the efficiency, effectiveness, and accessibility of government services but also may incorporate risks to the fundamental rights of individuals, which has led to regulatory efforts in the EU in the form of the EU's Artificial Intelligence Act (AI Act). By analysing use cases, regulatory documents, and literature, this paper aims to understand the key implications of the AI Act in relation to AI use cases in the Public Sector. The paper outlines the history and context of the rules, provides detailed impacts and recommendations for Public Sector entities to navigate the AI Act effectively and turns to general considerations for the Public Sector to take into account for their AI and compliance strategies, relating to the unbalance of risk framework of the AI Act, the goal of trustworthy AI in relation to citizen trust, the possible enforcement of the rules and a philosophical side step into state legitimacy and the effects of the rules worldwide. This way, this research offers a timely and detailed analysis, equipping public bodies with the knowledge and tools to address the upcoming regulatory changes.

Table Of contents

1. Introduction, methodology and limitations

1.1 Introduction and context

Artificial Intelligence (AI) is a technology that has become ever relevant over recent years in the Public Sector due to its potential to enhance and perhaps even revolutionize the efficiency, effectiveness and accessibility of government services.[1] In key areas, AI has the power to automate administrative work, enhance decision-making, optimise executive tasks and powers and improve service delivery to citizens. At the same time, the deployment of AI also raises critical issues related to fundamental rights. Bias, discrimination, privacy concerns, transparency and risks to the health and safety of individuals has led to several regulator efforts, including in the EU with the Artificial Intelligence Act (AI Act). This comprehensive framework is the world's first to regulate AI, with a focus on the safe and ethical use of AI technology, while trying to maintain innovation of AI to harness its positive aspects. As this Act is expansive and complex of nature, and is close to adoption, now is a perfect time for the Public Sector to understand its impact and prepare for the changes that lie ahead.

The aim of this paper is just that. It examines the historical context of the regulation, analyses key elements of the rules that are relevant for the Public Sector and provides insights into the main impacts for public bodies in the areas of public administration, citizen engagement, law enforcement, transportation and smart cities and national security and defense. It will outline key recommendations in dealing with the rules and provides context and general considerations relating to the risk framework of the rules, the aspect of trustworthy AI and citizen trust, and the potential enforcement to take into account for their AI and compliance decisions and strategies. This way, public bodies are equipped with the necessary knowledge and tools to form a deep understanding of the change coming, which helps them develop and implement further strategies and processes in dealing with the change.

In this sense, this paper is very innovative as current research mostly focuses on the general impacts of the AI Act, without focusing on a specific sector, without providing an

[1] See for example Australian Government, *How might artificial intelligence affect the trustworthiness of public service delivery*, Long-term Insight Briefings, 23 October 2023, p. 1-2.

in-depth analysis and without offering specific recommendations in dealing with the change. Furthermore, this research is very actual as it is one of the first that incorporates the final details of the text, with its final compromises and nuances, rather than the proposal of the Commission, which has been the go-to framework in current research on the impacts of the AI Act. This paper therefore provides the most actual and up to-date knowledge.

1.2 Methodology

This paper employs a multi-method approach to analyse the use of AI in the Public Sector and the subsequent implications of the AI Act. The research behind this paper has been as follows:

1. Use case analysis: the paper starts with an overview of AI use cases in the Public Sector, focusing on key areas of use where AI has high impacts but also high potential risks. It provides concrete examples of AI systems to enhance and optimise tasks in the Public Sector.
2. Regulatory analysis: the paper then continues with an examination of the history of the AI Act and the negotiation process to provide context to its impacts. Main sources include white papers, proposals and press releases from the European Institutions and articles of think thanks and watchdogs. Next, an in-depth analysis of the draft AI Act itself has been performed, to extract key elements of the rules that are impacting the Public Sector and create figures to explain the rules. At the time of writing of this paper, the AI Act has not yet been officially adopted and enforced. Therefore, this paper uses the corrigendum document of the text which has been published by Parliament on 19 April 2024 which will almost completely correspond with the final text.[2]
3. Literature review: focus has then shifted to an extensive literature review to place the rules of the AI Act into further perspective and create an overview of main impacts of the rules. Key sources include academic papers, (government) reports, news articles and analyses of stakeholders in the AI landscape.

[2] See the bibliography for a link to the corrigendum document.

4. Data synthesis and integration: the research above has been combined to further specify the key impacts of the AI Act. Based on this, specific recommendations have been created and summarized in a table format. On a deeper level, general reflections and considerations have been identified that highlight key knowledge for the Public Sector in determining the level of compliance, including a philosophical side-step into the context of state legitimacy and the reach of the AI Act as a basis for further research.
5. Summarizing: the paper ends with a conclusion in which the key findings are summarized and the main implications for the Public Sector are extracted.

1.3 Limitations

This paper faces several limitations that may be incorporated into future research. First of all, this paper specifically focuses on the impact of the AI Act in the areas of public services that have been outlined above. Two other major areas of public services, namely healthcare and education, are deliberately excluded from this overview due to limited resources but also due to the fact that these are often a mix between public and private sector services, and both areas are so diverse that they deserve their own analysis. Second, this paper does not aim to provide a complete overview of all impacts for the Public Sector and an exhaustive list of recommendations in a manual format (which is both too extensive and too repetitive for this paper). This way, public bodies are equipped with the most important knowledge and recommendations to deal with the change, to determine further course of action and steps to take, but still need to create specific strategies and action plans for their specific situation, based on further research and analyses that build on this paper (which can be done e.g. by compliance officers or legal departments). Third, as public bodies mostly operate within the areas of their own Member State, this paper does not go into detail in regulatory efforts across the world that may be similar to the AI Act. Fourth and finally, this paper has been written before the rules have come into effect. Therefore, the actual impacts and effects of the rules are not yet known and will need to be monitored by public bodies to optimise their strategies. Similarly, although the AI Act is broad in scope, new technological developments may render some rules ineffective or obsolete, and also this necessitates continuous updates to both the research of the impacts of the rules and its translation towards Public Sector AI and compliance strategies.

2. Use cases of AI in the Public Sector

Because of its possibility to simulate human like intelligence to take over human tasks and perform these more efficiently and effectively, the use of AI in the Public Sector has exponentially increased. AI systems can lead to tangible results and create public value[3] and can minimize the red tape perceived by citizens.[4] The possible application of AI in the Public Sector covers a wide range of use cases. Below, major use cases in the areas of public administration and decision making, citizen engagement, law enforcement, transportation and smart cities, and national security and defence are highlighted with concrete examples.

2.1 Area 1: Public administration and decision making

First of all, AI can be deployed in the Public Sector to directly increase the effectiveness and efficiency of policies and decision making. AI systems can be used for the automation of 'simple tasks' such as documenting information and other basic administrative tasks to change the way public servants can do their jobs and shift from low-value to high-value work.[5] In addition, AI based on machine learning can analyse vast amounts of data to extract valuable insights to provide better public services. For example, Finland's AI programme 'AuroraAI' uses personal and population-level data to provide proactive services to citizens based on life events, for example by suggesting classes to workers needing retraining or possible college applications to a graduating student.[6]

At the same time, AI can also be utilized by government agencies to detect and manage fraudulent behaviour of citizens, for example by using smart algorithms to determine if citizens are eligible for financial aid, which is employed by the Spanish government, or machine learning to detect tax fraud, as employed by the French Ministry of Finance.[7] The most striking example of this type of use is however the fraud algorithm implemented at the

[3] See for example Van Noordt, Colin and Luca Tangi,"The dynamics of AI capability and its influence on public value creation of AI within public administration", *Government Information Quarterly*, 40, 2023, p. 1-3 see also Entsminger, Josh "Public Sector Artificial Intelligence Strategies, Considerations for a Public Value Approach", *The Digital Revolution and the New Social Contract series, Center for the Governance of Change*, IE University, July 2022.

[4] Ingrams, Alex, Wesley Kaufmann and Daan Jacobs, "In AI we trust? Citizen perceptions of AI in government decision making." *Policy & Internet*, 14, no. 2 (2022).

[5] Berryhill, J. Kévin Kok Heang, Rob Clogher, and Keegan McBride. *Hello, World: Artificial intelligence and its use in the Public Sector*, OECD Report, November 2019, p. 77.

[6] Observatory of Public Sector Innovation, "The AuroraAI: A Human-Centric and Life-Event Based Public Sector Transformation", last accessed on 25 May 2024.

[7] European Parliamentary Research Service, *Regulatory divergences in the draft AI act, Differences in public and private sector obligations*, Study Panel for the Future of Science and Technology, May 2022, p. 17.

Dutch Tax authority to detect (child) benefits fraud which has resulted in a nationwide scandal and was one of the reasons for the fall of the Dutch Cabinet Rutte III.[8]

2.2 Area 2: Citizen engagement

AI can be a valuable tool for governments to better engage with citizens or offer front-office services in a more personalized way. A good example is the chatbot, which can be used to efficiently and personally engage with citizens and businesses alike. Simple chatbots in government can be used to answer frequently asked questions that citizens may have for the government agency, but more sophisticated bots, those which leverage machine learning, can allow for more complex interactions. Multiple government agencies in the EU are currently using chatbots, such as chatbot 'Hardi' of the city of Heidelberg in Germany, which uses AI in a special feedback program that becomes more effective the more citizens use it[9], and the ChatGPT based chatbot of the municipality of Kortrijk in Belgium that helps citizens with all kinds of questions to the municipality, understanding the context of the questions.[10]

2.3 Area 3: Law enforcement

In law enforcement, AI can also be useful in a variety of ways. Similar to the area of public administration, AI can be used to alleviate administrative police tasks such as writing reports or finding errors in these reports. In addition, AI can be used to find connections from different databases such as fingerprints, license placed numbers and tax filings, which is for example employed by the AI tool 'FOCUS' of the police of the Belgian city of Antwerp that combines over 50 databases.[11] On a more sophisticated and perhaps intrusive level, AI systems such as facial recognition can be used to identify civilians for law enforcement purposes, something which the company Clearview AI has been doing by scraping the web for faces, in partnership with law enforcement agencies, which has resulted in several fines in Europe.[12] Facial recognition may also be employed to provide surveillance of public accessible spaces, monitor suspicious behaviour and ensure people that are not allowed in

[8] NL Times, "Dutch Cabinet collapses over childcare allowance scandal", 15 January 2021.
[9] City of Heidelberg, " "Frag Hardi" Der chatbot der Stadt Heidelberg". Last accessed on 25 May 2024.
[10] City of Kortrijk, "Primeur: Kortrijk lanceert AI Virtuele Assistent als prototype voor Vlaanderen", 10 October 2023 (in Dutch).
[11] Goldenberg, Paul and Michael Gips, "AI is set to revolutionize policing: Are we ready?", Police1, 4 March 2024.
[12] European Data Protection Board," Facial recognition: Italian SA fines Clearview AI EUR 20 million", 10 March 2022 and European Data Protection Board, "The French SA fines Clearview AI EUR 20 million", 20 October 2022.

these spaces can be identified, something which has been widely used in Europe for example in the German cities of Cologne[13] and across France.[14] Furthermore, AI can be used for predictive policing (to predict future criminal behaviour), for which the city of Amsterdam employs multiple systems such as the 'top 600' to profile the 600 young people most at risk in committing a crime.[15] Predictive policing may also be based on geographic crime data to predict crime, such as the 'Delia' system used by the Milan police to predict the places of crime based on machine learning and other AI techniques.[16]

2.4 Area 4: Transportation and smart cities

In the context of transportation, AI can optimise public transport systems such as railways, trams and metro systems. Use cases of AI relate for example to biometric identification for ticketing purposes, such as employed in the public transport of Moscow and Dubai[17]. AI can also be used for predicting passenger flows, assisting in scheduling and traffic planning and autonomous driving of vehicles.[18] This includes the mapping and management of city traffic flows based on the analysis and classification of urban mobility and situational context data, which has been implemented for example by Transport for London to predict congestion hotspots and adjust signals to ease traffic flows.[19] In a broader context, AI can also be applied to manage and optimise water supply, waste disposal facilities and energy management[20] to analyse and optimise these networks in cities. This is one important aspect of the bigger umbrella of 'smart cities' which uses AI in a variety of domains with highly integrated systems, not only in transport and mobility, but also in healthcare, living, economy and environment.[21] One of the pioneers of building a smart city worldwide is the city of

[13] Montag, Luca et al., *The rise and rise of biometric mass surveillance in the EU*, European Digital Rights (EDRi) Report, 7 July 2021, p. 20-21.
[14] The Brussels Times, " 'All-out assault on privacy': France is first EU country to legalise AI-driven surveillance, 29 March 2023.
[15] Fair Trials, *Automatic Injustice: The use of Artificial intelligence & automated decision-making systems in criminal justice in Europe*, Fair Trials report, 9 September 2021, p. 10.
[16] Idem, p. 20.
[17] Macdonald, Ayang, "Moscow, Dubai ramp up biometric payments in public transportation", Biometric Update, 1 February 2024.
[18] See for example Tang, Ruifan et al.," Transportation Research Part C: Emerging Technologies 140 (2022).
[19] Johnston, Lee, "Artificial Intelligence as a vehicle for Transport innovation and economic growth (Guest blog Kainos)", Tech UK, 21 April 2023, point 2.
[20] European Commission, "Smart cities", last accessed on 25 May 2024. See also European Parliament, *Artificial Intelligence in smart cities and urban mobility*, Briefing requested by AIDA Committee, July 2021.
[21] Herath, H. M. K. K. M. B., and Mamta Mittal, "Adoption of artificial intelligence in smart cities: A comprehensive review," *International Journal of Information Management Data Insights* 2, no. 1 (2022), p. 3.

Rotterdam, which hosts a platform to create a 'digital' city with several initiatives, for example the 3D mapping of buildings to optimise their security and better tackle calamities such as fires.[22]

2.5 Area 5: National security and defence

One of the most popular areas of AI in the Public Sector, but also one with the most risks, is the application of its use in the national security and defence domain. In military and national security, AI is deployed in warfare systems such as drones, weapon navigation systems and surveillance, especially in advanced militaries such as the United States, which is experimenting with drone swarms for battlefield deployment, reconnaissance missions and targeted hunter-killer teams.[23] At the same time, AI can also prove valuable for strategic decision making and data processing on a more tactical and strategic level of military, for example by using generative AI to test possible tactical and operational scenarios and show connections of different types of intelligence data.[24] Also in cybersecurity, AI can be a valuable tool for governments, for example by monitoring and analysing behaviour patterns to create baselines and detect unusual behaviour such as intrusions and malware, to identify anomalies in data, to spot vulnerabilities in computer systems and to automate scans for weaknesses.[25]

2.6 Risks of Public Sector AI use cases

There are a variety of valuable use cases of AI in the Public Sector, with positive effects on the efficiency and effectiveness of decision making, personalized and easy-to-use services for citizens, targeted law enforcement or military efforts and integrated and connected systems in the context of smart cities. Yet, the application of Public Sector AI is not without risks. On the contrary, the many use cases of AI in the Public Sector may lead to violation of the safety, health and rights of individuals and may lead to unfair and discriminatory outcomes due to bias.[26] In the context of public administration, the Dutch tax fraud algorithm scandal is exemplary to this as it has led to much criticism regarding the use of AI by

[22] City of Rotterdam, "Digitale Stad", last accessed: 25 May 2024 (in Dutch).
[23] Hambling, David, "Hives for U.S. Drone Swarms Ready to Deploy This Year", Forbes, 16 May 2024.
[24] Sentient Digital Inc., "The most useful military applications of AI in 2024 and beyond", March 2024.
[25] Shutenko, Victoria, "AI in Cybersecurity: Exploring the Top 6 Use Cases", TechMagic, 13 Setepmber 2023.
[26] Australian Government, *how might artificial intelligence affect the trustworthiness of public service delivery*, p. 2.

governments as it may violate principles such as non-discrimination.[27] In the context of law enforcement, there is much criticism on the application of predictive policing as it may lead to discrimination, violations of the right to a fair trial, and transparency violations.[28] Mass surveillance is also not without dangers, as it may lead to privacy violations due to high amounts of data collection and monitoring of individuals behaviour and chilling rights for the exercise of basic freedoms such as freedom of speech or peaceful protest in fear for the consequences.[29] This expands even more to smart cities, where the integration of multiple AI systems and the massive data collection may lead to a combination of use cases and thus a combination and expansion of possible violations to human rights.[30]

[27] Heikkilä Melissa, "Dutch scandal serves as a warning fro Europe over risks of using algorithms", Politico, 29 March 2022.
[28] Purves, Duncan, "What's Wrong with Predictive Policing?", Public Ethics, 13 June 2023.
[29] Day, Jonathan, "What is Harmful About Public Surveillance", Liberties, 25 April 2023.
[30] Fabregue, Brian, "Artificial intelligence governance in smart cities: A European regulatory perspective." *Journal of Autonomous Intelligence* 7, no. 2 (2024), p. 1.

3. The historical overview of the AI Act

In order to combat the risks to fundamental rights and health and safety of individuals, including those in Public Sector use cases, several efforts in regulating AI have spawned across the world, including in the EU with the AI Act as its culmination. In this section, to gain a better understanding of its impact, the historical overview of the AI regulation in Europe will be analysed and described, providing the context of the rules, the process from proposal to finalized texts and a timeline of events.

3.1 AI regulation in a broader context

Since its rapid rise in the 2010s, several aspects of AI have been captured in legislation of digital technology before AI in its entirety became subject to regulatory efforts. For example, in the General Data Protection Regulation (GDPR), individuals have the right to not be subject to decisions solely based on automated processing of personal data,[31] which also applies to AI as it often uses personal data in its analyses and makes automated decisions on the basis thereof.[32] Similarly, rules on AI are also present in other digital laws of the EU as part of the 'Europe fit for a digital age' regulatory package, one of the main strategic priorities of the previous and current European Commission.[33] For example, the Digital Markets Act (DMA), which specifies rules for 'gatekeepers' (a select group of powerful online platforms), imposes requirements such as transparency and rules on the collection and use of data used for Generative AI.[34] In addition, the Digital Services Act (DSA) introduces due diligence and transparency obligations for algorithmic decision-making by online platforms such as social media, including decisions based on AI.[35]

Besides complementing the existing legal framework discussed above, such as the GDPR, the DMA and the DSA, the upcoming AI Act is part of a broader initiative to foster trustworthy[36] and innovative AI in the EU, such as the AI innovation package, which

[31] Article 22 of the GDPR.
[32] Fieldfisher, "Artificial Intelligence and automated individual decision making, including profiling, under Art. 22 GDPR", 30 June 2023.
[33] European Commission, "A Europe fit for the digital age", last accessed on 25 May 2024.
[34] Some experts say that the DMA has even more far-reaching impacts on AI used by Big Tech than the AI, see Hacker, Philipp, Johann Cordes, and Janina Rochon. "Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and beyond", *Cornell University arXiv Pre-Print* (2022).
[35] Beck, Benjamin and Ulrich Worm, "Eu Digital Services Act's effects on algorithmic transparency and accountability", Mayer Brown, 27 March 2023.
[36] Which is AI that is considered lawful, ethical, and technically robust, see European Commission, *Ethics guidelines for trustworthy AI*, European Commission Report, 8 April 2019.

supports European startups and Small-Medium Enterprises (SMEs) in the development of AI that respects EU values and rules, for example by financial support and AI factories to acquire, update and operate AI-dedicated supercomputers to enable fast machine learning.[37] In addition, the AI Act fits in the Coordinated Plan on AI, which aims to accelerate investment in AI, implement strategies and programmes and align AI policy to prevent fragmentation in Europe.[38]

3.2 The history of the AI Act

To focus on the history of the AI Act itself; specific efforts to investigate regulating AI in the EU started in 2018, with the creation of an expert group that i.a. was tasked with the creation of a proposal for guidelines on AI ethics.[39] In December 2018, these efforts led to a Coordinated Plan on Artificial Intelligence where the EU posed a daring ambition: "to become the world-leading region for developing and deploying cutting-edge, ethical and secure AI.[40] Yet, in the Commissions White Paper on Artificial Intelligence of 2020, the EU already toned down this ambition of developing 'cutting edge' AI, acknowledging for example fierce global competition and that the EU is in a weaker position in consumer applications and on online platforms, resulting in a competitive disadvantage in data access.[41] Thus, although innovation remained an important pillar, The White Paper, which proposed policy options for a future EU regulatory framework on AI, put a strong focus on the challenges that AI could bring and the need for AI to be grounded in values and fundamental rights such as human dignity and privacy protection. The White Paper specifically paid attention to the Public Sector, arguing that it is essential for Public Sector institutions to rapidly begin deploying products that rely on AI in their services.[42] Based on the White Paper, the Commission officially launched a proposal for an AI Act in April 2021, which

[37] European Commission, "Commission launches AI innovation package to support Artificial Intelligence startups and SMEs", European Commission Press Release, 24 January 2024.
[38] European Commission, "Coordinated Plan on Artificial Intelligence", last accessed on 25 May 2024.
[39] European Commission, "Artificial intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards", European Commission Press Release, 9 March 2018.
[40] European Commission, "Member States and Commission to work together to boost artificial intelligence "made in Europe"", European Commission Press Release, 7 December 2018.
[41] European Commission. *White Paper on Artificial Intelligence – A European approach to excellence and trust,* European Commission White Paper COM (2020) 65, 19 February 2020, p. 4.
[42] Idem, p. 8.

highlights the concepts of trustworthiness and the protection of fundamental rights once more.[43]

After the official proposal of the AI Act, the Council of the EU adopted its position in December 2022, where it supported i.e. a narrow definition of AI (to solely machine learning and logic- and knowledge-based approaches), an explicit exclusion of applicability of the rules to national security, defence and military purposes and specific rules on General purpose AI, with the rapid boom of Generative AI such as ChatGPT.[44] The European Parliament followed with its position in June 2023 which again was substantially different. Amongst others, Parliament wanted to follow the Organisation for Economic Co-operation and Development (OECD) definition of AI, moved to impose certain obligations such as due diligence on organisations developing foundation models (used for Generative AI) and urged to ban the use of biometric identification systems completely.[45] Because of these three very different starting points, the negotiation process was lengthy and several Trilogues in the second half of 2023 were needed to reach consensus.[46] There were some hiccups during this process. For example, Big Tech lobbied to leave advanced AI systems, such as foundation models unregulated.[47] Europe's three largest economies: Germany, France and Italy supported this position as, under pressure of national AI companies, they were worried that stringent rules on foundation models would harm the EU's own innovation in the race to harness AI technology, compared to China and the United States.[48]

With coordination of the Spanish council presidency, intense negotiations started on the rules and after 3-day marathon talks in December 2023, a political agreement between the blocs

[43] European Commission, "Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence", European Commission Press Release, 21 April 2021.
[44] Council of the European Union, "Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights", Council Press Release, 6 December 2022.
[45] European Parliament Research Service, "Parliament's negotiating position on the artificial intelligence act", June 2023.
[46] This is also indicated by the Act's 'four column', a working sheet which shows the position of the Commission, Council, Parliament and the final draft text used in the Trilogues, see EU Artificial Intelligence Act, "Documents", last accessed on 25 May 2024, AI Mandates (20 June 2023).
[47] The massive presence of Big Tech in the negotiation process is supported by clear figures; 66% of meetings from 2023 on AI involving members of the European Parliament have been with corporate interests and 86% of meetings of Commission officials have been with the industry. See Corporate Europe Observatory, "Big Tech Lobbying is derailing the AI Act", 24 November 2023.
[48] See Volpicelli, Gian, "Power grab by France, Germany and Italy threatens to kill EU's AI bill", Politico, 20 November 2023.

was finally reached.[49] The final plenary vote of the AI Act in Parliament has taken place on 13 March in 2024[50] and the Council has given its final green light on 21 May 2024. The AI act will finally be adopted 20 days after publication in the official Journal, which is expected soon.[51] From that moment onwards, the AI Act will be applicable for organisations that use AI in Europe, including the Public Sector. However, not all rules will apply immediately. For example, rules on prohibited systems will apply 6 months after entry into force and the rules on generative AI and penalties will apply 12 months after. All other rules, including the rules on high-risk systems will apply 2 years after entry into force.[52]

Figure 1: Timeline of the AI Act.

[49] European Commission, "Commission welcomes political agreement on Artificial Intelligence Act, European Commission Press Release, 8 December 2023.
[50] European Parliament, "Artificial Intelligence Act: MEPs adopt landmark law", European Parliament Press Release, 13 March 2024.
[51] Council of the European Union, "Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI", Council Press Release, 21 May 2024.
[52] Article 113 of the Draft AI Act (corrigendum).

4. Key elements of the rules

In this chapter, the regulatory framework of the AI Act will be outlined. Many of the rules in the regulation focus specifically on the Public Sector and may therefore greatly impact the way AI is used in this context.[53] Key elements of the Act will be analysed and used to determine its impact on the Public Sector and to understand its main implications.

4.1 Definitions

As is obvious from its name, the AI Act will set rules on Artificial Intelligence. Yet, with its massive attention, the term AI has become somewhat of a buzzword. It may apply both to 'simple' algorithms creating output from predetermined inputs to more extensive simulation of human intelligence through machine learning, which forms the basis of most AI models in use.[54] In the negotiation process, the European stakeholders also had difficulties with the variety of interpretations of AI, which became even more difficult with the rapid rise of new use cases, such as generative AI based on large language models. In the final text, based on suggestions from Parliament, the definition of AI is based on the OECD: "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".[55] [56]
The definition used in the AI Act is intentionally broad, with a large variety of AI use cases subject to the rules and a potential to capture future use cases. This broad definition ensures that the AI Act keeps up with recent developments and aims to be technological neutral.[57]

Equally broad and 'future proof' is the definition of large language models (which are coined 'General Purpose AI models' - GPAI), which is an 'AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and

[53] Historically, it is surveillance of the state that individuals need to be protected from. Therefore, examples of the Public Sector use of AI such as fraud-detection or facial recognition misuse are specifically touched upon in the AI Act. See European Parliamentary Research Service, *Regulatory divergences in the draft AI act, Differences in public and private sector obligations*, p. 25.
[54] Wiener, Mark, "AI is a Buzzword. Here Are the Real Words to Know", Medium, 8 April 2023.
[55] Article 3(1) of the Draft AI Act (corrigendum).
[56] Bertuzzi, Luca, "EU lawmakers set to settle on OECD definition for Artificial Intelligence, Euractiv, 7 March 2023.
[57] Stibbe, "The EU Artificial Intelligence Act: our 16 key takeaways, 13 Februrary 2024, takeaway 1.

is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications'.[58] GPAI models thus include large generative AI models such as GPT-4.[59]

4.2 Scope and applicability

Not only based on its definitions the AI Act has a wide applicability, but also because of the territorial scope of the rules. The AI Act states that it applies to organisations that place on the market or put into service AI systems or general-purpose AI models in the European Union, irrespective of whether these organisations are located within or outside the EU. Furthermore, the rules apply to deployers of AI systems that are located in the EU (or have their place of establishment there), organisations that provide or deploy AI in a third country but its output is used in the EU and importers and distributors of AI systems into or within the EU.[60] This shows again that the rules are very wide reaching and geographical loopholes cannot be exploited to evade the AI Act's reach.[61]

However, there are some exemption situations in which the AI Act does not apply. First of all, the AI Act will not apply to AI systems and models, including output, that are developed and put into service solely for scientific research and development purposes.[62] More relevant to the Public Sector, the AI Act shall not apply to systems put in the market or used for military, national security and defence purposes, regardless whether the related activities are carried out by public or private entities.[63] However, if such systems are used in another context, for example in civilian use cases or law enforcement, the rules do apply, meaning that the scope of exclusion is somewhat narrowly defined.

4.3 Risk Based Approach

In order to not overregulate all AI use cases, to be flexible with the technology and to distinguish between the possible impacts that different types of AI have, the AI Act employs a risk-based approach with different rules related to the risk AI systems pose to fundamental

[58] Article 3(63) of the Draft AI Act (corrigendum).
[59] Recital 99 of the Draft AI Act (corrigendum).
[60] Article 2 of the Draft AI Act (corrigendum).
[61] Wörsdörfer, Manuel, "Mitigating the adverse effects of AI with the European Union's artificial intelligence act: Hype or hope?", forthcoming in: *Global Business and Organisational Excellence*, 43(3) (2024), p. 15.
[62] Article 2.6 of the Draft AI Act (corrigendum).
[63] Article 2.3 of the Draft AI Act (corrigendum).

rights and freedoms of individuals. In this risk framework, the AI Act distinguishes different levels of risk:

Prohibited systems

First of all, there is the most severe category of unacceptable risk, which are AI practices that are entirely prohibited. These include systems that deploy subliminal (beyond a person's consciousness), manipulative or deceptive techniques, impairing a person's ability to make an informed decision which is likely to cause harm. In addition, many prohibited systems relate to the use of AI in the Public Sector such as systems that evaluate or classify persons based on social behaviour leading to certain unfavourable treatment (social scoring), but also remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement and risk assessment systems to predict the risk of a person to commit a criminal offence (both subject to exemptions). Finally, prohibited practices relate to the creation of facial recognition databases from the internet or CCTV.[64]

High risk systems

The next category of risk in the AI Act relates to high-risk AI practices which are either certain types of products or safety components of products that fall under the EU's harmonisation legislation such as toys, aircraft, medical devices and cars[65] or practices that fall under a list of high-risk areas identified by the European Commission, which is subject to review and amendments by the Commission in order to keep up with technological developments.[66] This list of systems again encompass many Public Sector use cases of AI such as systems to detect fraud, systems to determine eligibility for public services and benefits and systems used in migration and law enforcement.[67] AI systems that only perform a narrow procedural task, to confirm or improve a human assessment or perform a preparatory task are excluded from the high-risk category.[68]

[64] Article 5 of the Draft AI Act (corrigendum)
[65] Article 6.1 and Annex I of the Draft AI Act (corrigendum).
[66] Articles 6 and 7 of the AI Act (corrigendum).
[67] Annex III of the Draft AI Act (corrigendum).
[68] Article 6.3 of the Draft AI Act (corrigendum).

When an AI practice falls under the high-risk category, the majority of the rules in the AI Act apply and there are many requirements, dependent on the role a party has in the AI value chain (see section 4.4 below).

Limited risk systems

For any AI system that does not fall under one of the categories outlined above but that directly interacts with individuals, there are only minimal requirements as laid out by the rules, as these systems only provide limited risk. These are systems where users may not realize they are interacting with AI such as chatbots or AI-generated content. Therefore, obligations of these systems centre around transparency to the end user, for example obligations to disclose that content has been artificially generated in case of deep fake audio or video.[69] For limited risk systems, the Act also specifies voluntary compliance with the rules by means of codes of conduct, for example for developing trustworthy AI, facilitating inclusiveness and promoting AI literacy.[70]

Minimal risk systems

If an AI system does not fall under any of the categories above, the system can be considered minimal risk and there are no requirements under the AI Act.

Figure 2: Risk categories of the AI Act.

[69] Article 50 of the Draft AI Act (corrigendum).
[70] Article 95 of the Draft AI Act (corrigendum).

General Purpose AI Models

A special category of the AI Act relates to the, during negotiations much debated, GPAI which are not systems in itself but form part of AI systems. Because of the pressure of Big Tech and several countries during negotiations (see section 3.2), this category now follows a two-tiered risk approach, with general transparency measures such as technical documentation about the model including the training and testing process for 'basic' GPAI models.[71] However, for GPAI models that pose systemic risks (which is the case when a model has high impact capabilities on health, safety or the rights of individuals, for example when these models could cause serious accidents or be misused for cyberattacks[72]), there are other requirements such as performing model evaluation, assessing and mitigating the risks and ensure an adequate level of cybersecurity.[73] Models such as GPT-4 and possibly Google's Gemini currently pose systemic risks according to the European Commission.[74]

4.4 Obligations across the value chain

The obligations under the AI Act are directed to a variety of parties in the AI value chain. Most requirements are directed towards organisations that develop AI systems or places the system in service under its own name or trademark, also called 'providers' under the AI Act. Obligations for these parties range from keeping documentation to providing transparency (for GPAI models and limited risk systems). For high-risk systems, there are additional requirements such as 1) the implementation of risk management and quality management systems to estimate and evaluate risks when the AI system is used; 2) data governance management practices for the datasets used in training, validation and testing; 3) drafting technical documentation to demonstrate compliance; 4) logging of the system's events, including its functioning for its entire lifecycle and 5) conformity assessments to ensure systems adhere to the rules.[75]

There are also requirements for the user or 'deployer' of AI systems, that implement AI under its authority. For high-risk systems, the deployer i.a. needs to 1) implement technical and

[71] Article 53 of the Draft AI Act (corrigendum).
[72] European Commission, "Artificial Intelligence – Questions and Answers", European Commission Press Corner, 12 December 2023.
[73] Article 55 of the Draft AI Act (corrigendum).
[74] European Commission, "Artificial Intelligence – Questions and Answers".
[75] Articles 8 to 18 and article 43 of the Draft AI Act (corrigendum).

organisational security measures; 2) mandatory human oversight with the necessary competence, training and authority; 3) monitor the operations of an AI system and 4) keeping the logs generated by the system[76] When the deployer is a Public Sector body or provides public services it also needs to conduct Fundamental Rights Impact Assessments (FRIA) to evaluate risks to individuals and mitigate these risks and register the use of AI high-risk AI systems in an EU database.[77]

Finally, rules apply to the 'importer' and 'distributor' of AI systems which are parties that make an AI system available on the EU market on behalf of another party. Requirements for these organisations mainly relate to verification of conformity assessments and the availability of relevant documentation.[78] Public Sector bodies will usually be considered 'deployers' under the AI Act as they will mostly use AI systems for their use cases that have been developed by other (private) parties. However, public bodies may also be deemed 'providers' of AI systems if they develop their own AI systems or purchase tailor made systems.

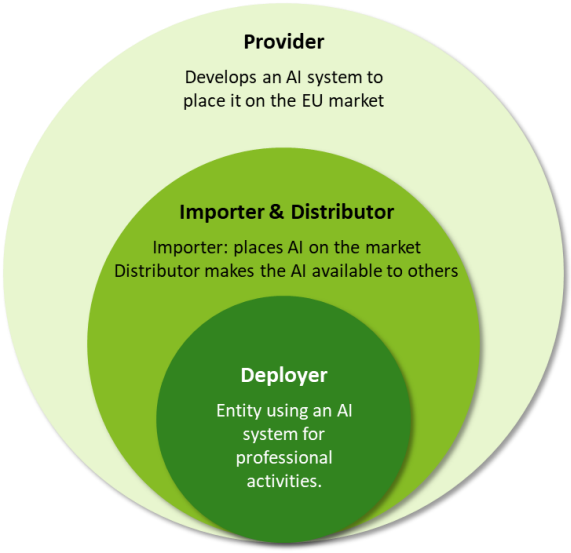

Figure 3: Parties under the AI Act.

[76] Article 26 of the Draft AI Act (corrigendum).
[77] Article 27 and 49 of the Draft AI Act (corrigendum).
[78] Articles 23 and 24 of the Draft AI Act (corrigendum).

4.5 Governance and enforcement

In addition to the rules put on organisations that develop, distribute or deploy AI, a large part of the AI Act is devoted to the creation of a governance framework to ensure compliance. In principle, the rules aim for self-regulation and self-compliance. Organisations themselves can deem if they think their systems fall under the definition of AI and can subsequently determine the risk category of these systems in order to decide on the measures they take.

Regarding regulatory oversight, the rules follow the principle of subsidiarity. Member States need to designate national competent authorities as either notifying bodies or market surveillance authorities and need to provide them with adequate financial and human resources.[79] Market surveillance authorities have the power i.a. to conduct investigations and access all documentation and datasets used for the development of high-risk AI systems including the source code of these systems.[80] Notifying bodies are responsible for the designation and notification of conformity assessments and monitoring thereof.[81] On the European level, the Commission will install an AI Office that is tasked with ensuring uniform application on a EU level, drafting guidelines and manuals and monitoring to ensure the rules remain relevant given the rapid advances in technology (for example by updating the list of high-risk AI systems).[82] The AI Office is also tasked with supervising GPAI models, including monitoring compliance and conducting evaluations.[83] The AI Office will be supported by an Artificial Intelligence Board with representatives from each Member State that ensures consistency and coordination between national authorities, an advisory forum from industry stakeholders to provide technical expertise and to advise the Board and the Commission, and a scientific panel to support the AI Office related to enforcement, for example on the classification of GPAI models.[84]

[79] Article 70 of the Draft AI Act (corrigendum).
[80] Articles 75 and 76 of the Draft AI Act (corrigendum).
[81] Article 28 of the Draft AI Act (corrigendum).
[82] Article 64 and 56 up to 58 of the Draft AI Act (corrigendum) and EU Artificial Intelligence Act, "The AI Office: What is it and how does it work?", 21 March 2024. The setup of the office has just been announced by the commission, see Kroet, Cynthia, "EU Policy. AI Office set-up announced, Lucilla Sioli to be in charge", Euronews, 29 May 2024.
[83] Articles 53 up to 55 and articles 88 up to 93 of the Draft AI Act (corrigendum).
[84] Articles 65 up to 68 of the Draft AI Act (corrigendum).

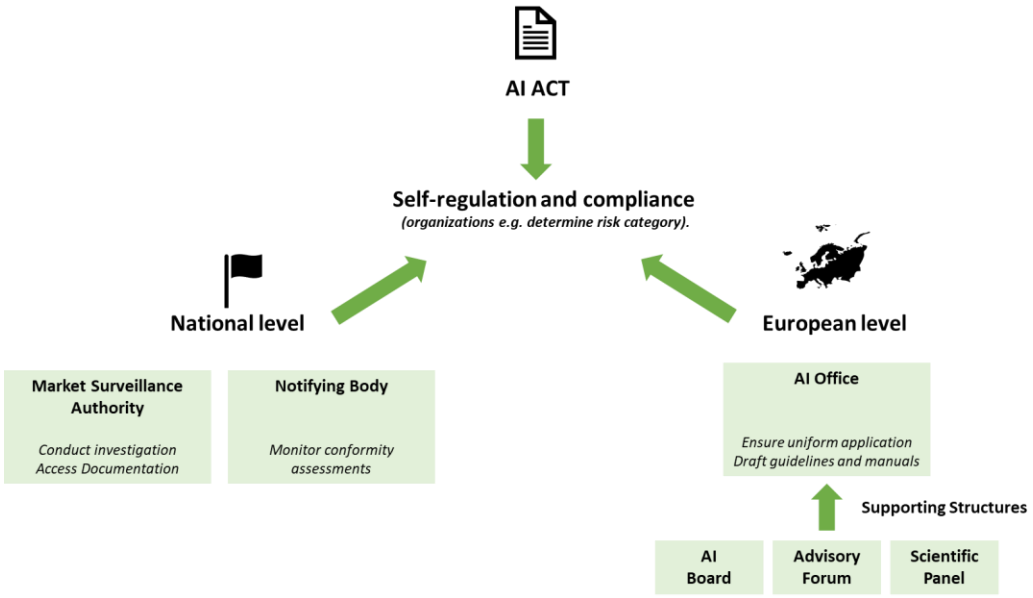

Figure 4: Governance Framework.

Regarding non-compliance, the AI Act specifies that Member States should lay down the rules on penalties and other measures, including warnings and non-monetary measures, with guidelines developed by the Commission.[85] What is clear already is that non-compliance is subject to administrative fines that can reach up to 35 million euros or 7% of global annual turnover for violating rules on prohibited systems, and up to 15 million euros or 3% of global annual turnover for other violations such as the requirements for high-risk systems.[86]

4.6 Measures for innovation

As mentioned before, the AI Act aims not only to regulate AI in the EU, but also tries to stimulate innovation. To this end, the AI Act introduces a regulatory sandbox which aims to achieve legal certainty, supports sharing best practices and fosters innovation and competitiveness for the development of AI systems.[87] This allows organisations, including the Public Sector to limit AI bias and other unintended consequences in a controlled environment Within the sandbox, the above described authorities supervise actors to comply with the AI Act while simultaneously provide guidance and information on how to be compliant.[88]

[85] Article 99 of the Draft AI Act (corrigendum).
[86] Article 99.3 up to 99.6 of the Draft AI Act (corrigendum).
[87] Article 57 of the Draft AI Act (corrigendum).
[88] Article 57.6 and 57.7 of the Draft AI Act (corrigendum).

5. Key implications

The chapter above indicates that the AI Act will have a large potential impact on the Public Sector, as many rules in the AI Act focus on the Public Sector (such as prohibited and high-risk systems). This chapter will provide more detail as to how the AI Act will impact the different use cases outlined in chapter 2, focusing on some key impacts in the described areas and important recommendations to deal with these.

5.1 Area 1: Public administration

In the context of government decision making and public administration, the extent of impact depends on the exact use case, where the level of risk of the AI should be taken into account. For AI systems used to alleviate public service agents in their work, for example by automating simple tasks, the AI Act will have minimal impact as these will most likely fall under the limited risk category or the high-risk category filter of performing narrow procedural tasks. In this cases, there are only transparency requirements to end users that they are interacting with AI.[89] However, more sophisticated AI systems that perform complex tasks, such as models involving profiling to determine if citizens are eligible for certain services such as financial aid will likely fall under a high-risk AI system.[90] However, to complex things, those AI use cases often employ a fraud detection component to determine eligibility[91], yet AI systems used for financial fraud detection are excluded from high-risk AI systems.[92] Up to what extent the models used in this context relate to *financial fraud* detection (if it is rather *tax fraud* or *social benefits fraud* detection) is also up for debate.

Furthermore, determining eligibility for certain benefits or access to public facilities may be based on 'scores' resulting from machine learning output. If these 'scores' are used in contexts that are unrelated to the original gathering of data or disproportionate to the gravity of social behaviour, this is completely prohibited under the AI Act since it is considered social scoring.[93] The widely covered social scoring initiative in China, to classify individuals

[89] See Article 50.1 of the Draft AI Act (corrigendum).
[90] Annex III 5(a) of the Draft AI Act (corrigendum).
[91] See for example the SyRI use case in European Parliamentary Research Service, *Regulatory divergences in the draft AI act, Differences in public and private sector obligations*, p. 17.
[92] Annex II 5(b) of the Draft AI Act (corrigendum).
[93] Article 5.1 (c) of the Draft AI Act (corrigendum).

based on social credit resulting from different kinds of public behaviour[94] is therefore not imaginable in the EU. Government agencies that want to be 'innovative' i.e. by using scoring systems in new contexts and combining multiple datasets should be wary as to not let their AI systems slowly move towards this path as it will have major repercussions, namely a total ban.

Therefore, it is imperative for government agencies to conduct a thorough risk analysis of their AI systems in place to determine the associated risk category in the AI Act, and subsequently determine which measures they need to take to ensure compliance, which are substantially more extensive if a system is high risk and which leads to a complete prohibition if it falls under the unacceptable risk category. In this context, public bodies also need to consider the broader regulatory framework. For example, if the AI system uses personal data, the GDPR should be considered, which also has rules in place for profiling and automated decision making.[95] This is a field that is recently very actively scrutinized and observed. For example, just in December 2023, the Court of Justice of the EU (CJEU) ruled that 'scoring systems' that use personal data are classified as automated individual decision making and thus the GDPR may be violated.[96]

Use case	Impacts	Recommendations
Public administration	- Impact depends on specific use case - Scoring systems may be high risk but may fall under the exception if they are mainly used to detect (financial fraud) - Scoring systems repurposed in other areas may even move towards unacceptable risks	- Conduct a thorough analysis of AI systems to determine exact risk category and if exceptions apply - Ensure repurposing of scoring systems is thoroughly reviewed as this may lead to unacceptable risk - When personal data is used: consider the GDPR and the way it interacts with the rules of the AI Act, particularly for scoring algorithms

Table 1: Impacts and recommendations for public administration use cases

[94] See for example, Velocity Global, "The Chinese social credit system: what to know as a business owner", 6 October 2023.
[95] Article 22 of the GDPR.
[96] See for example, Hartmann, Théophane, "EU top court's ruling spells trouble for scoring algorithms", Euractiv, 7 December 2023.

5.2 Area 2: Citizen engagement

In the context of engagement with citizens, the impact of the AI Act on the Public Sector is more straightforward. The AI Act specifically mentions chatbots as being examples of limited risk systems, which means that only the previously mentioned transparency requirements apply, i.e. informing users that they are interacting with an AI. As chatbots often also process personal data, Public Sector bodies could align the new transparency requirements with existing obligations under the GDPR such as privacy notices in the chatbot.[97] Therefore, minimum additional efforts are to be expected. Furthermore, AI systems generating text content should be robust and reliable, meaning that particular attention should be given to the cybersecurity of these applications.[98] Again, if chatbots process personal data, information security is likely already in scope in relation to GDPR compliance efforts.[99] If more sophisticated chatbots based on GPAI models are used, there are extra precautions, but the focus of the rules of the AI Act related to these models lays on 'providers' of such as OpenAI and Google. It is unlikely that Public Sector bodies themselves will become providers of advanced GPAI models as this does not relate to their task and functions.

Use case	Key impacts	Recommendations
Citizen engagement	- Only limited requirements as mostly limited risk - Transparency obligations and security requirements - Requirements for GPAI models that are incorporated in Chatbots are mostly on the provider (not the Public Sector as user)	- Align transparency requirements with GDPR requirements - Align security requirements with GDPR requirements

Table 2: Impacts and recommendations for citizen engagement use cases

[97] Articles 12 up to 14 of the GDPR specify the requirements for transparency. See for example the privacy notice of Chatbot Hardi on City of Heidelberg, " "Frag Hardi" Der chatbot der Stadt Heidelberg".
[98] Article 50.2 of the AI Act (corrigendum).
[99] Article 32 of the GDPR.

5.3 Area 3: Law enforcement

Contrary to the area of citizen engagement, the impact of AI Act on law enforcement use cases will be considerable. AI used for law enforcement purposes

form a separate category of high-risk use cases of AI in Annex III. These include systems for law enforcement authorities for remote biometric identification systems, systems to assess the risk of a person to become victim of criminal offences, systems to support polygraphs and systems for profiling persons to assess personality traits in order to predict criminal behaviour or detect, investigate or prosecute criminal offences.[100] Similar high-risk systems are listed in the context of migration and border control management.[101]

Yet, what is key in the context of law enforcement, is that there are some exceptions to the requirements due to pressure of the council during negotiations to obtain leeway for law enforcement agencies (being a strong Member State competence). Law enforcement authorities are for example not subject to conformity assessments and can start real world testing of high-risk systems without prior authorisation.[102] Furthermore, the human oversight requirement is somewhat loosened for law enforcement agencies with no mandatory verification of individuals in the context of remote biometric identification.[103] On the other hand, in the context of remote biometric identification, there are also some additional requirements to protect individuals, such as transparency safeguards and requesting authorisation for post-remote identification based on biometrics.[104] [105]

Some systems in the context of law enforcement are completely prohibited. These relate for example to real-time remote biometric identification systems in publicly accessible spaces[106] (as opposed to post), but here again there are some specific exceptions, as now systems specifically used for a targeted search of a missing person or preventing a terrorist attack are

[100] Annex III 6 of the Draft AI Act (corrigendum).
[101] Annex III 7 of the Draft AI Act (corrigendum).
[102] See Draft AI Act – main elements of the compromise, number 5.
[103] Article 14.5 of the Draft AI Act (corrigendum).
[104] Post identification relates to biometric identification based on already existing footage, as opposed to real-time identification which uses actual footage.
[105] See article 26.10 of the Draft AI Act (corrigendum). See also Draft AI Act – main elements of the compromise, number 4.
[106] See article 3(44) of the Draft AI Act (corrigendum).

exempted from the prohibitions.[107] Yet, for these exemptions there again are some additional safeguards, such as authorisation and oversight measures.[108] Predictive policing is also completely prohibited, but this is not the case when AI systems support the human assessment of a person in a criminal activity. This will likely lead to criticism of multiple groups who strongly advocated for a stronger predictive policing ban under the rules.[109]

What is clear from the above, is that the impact of the AI Act in the area of law enforcement is complex. There are many specific rules for this context in the regulation, with many exceptions on the one hand, but also additional requirements on the other hand. It is recommended for law enforcement authorities to deeply familiarize themselves with the rules to ensure the systems can be used. Focus should therefore lie on implementing and developing those systems that fall under the exception of the rules in the AI Act, while minimizing systems that are likely to be prohibited. In those cases, additional safeguards may need to be taken, but in the context of trust in government and its reputation this may be the better alternative than to violate the rules.[110]

Use case	Key impacts	Recommendations
Law enforcement	- Many impacts as law enforcement is mentioned multiple times in the areas of high-risk and unacceptable risk - Several exceptions to the stringent requirements or prohibitions due to pressure of the Council - Some additional safeguards as to protect individuals	- Familiarize yourself with the specific rules of the Act, as there are many exceptions and exceptions to exceptions - Focus on developing systems and implementing systems that fall under the exceptions. Extra safeguards may need to be taken, but this may be better than violating the rules

Table 3: Impacts and recommendations for law enforcement use cases

5.4 Area 4: Transportation and smart cities

Related to transportation and smart cities, the AI Act also has some clear impacts. To start, in the context of smart cities, AI that is used often forms a deeply integrated network of systems across multiple domains. Therefore, it may be difficult for public institutions such

[107] Article 5.1(h) of the Draft AI Act (corrigendum). See also European Parliament, "Artificial Intelligence Act: MEPs adopt landmark law".
[108] See Article 5.2 and 5.3 of the Draft AI Act (corrigendum). See also Draft AI Act – main elements of the compromise, number 3.
[109] See for example, Fair Trials, "AI Act: EU must ban predictive AI systems in policing and criminal justice", 1 March 2022.
[110] More on this intricate balance below in section 6.2.

as municipalities to determine whether their systems used in a smart city context, fall under the definition of AI and subsequently under what specific risk category.[111] To illustrate this, systems that may influence certain behaviour of individuals are completely prohibited, but it is not directly clear how e.g. AI systems that analyse massive amounts of data to help implementing nudging to direct citizens to use public transport or recycle their waste[112] fall under this prohibition. Something similar happens with facial recognition or fingerprint scanning for access to public transport. If these systems are only used to provide access to the service, the high-risk category does not apply, but if the biometric identification system has an additional use, it is a high-risk system.[113]

The same difficulty applies to safety components in the management and operations of critical infrastructure (such as road traffic and the supply of water and electricity). These are classified as high risk as their malfunctioning may put at risk the life and health of persons at a large scale and lead to disruptions in social and economic activity.[114] However, it should be noted that only those systems used as safety components are classified as high risk, such as systems monitoring water pressure, and not AI systems that manage these critical infrastructure, such as managing the flow of water in a dam.[115] Yet, some unclarity exists when AI systems are used as a safety component to secure critical infrastructure, yet do not pose an immediate threat to individuals. In these cases, government agencies should analyse their AI systems used for critical infrastructure and determine whether these are actually deemed safety components.

The above shows that public bodies responsible for smart cities such as municipalities should thoroughly map and analyse the systems used in the smart city context and determine 1) whether they fall under the definition of the AI Act; and 2) if so under which risk category and what measures should be taken. Especially in the context of smart cities, the regulatory sandbox to test high risk systems in a real-life setting, may be a valuable method for governments (together with private actors that develop the AI systems for smart cities) to

[111] Fabregue, "Artificial intelligence governance in smart cities: A European regulatory perspective", p. 2-3.
[112] See for example, Ranchordás, Sofia, "Nudging citizens through technology in smart cities," *International Review of Law, Computers & Technology* 34, no. 3 (2020), p. 265.
[113] Draft AI Act Annex III 1(a) and recital 54 (corrigendum).
[114] Annex III 2 and recital 55 of the Draft AI Act (corrigendum).
[115] Bertuzzi, Luca, "The AI Act's fine line on critical infrastructure", Euractiv, 8 Feburary 2023.

gain understanding of the risk of these systems and the possible impacts on fundamental rights such as privacy and non-discrimination.[116]

Use case	Key impacts	Recommendations
Transportation & Smart Cities	- Interconnected systems make the classification of individual systems difficult regarding the definition of the AI Act and the associated risk category - Nudging systems are prohibited, but it is not clear how this relates to nudging in the context of smart cities - Systems used may fall under high-risk if they perform certain functions (such as safety components in critical infrastructure)	- Map and analyse systems in the transport and smart city context to determine if they fall under the definition of AI (also in the near future) and under what risk category - Understand the concept of safety components to determine if critical infrastructure systems are classified as high-risk - Make use of the regulatory sandbox to test high-risk systems in a controlled environment to minimize impact on individuals

Table 4: Impacts and recommendations for transportation and smart cities use cases

5.5 Area 5: National security and defence

The impact of the AI Act on national security and defence is interesting, since, as mentioned in section 4.2, the areas of (national) security and defence are completely excluded. Although there are many innovative use cases for AI in this context, the nature of national security as a responsibility of Member States make that these areas are not affected by the AI Act.[117] AI systems in the context of national security and defence are rather (potentially) regulated by other frameworks which should be monitored by governments in order to ensure compliance.[118]

Yet, Public Sector bodies should be wary that although the AI Act may not be applicable in situations of national security and defence, innovation in this area could still be hampered by the rules. This is because the effects of the rules may be applicable (private) sector bodies that develop the technologies behind the use cases, such as the large language models

[116] See an example in European Commission, "Sectoral AI Testing and Experimentation Facilities under the Digital Europe Programme". Last accessed on: 26 May 2024.
[117] Recital 24 of the Draft AI Act (corrigendum) argues that this exclusion is justified by Article 4(2) TEU and by the common EU defence policy which are subject to public international law and is therefore the more appropriate framework to regulate these type of AI uses.
[118] Currently however, there are little appropriate frameworks to regulate AI in the military context, see Rönnback, Ronja, "Challenges of Governing AI for Military Purposes and Spill-Over Effects of the AI Act", European AI Alliance, 27 February 2023.

employed for military purposes. Organisations downstream, even outside the EU[119], may be impacted by the rules and affect their ability to develop the systems that will enable future military capabilities.[120] Furthermore, AI systems in these contexts are often dual-use with both civilian and military purposes (e.g. drones).[121] In these dual-use cases, the AI Act would apply to the systems (as it is not solely used for national security and defence) and may be categorized as high risk, with many requirements. Fulfilling the corresponding requirements, such as human-centricity and oversight, may be difficult for these systems as they operate autonomously or in a classified environment. Additionally, most defence organisations do not closely follow civilian digital policy developments, and thus may have a hard time to align with the many documentation requirements.[122]

It is therefore recommended to government agencies to review the potential of dual-use AI and incorporate a framework to deal with these use cases both on a practical and policy level. Governments should aim to be involved in the whole ecosystem of development from inception to field deployment so that the development can be controlled, dual-use may be avoided and the military exception may completely apply and future use cases of AI in military and national security may be safeguarded.[123]

Use case	Key impacts	Recommendations
National security & defence	- General exemption of AI systems used exclusively in these contexts, regulation should be in other frameworks - Organisations downstream are impacted which may affect the way public bodies can innovate with AI - Dual-use cases are impacted by the rules and are possibly high-risk systems	- Monitor frameworks that regulate AI in the national security and defence context and determine compliance with these frameworks - Review dual-use cases of AI and incorporate a framework of use, both on a policy and practical level. - Involve yourself in the entire ecosystem of development of AI to exercise control and avoid dual-use case AI so that the exception applies.

Table 5: Impacts and recommendations for national security & defence use case

[119] See section 4.2.
[120] Greene, Noah, "The EU AI Act could hurt military innovation in Europe", Encompass, January 2024.
[121] See for example. Carrozza, Ilaria, Nicholas Marsh and Gregory M. Reichberg, *Dual-Use AI Technology in China, the US and the EU*, PRIO Paper 2022.
[122] Fanni, Rosanna, "Why the EU must now tackle the risks posed by military AI", CEPS, 8 June 2023.
[123] Greene, "The EU AI Act could hurt military innovation in Europe".

6. General considerations: to comply or not to comply

As already becomes clear from the chapter above and also from the key elements of the rules, some aspects of the AI Act impact the use of AI in the Public Sector more in its entirety and shed light on the complicated balance and decision between compliance and non-compliance. In this chapter, three of these aspects will be further explored and analysed, namely 1) the dichotomy of risks in the rules related to the way the Public Sector uses AI (and will use in the future); 2) trustworthy AI as a goal of the rules and how this relates to trust in the Public Sector; and 3) the possible enforcement of the rules and how this influences the Public Sector's course of action. To deepen the understanding for Public Sector institutions, from this analysis, a more philosophical dimension of state legitimacy in the context of trust versus efficiency will be touched upon.

6.1 The dichotomy of risks in the AI Act

The key elements of the AI Act and its implications for the different areas of the Public Sector show that the requirements in the rules are somewhat unbalanced. In this regard, there exists a clear dichotomy in the risk classification system that is utilized: stringent rules or prohibitions for high-risk and unacceptable risk systems, but only little requirements, i.e. transparency requirements for other AI systems.[124] For some government use cases of AI, such as chatbots to tailor citizen engagement with public agencies, this is good news, as these only need to take into account transparency requirements. Yet, for the wide range of applications of AI in the Public Sector that fall under the high risk category of AI, which means that public institutions that deploy AI have many responsibilities.[125] If public institutions do not only deploy AI that has been developed by other actors, but also develop the AI systems themselves, they are provides and there are a myriad of additional requirements.[126] Thus, regulatory pressure for high-risk systems is significantly higher than for non-high-risk systems and the costs of compliance with the rules are similarly high in these instances, as many requirements for high risk AI systems necessitate investments in e.g. human training and understanding of AI, setting up an infrastructure for cybersecurity

[124] See sections 4.3 and 4.4. See also Wörsdörfer, "Mitigating the adverse effects of AI with the European Union's artificial intelligence act: Hype or hope?", p. 22.
[125] Articles 26 and 27 of the Draft AI Act (corrigendum). See also section 4.4.
[126] Articles 10 and 12 of the Draft AI Act (corrigendum). See also section 4.4.

and monitoring of systems and spending resources to create data management systems and technical documentation.[127]

Under this framework, public institutions may consider to shift their AI strategies from developing and implementing high-risk applications towards AI use cases that have only limited risk, as positive effects on effectiveness and efficiency may outweigh the costs of compliance that otherwise are applicable. Yet, some criticists argue that the EU AI Act, with its dichotomy of risks, may not completely grasp all the risks that non-high-risk systems AI may pose to individuals and does not adequately regulate these types of systems with only transparency requirements.[128] Public bodies should take into account that although systems are deemed non-high-risk under the AI Act, they may still carry risks towards health, safety and fundamental rights of individuals. Therefore, public values such as transparency, privacy, non-discrimination, inclusivity and the right to a fair hearing are important even for non-high-risk systems.[129] Public bodies also could consider to proactively stimulate the development of trustworthy AI based on the role that they fulfil in society and the related expectations of society.[130] This brings us to the following question: how much will the AI Act contribute to the development of trustworthy AI and how much will this in turn lead to more trust in governments by its citizens.

6.2 Trustworthy AI and citizen trust

The AI Act started out as an instrument to protect the fundamental rights of individuals that are threatened by AI.[131] However due to the many compromises during negotiations and pressure to preserve innovation, focus on the protection of fundamental rights and the development of trustworthy AI has been reduced in the final text, with no mention of the

[127] Wörsdörfer, "Mitigating the adverse effects of AI with the European Union's artificial intelligence act: Hype or hope?", p. 18.
[128] De Cooman, Jerome, "Humpty dumpty and high-risk AI systems: the ratione materiae dimension of the proposal for an EU artificial intelligence act." *Mkt. & Competition L. Rev.* 6 (2022), pp. 63-64.
[129] Public institutions struggle for example with accountability and transparency when using AI systems, see The Committee on Standards in Public Life, *Artificial Intelligence and Public Standards*, Committee of Standards Report, February 2020, pp. 18-20. See again on what could go wrong: Heikkilä, "Dutch scandal serves as a warning from Europe over risks of using algorithms".
[130] Kennisnetwerk Data en Samenleving, " 'AI Act als bodem, ethiek als plafond' – Verslag meetup AI Act", VNG nieuws, 4 April 2024 (in Dutch).
[131] See section 3.2

public values above.[132] Focus of the rules lie mainly on market access and product safety and some consider human rights to be an afterthought.[133] Somewhat similar can be said of GPAI models, where the risk is based not on the impact on fundamental rights but on their computing power or reach of individuals.[134] In relation to the Public Sector, the many exemptions in for example national security and law enforcement may detract from the adequate protection of certain individuals and thus the development of trustworthy AI, as criticists have pointed out.[135] The same applies to the filters with which certain systems can be exempted from the high-risk category, for example if these only perform narrow procedural tasks.[136]

Thus, although a key goal of the EU AI Act is to develop trustworthy AI[137], several aspects of the AI Act detract from this goal. Yet, it could again be argued that public bodies should take a step extra and take into account public values and fundamental rights when developing and deploying AI. To achieve this, governments can harness elements of the AI Act such as 1) the FRIA; 2) the sandbox to develop trustworthy AI and limit bias in these systems; and 3) the registration of high-risk systems in the EU wide database. In turn, trust of citizens in public institutions may increase as citizens perceive better, more personalized and more efficient interactions.[138] Consequently, the full potential of AI in the Public Sector may be unlocked due to increased transparency and accountability.[139] At the same time, current research shows that trustworthiness of AI systems may not actually lead to more trust in governments for several reasons. First of all, the actual effects of transparent and accountable

[132] Which is interesting as a majority of the rules of the AI Act are directed to Public Sector institutions, see Van Dijck, José, Natali Helberger en Corien Prins, "Nederland moet doen wat de EU nalaat: burgers beschermen tegen AI", Netkwesties, 30 December 2023 (in Dutch).
[133] Wörsdörfer, "Mitigating the adverse effects of AI with the European Union's artificial intelligence act: Hype or hope?", p. 19.
[134]. Van Dijck, Helberger en Prins, "Nederland moet doen wat de EU nalaat: burgers beschermen tegen AI (in Dutch).
[135]Section 5.3. See also Breyer, Patrick, Sergey Lagondinsky and Kim van Sparrentak, "Protecting privacy: biometric mass surveillance and the AI Act, The Greens/EFA, 6 March 2024.
[136] Bertuzzi, Luca, "AI Act: EU Parliament's legal office gives damning opinion on high-risk classification 'filters'", Euractiv, 19 October 2023.
[137] See section 3.2.
[138] Australian Government, How might artificial intelligence affect the trustworthiness of public service delivery, p. 21-28.
[139] Something which consulting companies also propose, see Mills, Steven et al., "Responsible AI Builds Trust in Government, Boston Consulting Group, 22 January 2021 and Austin, Tasha and Edward van Buren, "Trusted AI, trusted government", Deloitte Article, last accessed on 29 May 2024. Thus, trustworthy AI as an enabler of citizen trust may also be somewhat of a selling point.

AI on trust are unclear as this topic has been understudied in the EU.[140] Furthermore, trustworthiness is more than just the acceptability of risks which is currently the central focus of the AI Act.[141] In addition, trust has an irrational component as it is not based on purely rational deliberations (e.g. the fear of what AI is capable of may play a role in trusting it, even if it is factually more trustworthy than a human or has less bias).[142] Finally, philosophically, there exists the question whether the term trust even applies to AI as that is a human construct. AI can be reliable, but can it be trustable?[143]

Thus, for governments to determine if they want to create more responsible and trustworthy AI strategies is both dependent on their desire to harness citizens trust and improve their perception of society and the actual effectiveness that trustworthy AI has towards a citizen's trust. The benefits of the AI Act for the Public Sector to increase public trust may be limited, compared to the actual costs of compliance and its impacts on Public Sector effectiveness and efficiency due to innovative AI use cases. This balance is further complicated by the expected enforcement of the rules.

6.3 The effectiveness of monitoring and enforcement

What section 4.5 makes clear is that it is up to organisations themselves to classify their AI systems (regarding definition and risk category). This may offer leeway to Public Sector institutions to classify their systems under the category that is most suitable, and avoid having to take (expensive) measures. After determining the risk category, it is again up to organisations to ex-ante determine if their systems comply with the measures described in the rules, or subsequently apply these measures. Hence, the assessments that need to be made, such as the conformity assessment or a FRIA, are self-assessments without external control, and the risk management system that needs to be in place, or the security measures

[140] Laux, Johann, Sandra Wachter and Brent Mittelstadt, "Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk", *Regulation & Governance* 18, no. 1 (2024), pp. 25-26.
[141] With prohibited systems due to unacceptable risk and several requirements for high-risk systems to ensure they do not become unacceptable, see Laux, Wachter and Mittelstadt, "Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk", p. 6.
[142] Idem, p. 26.
[143] Idem, p. 4.

that need to be taken, are all up to the discretion of the organisation, and may thus differ in quality.[144]

In addition, Member States need to designate authorities responsible for monitoring and enforcement of the rules, i.e. the notifying bodies and market surveillance authorities[145] This Member State discretion may lead to uneven implementation of enforcement across the EU, with a burden to regulate and subsequent lack of resources for these enforcement authorities as a result. It is yet unclear how these enforcement bodies will work in practice, whether they will be efficient and whether their powers (which are mostly ex-post such as implementing fines) will be efficient.[146] To go even further, section 4.5 mentions that Member States themselves should lay down rules regarding the fines to impose organisations. But, for public bodies, Member States also lay down rules as to what extent administrative fines may be imposed to these and can lower these or abolish them altogether.[147] [148] Again, this rule may also be unevenly applied across Member States.

Lastly, as mentioned before, focus of the AI Act lays on conformity and risk rather than the protection of individuals. This is also shown in the enforcement mechanisms. Individuals have no right to redress or complaint under the rules and only those with obligations under the AI Act can challenge regulators' decisions, not those whose rights are impacted.[149]

6.4 The context of state legitimacy

Navigating the new legal reality due to the AI Act may thus be difficult for the Public Sector. On the one hand, the AI Act may lead to opportunities to harness citizen trust and protect fundamental rights when developing and using AI. Compliance with the rules also signals the will of public institutions to proactively adhere to public values such as transparency, inclusiveness and privacy and may influence public opinion positively. On the other hand,

[144] . The supranational AI Office and AI Board mostly do not have enforcement powers themselves. See Smuha, Nathalie A., et al., "How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act," *LEADS Lab @University of Birmingham* (2021), p. 37-39.
[145] EU Artificial Intelligence Act, "The AI Office: What is it and how does it work?".
[146] Smuha, "How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act,", p. 46-48.
[147] See also Article 99.8 of the Draft AI Act (corrigendum).
[148] This may be likely, in the absence of a profit motive in the Public Sector and since funds flow only within the government. See for example (related to the GDPR) Information Commissioner's Office, The Effectiveness of Regulatory Penalties in the Public Sector, ICO Economic Analysis, June 2022.
[149] Smuha, "How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act,", p. 44-46.

the possible limited actual positive effects on citizen trust, combined with significant investments for compliance and possibly little and scattered enforcement may deter public institutions from compliance with the rules in order to prioritize efficiency and effectiveness of decision making based on AI.

On a more philosophical level, this dilemma can be further outlined in the context of state legitimacy. Increased citizen trust in AI due to compliance and signalling compliance may increase the support of citizens in public institutions and thus its ability to perform well which increases perceived legitimacy of the state.[150] In this context, transparency about AI decision making by the Public Sector may similarly positively affect the public's perception of the legitimacy of decisions taken by public institutions.[151] At the same time, governments should not underestimate the benefits of better efficiency and effectiveness of government decision making based on AI and the reduction of (perceived) red tape. Disruptions in public administration organisation and decision making due to the burden of compliance may also decrease state legitimacy. This may open pathways to entirely different scenarios, namely a perception that when current (democratic) systems are not efficient, the allure of simplified, yet undemocratic solutions such as populist and authoritarian regimes that are not covered by rules on AI gain traction.[152] Future research should further investigate and conceptualize this dilemma and outline how rules related to AI may eventually affect the working of Public Sector institutions.

With a large territorial scope, a Brussels effect of the AI Act may be likely, for example because the prohibitions laid down in the AI Act may lead to prohibitions worldwide, as offering EU non-compliant AI services may deter users in other countries and may lead to reputational damage.[153] It can also be expected of the EU to exploit its first mover advantage (being the first with comprehensive rules on AI worldwide) and promote its blueprint through participation in international for a and negotiations and incentivize the adoption of EU-like

[150] Nye, Joseph S. "Introduction: The Decline of Confidence in Government", in *Why People Don't Trust Government*, eds. Nye, Joseph S., Philip D. Zelikow, and David C. King (Cambridge: Harvard University Press, 1997), pp. 1-18.
[151] de Fine Licht, Karl, and Jenny de Fine Licht, "Artificial intelligence, transparency, and public decision-making: Why explanations are key when trying to produce perceived legitimacy", *AI & society* 35 (2020), pp. 917-926.
[152] Peixoto, Tiago C., Otaviano Canuto, Luke Jordan, "AI and the future of government: unexpected effects and critical challenges", *Policy Center for the New South*, 20 March 2024.
[153] Siegmann, Charlotte and Markus Anderljung, "The Brussels Effect and Artificial Intelligence, How EU regulation will impact the global AI market", *Centre for the Governance of AI*, August 2022, p. 18-20.

regulation based on trade rules.[154] Because of this effect, differences in approaches regarding AI between regimes may be reduced and may lead to a global governance framework on AI. Such a global governance framework, setting a global standard for trustworthy and responsible AI may provide clarity and may strengthen global trust in (democratic) public institutions and their legitimacy[155] and also deserves further attention of future research.

[154] Idem, p. 20-22.
[155] Erman, Eva, and Markus Furendal. "Artificial intelligence and the political legitimacy of global governance." *Political Studies* 72, no. 2 (2024), pp. 421-441.

7. Final Conclusion

The rapid rise of AI in recent years has led to a variety of areas in which the use of AI contributes to efficiency and effectiveness of services in the Public Sector. At the same time, challenges to fundamental rights such as possible discrimination due to bias has led to several regulatory efforts, including the EU AI Act. This paper has analysed the EU AI Act and based on its history, its legislative framework and its key elements, has identified its impact for the use of AI in the Public Sector in key areas and equipped public institutions with crucial knowledge and recommendations for adapting to the upcoming change:

- In public administration, AI presents opportunities for improving decision-making efficiency but may involve high-risk systems that are strictly regulated under the new rules. Understanding the risk categorization is key to avoid the movement towards prohibited systems. Human oversight should be implemented to ensure bias and discrimination are minimized and the interplay with other legal frameworks such as the GDPR should be understood to navigate the rules.
- In citizen engagement, AI tools such as chatbots offer valuable interaction channels and are limited risk under the regulation, meaning only minimal transparency requirements. For advanced chatbots based on GPAI, focus of the rules lie on providers such as OpenAI and thus do not massively impact public institutions that only utilize these tools.
- The impact of the AI Act in law enforcement is less straightforward, with numerous rules and exceptions, demanding a deep understanding of the legal landscape and attention spend to developing systems that fall within the exceptions to the rules.
- A similar level of complexity can be found in transportation and smart cities, where classifying interconnected AI systems correctly is challenging. The regulatory sandbox proposed by the AI Act can help public institutions in safely developing valuable interconnected AI systems and determine associated risks for individuals.
- In the area of defence and national security, the AI Act applicability is limited. Yet, dual-use AI systems, serving both civilian and military remain subject to regulation and may be classified as high-risk. Governments must navigate these complexities to ensure compliance, innovation, and security in AI applications in this area.

Next to key impacts and recommendations for several areas of AI use in the Public Sector, this paper has also touched upon general considerations related to the question of the level of compliance:

- The dichotomy of risks and requirements offers leeway, but may not do justice to the factual situation, as also limited risk systems may provide risks to individuals and should take into account public values for these systems to become trustworthy.
- Regarding trustworthiness however, the AI Act is less focused on the protection of fundamental rights as its original plans and the question rises whether trustworthiness in AI can actually lead to more trust in governments.
- Together with the significant monetary investment to comply with the rules, the strong focus on self-compliance and limited and possible scattered enforcement of the rules, this may eventually lead to a dilemma of (non-)compliance for Public Sector institutions.

On a philosophical level, this dilemma between compliance and trustworthiness and non-compliance and effectiveness have been discussed in the context of state legitimacy. Both elements may influence perceived legitimacy and a comparison between trustworthy AI and legitimacy based on citizen's trust on the one hand, and legitimacy of public bodies that can work more efficiently and effective due to unregulated AI on the other hand, is a valid topic for future research. The same applies for the possible Brussels effect of the AI Act and a move towards a global framework of AI governance to harmonize the rules worldwide.

For public institutions themselves, navigating the rules and determining their course of action may be not straight-forward, and will depend on the organisation's strategic objectives in line with overall government objectives of Member States. For public institutions that aim for compliance and the upkeep of public values, the recommendations and considerations in this paper may provide useful as a basis for creating strategies and action plans to deal with the rules tailored to their specific situations.

Bibliography

Austin, Tasha and Edward van Buren, “Trusted AI, trusted government”, Deloitte Article, last accessed on 29 May 2024. Available at: https://www2.deloitte.com/us/en/pages/public-sector/articles/trustworthy-artificial-intelligence-government.html.

Australian Government, *How might artificial intelligence affect the trustworthiness of public service delivery*, Long-term Insight Briefings, 23 October 2023. Available at: https://www.pmc.gov.au/sites/default/files/resource/download/ltib-report-how-might-ai-affect-trust-ps-delivery.pdf.

Beck, Benjamin and Ulrich Worm, “Eu Digital Services Act’s effects on algorithmic transparency and accountability”, Mayer Brown, 27 March 2023. Available at: https://www.mayerbrown.com/en/insights/publications/2023/03/eu-digital-services-acts-effects-on-algorithmic-transparency-and-accountability.

Berryhill, J. Kévin Kok Heang, Rob Clogher, and Keegan McBride. *Hello, World: Artificial intelligence and its use in the Public Sector*, OECD Report, November 2019. Available at: https://www.oecd.org/governance/innovative-government/working-paper-hello-world-artificial-intelligence-and-its-use-in-the-public-sector.htm.

Bertuzzi, Luca, “AI Act: EU Parliament’s legal office gives damning opinion on high-risk classification ‘filters’”, Euractiv, 19 October 2023. Available at: https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-parliaments-legal-office-gives-damning-opinion-on-high-risk-classification-filters/.

Bertuzzi, Luca, “EU lawmakers set to settle on OECD definition for Artificial Intelligence, Euractiv, 7 March 2023. Available at: https://www.euractiv.com/section/artificial-intelligence/news/eu-lawmakers-set-to-settle-on-oecd-definition-for-artificial-intelligence/.

Bertuzzi, Luca, “The AI Act’s fine line on critical infrastructure”, Euractiv, 8 Feburary 2023. Available at: https://www.euractiv.com/section/next-generation-infrastructure/news/the-ai-acts-fine-line-on-critical-infrastructure/.

Breyer, Patrick, Sergey Lagondinsky and Kim van Sparrentak, “Protecting privacy: biometric mass surveillance and the AI Act, The Greens/EFA, 6 March 2024. Available at: https://www.greens-efa.eu/opinions/protecting-privacy-biometric-mass-surveillance/.

Carrozza, Ilaria, Nicholas Marsh and Gregory M. Reichberg, *Dual-Use AI Technology in China, the US and the EU,* PRIO Paper 2022. Available at: https://cdn.cloud.prio.org/files/6c0dc6db-c6b3-44a4-b775-126ff97588b4/Carrozza%20Marsh%20Reichberg%20-%20Dual-Use%20AI%20Technology%20in%20China%20the%20US%20and%20the%20EU%20-%20Strategic%20Implications%20for%20the%20Balance%20of%20Power%20PRIO%20Paper%202022.pdf?inline=true.

City of Heidelberg, “ “Frag Hardi” Der chatbot der Stadt Heidelberg”. Last accessed on 25 May 2024. Available at:

https://www.heidelberg.de/HD/Rathaus/_frag+hardi_+-+der+chatbot+der+stadt+heidelberg.html.

City of Kortrijk, “Primeur: Kortrijk lanceert AI Virtuele Assistent als prototype voor Vlaanderen”, 10 October 2023 (in Dutch). Available at: https://pers.kortrijk.be/230558-primeur-kortrijk-lanceert-ai-virtuele-assistent-als-prototype-voor-vlaanderen.

City of Rotterdam, “Digitale Stad”, last accessed: 25 May 2024 (in Dutch). Available at: https://www.rotterdam.nl/digitale-stad.

De Cooman, Jerome, "Humpty dumpty and high-risk AI systems: the ratione materiae dimension of the proposal for an EU artificial intelligence act." *Mkt. & Competition L. Rev.* 6 (2022), pp 49-88. Available at: https://revistas.ucp.pt/index.php/mclawreview/article/view/11304.

Corporate Europe Observatory, “Big Tech Lobbying is derailing the AI Act”, 24 November 2023. Available at: https://corporateeurope.org/en/2023/11/big-tech-lobbying-derailing-ai-act.

Council of the European Union, “Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights”, Council Press Release, 6 December 2022. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/.

Council of the European Union, “Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI”, Council Press Release, 21 May 2024. Available at: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/.

Day, Jonathan, “What is Harmful About Public Surveillance”, Liberties, 25 April 2023. Available at: https://www.liberties.eu/en/stories/public-surveillance/44774.

Van Dijck, José, Natali Helberger en Corien Prins, “Nederland moet doen wat de EU nalaat: burgers beschermen tegen AI”, Netkwesties, 30 December 2023 (in Dutch). Available at: https://www.netkwesties.nl/1731/nederland-moet-doen-wat-de-eu-nalaat.htm.

Entsminger, Josh. “Public Sector Artificial Intelligence Strategies, Considerations for a Public Value Approach”, *The Digital Revolution and the New Social Contract series, Center for the Governance of Change, IE University*, July 2022. Available at: https://static.ie.edu/CGC/Entsminger_Public%20Sector%20AI%20Strategies.pdf .

Erman, Eva, and Markus Furendal. "Artificial intelligence and the political legitimacy of global governance." *Political Studies* 72, no. 2 (2024), pp. 421-441. Available at: https://journals.sagepub.com/doi/pdf/10.1177/00323217221126665.

EU Artificial Intelligence Act, “Documents”, last accessed on 25 May 2024. Available at: https://artificialintelligenceact.eu/wp-content/uploads/2023/08/AI-Mandates-20-June-2023.pdf.

EU Artificial Intelligence Act, “The AI Office: What is it and how does it work?”, 21 March 2024. Available at: https://artificialintelligenceact.eu/the-ai-office-summary/.

European Commission, “A Europe fit for the digital age”, last accessed on 25 May 2024. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en.

European Commission, “Artificial Intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards”, European Commission Press Release, 9 March 2018. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_1381.

European Commission, “Artificial Intelligence – Questions and Answers”, European Commission Press Corner, 12 December 2023. Available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683.

European Commission, “Commission launches AI innovation package to support Artificial Intelligence startups and SMEs”, European Commission Press Release, 24 January 2024. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383.

European Commission, “Commission welcomes political agreement on Artificial Intelligence Act, European Commission Press Release, 8 December 2023. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473.

European Commission, “Coordinated Plan on Artificial Intelligence”, last accessed on 25 May 2024. Available at: https://digital-strategy.ec.europa.eu/en/policies/plan-ai.

European Commission, “Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence”, European Commission Press Release, 21 April 2021. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682.

European Commission, *Ethics guidelines for trustworthy AI*, European Commission Report, 8 April 2019. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

European Commission, “Member States and Commission to work together to boost artificial intelligence “made in Europe””, European Commission Press Release, 7 December 2018. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6689.

European Commission, “Sectoral AI Testing and Experimentation Facilities under the Digital Europe Programme”. Last accessed on: 26 May 2024. Available at: https://digital-strategy.ec.europa.eu/en/activities/testing-and-experimentation-facilities.

European Commission, “Smart cities”, last accessed on 25 May 2024. Available at: https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.

European Commission. *White Paper on Artificial Intelligence – A European approach to excellence and trust*, European Commission White Paper COM (2020) 65, 19 February 2020. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0065.

European Data Protection Board,” Facial recognition: Italian SA fines Clearview AI EUR 20 million”, 10 March 2022. Available at: https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en#:~:text=in%20the%20EU.-,Decision,amounting%20to%20EUR%2020%20million.

European Data Protection Board, “The French SA fines Clearview AI EUR 20 million”, 20 October 2022. Available at: https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en.

European Parliament, “Artificial Intelligence Act: MEPs adopt landmark law”, European Parliament Press Release, 13 March 2024. Available at: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law#:~:text=On%20Wednesday%2C%20Parliament%20approved%20the,46%20against%20and%2049%20abstentions.

European Parliament, *Artificial Intelligence in smart cities and urban mobility*, Briefing requested by AIDA Committee, July 2021. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662937/IPOL_BRI(2021)662937_EN.pdf.

European Parliament Research Service, “Parliament’s negotiating position on the artificial intelligence act”, June 2023. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747926/EPRS_ATA(2023)747926_EN.pdf.

European Parliamentary Research Service, *Regulatory divergences in the draft AI act, Differences in public and private sector obligations*, Study Panel for the Future of Science and Technology, May 2022. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU(2022)729507_EN.pdf.

Fabregue, Brian, "Artificial intelligence governance in smart cities: A European regulatory perspective." *Journal of Autonomous Intelligence* 7, no. 2 (2024). Available at: https://jai.front-sci.com/index.php/jai/article/view/672.

Fair Trials, “AI Act: EU must ban predictive AI systems in policing and criminal justice”, 1 March 2022. Available at: https://www.fairtrials.org/articles/news/ai-act-eu-must-ban-predictive-ai-systems-in-policing-and-criminal-justice/.

Fair Trials, *Automatic Injustice: The use of Artificial intelligence & automated decision-making systems in criminal justice in Europe,* Fair Trials report, 9 September 2021. Available at: https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf.

Fanni, Rosanna, "Why the EU must now tackle the risks posed by military AI", CEPS, 8 June 2023. Available at: https://www.ceps.eu/why-the-eu-must-now-tackle-the-risks-posed-by-military-ai/.

Fieldfisher, "Artificial Intelligence and automated individual decision making, including profiling, under Art. 22 GDPR", 30 June 2023. Available at: https://www.fieldfisher.com/en/insights/artificial-intelligence-and-automated-individual-decision-making.

de Fine Licht, Karl, and Jenny de Fine Licht, "Artificial intelligence, transparency, and public decision-making: Why explanations are key when trying to produce perceived legitimacy", *AI & society* 35 (2020), pp. 917-926. Available at: https://link.springer.com/article/10.1007/s00146-020-00960-w.

Goldenberg, Paul and Michael Gips, "AI is set to revolutionize policing: Are we ready?", Police1, 4 March 2024. Available at: https://www.police1.com/tech-pulse/ai-is-set-to-revolutionize-policing-are-we-ready.

Greene, Noah, "The EU AI Act could hurt military innovation in Europe", Encompass, January 2024. Available at: https://encompass-europe.com/comment/the-eu-ai-act-could-hurt-military-innovation-in-europe.

Hacker, Philipp, Johann Cordes, and Janina Rochon. "Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and beyond", *Cornell University arXiv Pre-Print* (2022). Available at: https://arxiv.org/pdf/2212.04997.

Hambling, David, "Hives for U.S. Drone Swarms Ready to Deploy This Year", Forbes, 16 May 2024. Available at: https://www.forbes.com/sites/davidhambling/2024/05/16/hives-for-us-drone-swarms-ready-to-deploy-this-year/.

Hartmann, Théophane, "EU top court's ruling spells trouble for scoring algorithms", Euractiv, 7 December 2023. Available at: https://www.euractiv.com/section/data-privacy/news/eu-top-courts-ruling-spill-trouble-for-scoring-algorithms/.

Heikkilä Melissa, "Dutch scandal serves as a warning fro Europe over risks of using algorithms", Politico, 29 March 2022. Available at: https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/.

Herath, H. M. K. K. M. B., and Mamta Mittal, "Adoption of artificial intelligence in smart cities: A comprehensive review," *International Journal of Information Management Data Insights* 2, no. 1 (2022). Available at: https://www.sciencedirect.com/science/article/pii/S2667096822000192.

Information Commissioner's Office, *The Effectiveness of Regulatory Penalties in the Public Sector,* ICO Economic Analysis, June 2022. Available at: https://ico.org.uk/media/about-the-ico/disclosure-log/4024372/ic-212626-m7r2-evidence-note-june-2022.pdf.

Ingrams, Alex, Wesley Kaufmann and Daan Jacobs, "In AI we trust? Citizen perceptions of AI in government decision making." *Policy & Internet,* 14, no. 2 (2022), pp. 390-409. Available at: https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.276.

Johnston, Lee, "Artificial Intelligence as a vehicle for Transport innovation and economic growth (Guest blog Kainos)", Tech UK, 21 April 2023. Available at: https://www.techuk.org/resource/aiweek2023-kainos-fri.html.

Kennisnetwerk Data en Samenleving, " 'AI Act als bodem, ethiek als plafond' – Verslag meetup AI Act", VNG nieuws, 4 April 2024 (in Dutch). Available at: https://kennisnetwerkdata.pleio.nl/groups/view/5635563d-3ed7-4337-a81c-25a9798d4512/nieuws/blog/view/a58c3152-cdf4-4b97-9f87-22930e0b5981/ai-act-als-bodem-ethiek-als-plafond-verslag-meetup-ai-act.

Kroet, Cynthia, "EU Policy. AI Office set-up announced, Lucilla Sioli to be in charge", Euronews, 29 May 2024. Available at: https://www.euronews.com/next/2024/05/29/ai-office-set-up-announced-lucilla-sioli-to-be-in-charge.

Laux, Johann, Sandra Wachter and Brent Mittelstadt, "Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk", *Regulation & Governance* 18, no. 1 (2024), pp. 3-32. Available at: https://onlinelibrary.wiley.com/doi/pdf/10.1111/rego.12512.

Macdonald, Ayang, "Moscow, Dubai ramp up biometric payments in public transportation", Biometric Update, 1 February 2024. Available at: https://www.biometricupdate.com/202402/moscow-dubai-ramp-up-biometric-payments-in-public-transportation.

Mills, Steven, Elias Baltassis, Nadim Abilama and Matthew Mendelsohn, "Responsible AI Builds Trust in Government, Boston Consulting Group, 22 January 2021. Available at: https://www.bcg.com/publications/2021/responsible-ai-builds-trust-in-government.

Montag, Luca, Rory Mcleod, Lara De Mets, Meghan Gauld, Fraser Rodger and Mateusz Pełka, *The rise and rise of biometric mass surveillance in the EU,* European Digital Rights (EDRi) Report, 7 July 2021. Available at: https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf.

NL Times, "Dutch Cabinet collapses over childcare allowance scandal", 15 January 2021. Available at: https://nltimes.nl/2021/01/15/dutch-cabinet-collapses-childcare-allowance-scandal.

Van Noordt, Colin and Luca Tangi, "The dynamics of AI capability and its influence on public value creation of AI within public administration", *Government*

Information Quarterly, 40, 2023, available at:https://www.sciencedirect.com/science/article/pii/S0740624X23000606.

Nye, Joseph S. "Introduction: The Decline of Confidence in Government", in *Why People Don't Trust Government,* eds. Nye, Joseph S., Philip D. Zelikow, and David C. King (Cambridge: Harvard University Press, 1997), pp. 1-18. Available at: http://ereserve.library.utah.edu/Annual/POLS/6400/Tong/governance.pdf.

Observatory of Public Sector Innovation, "The AuroraAI: A Human-Centric and Life-Event Based Public Sector Transformation", last accessed on 25 May 2024. Available at: https://oecd-opsi.org/innovations/auroraai/.

Peixoto, Tiago C., Otaviano Canuto, Luke Jordan, "AI and the future of government: unexpected effects and critical challenges", *Policy Center for the New South*, 20 March 2024. Available at: https://www.policycenter.ma/sites/default/files/2024-03/PP_02-24_C.%20Peixoto%2C%20Otaviano%20Canuto%2CLuke%20Jordan.pdf.

Purves, Duncan, "What's Wrong with Predictive Policing?", Public Ethics, 13 June 2023. Available at: https://www.publicethics.org/post/what-s-wrong-with-predictive-policing#:~:text=The%20major%20risks%3A%20bias%20and,of%20some%20predictive%20policing%20systems..

Ranchordás, Sofia, "Nudging citizens through technology in smart cities," *International Review of Law, Computers & Technology* 34, no. 3 (2020), pp.254-276. Available at: https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1590928.

Rönnback, Ronja, "Challenges of Governing AI for Military Purposes and Spill-Over Effects of the AI Act", European AI Alliance, 27 February 2023. Available at: https://futurium.ec.europa.eu/en/european-ai-alliance/blog/challenges-governing-ai-military-purposes-and-spill-over-effects-ai-act.

Sentient Digital Inc., "The most useful military applications of AI in 2024 and beyond", March 2024. Available at: https://sdi.ai/blog/the-most-useful-military-applications-of-ai/

Shutenko, Victoria, "AI in Cybersecurity: Exploring the Top 6 Use Cases", TechMagic, 13 Setepmber 2023. Available at: https://www.techmagic.co/blog/ai-in-cybersecurity/.

Siegmann, Charlotte and Markus Anderljung, "The Brussels Effect and Artificial Intelligence, How EU regulation will impact the global AI market", *Centre for the Governance of AI*, August 2022. Available at: https://www.researchgate.net/publication/363052263_The_Brussels_Effect_and_Artificial_Intelligence_How_EU_regulation_will_impact_the_global_AI_market.

Smuha, Nathalie A., Emma Ahmed-Rengers, Adam Harkens, Wenlong Li, James MacLaren, Riccardo Piselli, and Karen Yeung, "How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act," *LEADS Lab @University of Birmingham* (2021). Available at:

https://strathprints.strath.ac.uk/85567/1/Smuha_etal_SSRN_2021_How_the_EU_can_achieve_legally_trustworthy_AI.pdf.

Stibbe, “The EU Artificial Intelligence Act: our 16 key takeaways, 13 Februrary 2024. Available at: https://www.stibbe.com/publications-and-insights/the-eu-artificial-intelligence-act-our-16-key-takeaways.

Tang, Ruifan, Lorenzo De Donato, Nikola Besinović, Francesco Flammini, Rob MP Goverde, Zhiyuan Lin, Ronghui Liu, Tianli Tang, Valeria Vittorini, and Ziyulong Wang, "A literature review of Artificial Intelligence applications in railway systems," *Transportation Research Part C: Emerging Technologies* 140 (2022). Available at: https://www.sciencedirect.com/science/article/pii/S0968090X22001206.

The Brussels Times, “‘All-out assault on privacy’: France is first EU country to legalise AI-driven surveillance, 29 March 2023. Available at: https://www.brusselstimes.com/430820/all-out-assault-on-privacy-france-is-first-eu-country-to-legalise-ai-driven-surveillance.

The Committee on Standards in Public Life, *Artificial Intelligence and Public Standards,* Committee of Standards Report, February 2020. Available at: https://assets.publishing.service.gov.uk/media/5e553b3486650c10ec300a0c/Web_Version_AI_and_Public_Standards.PDF.

Velocity Global, “The Chinese social credit system: what to know as a business owner, 6 October 2023. Available at: https://velocityglobal.com/resources/blog/chinese-social-credit-system/.

Volpicelli, Gian, “Power grab by France, Germany and Italy threatens to kill EU’s AI bill”, Politico, 20 November 2023. Available at: https://www.politico.eu/article/france-germany-power-grab-kill-eu-blockbuster-ai-artificial-intelligence-bill/.

Wiener, Mark, “AI is a Buzzword. Here Are the Real Words to Know”, Medium, 8 April 2023. Available at: https://medium.com/the-generator/ai-is-a-buzzword-here-are-the-real-words-to-know-47b1e0a324a7.

Wörsdörfer, Manuel, “Mitigating the adverse effects of AI with the European Union's artificial intelligence act: Hype or hope?”, forthcoming in: *Global Business and Organizational Excellence*, 43(3) (2024). Available at: https://www.researchgate.net/publication/375577655_Mitigating_the_Adverse_Effects_of_AI_With_the_European_Union's_Artificial_Intelligence_Act_Hype_or_Hope.

Laws and regulations

Draft AI Act (corrigendum): REGULATION (EU) 2024/… OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of … laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) – CORRIGENDUM. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf.

GDPR: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Draft AI Act – main elements of the compromise: Council of the European Union, 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 - Analysis of the final compromise text with a view to agreement, Interinstitutional file: 2021/0106(COD). Available at: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf.