AI & Partners

Amsterdam - London - Singapore

EU AI Act

Third-Country Preparedness

Examining the preparedness of organisations based outside of the European Union (EU) with the requirements imposed by the EU Artificial Intelligence (AI) Act

September 2024

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Contact: Michael Charles Borrelli | Chief Operating Officer | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

Our report finds that third-country organisations are likely to be well prepared for the EU AI Act, although this depends on both their size and sector. Moreover, larger firms, especially those in health and e-commerce, are more likely to be in a stronger position to achieve EU AI Act regulatory compliance given their large levels of resources, existing processes and procedures together with a large asset and knowledge base.

About this report

This report is based on market research, publicly available data, and interviews with AI specialists in AI & Partners, financial services organisations, and relevant third-parties. Moreover, quotations provided on specific topics reflect those of AI specialists at AI & Partners to be as representative as possible of real-world conditions. All references to EU AI Act reflect the version of text valid as at 13 June 2024. Accessible here. Any predictions, forecasts, estimates or projections made on the EU AI Act's impact are based on market-leading research, including findings from a survey conducted on GDPR preparedness given its analogous nature.

Contents

Foreword

Third-countries[1], such as India, have emerged as global service hubs and have been a partner of choice in the digital transformation journey of global enterprises across 100+ countries. The European Union ("EU") has been a key geography for the third-country industries such as IT, manufacturing, healthcare, retail, etc., which have been serving customers across several verticals and business functions.

Innovations in global service delivery models, best-in-class processes, and standardization have kept third-countries' service industry growth story flying high. With centres such as India maintaining a much-coveted position as one of the world's leading global delivery hubs, third-countries continue to scale their global delivery with innovation in business models, hyper-specialized services, and process maturity. Conformance to artificial intelligence ("AI") regulations in various geographies will be enabled by advancements in trustworthy AI and harnessing technology solutions for rigorous implementation globally.

Following the entry into force of the EU AI Act on **1st August 2024**, organisations are stepping up their focus on trustworthy AI practices as a key requirement to satisfy expectations of global customers and consumers.

Over the last three and a half years, AI & Partners has engaged with their clients and members respectively in their EU AI Act readiness journey. With the main objective of generating awareness, assessing EU AI Act readiness, understanding the evolving best practices and learnings, and to take stock of gaps (if any) and identify improvement areas, AI & Partners has worked hand-in-hand to ascertain the EU AI Act readiness state of organisations in third-country industries servicing/operating in the EU geography.

Moreover, this report takes into consideration existing market research conducted on an analogous regulation, the General Data Protection Regulation ("GDPR"), to make logical inferences on the expected EU AI Act readiness state. The result is a report encapsulating the research findings that will enable adoption and sharing of best practices and delineation of the next steps for scaling up EU AI Act readiness.

[1] A third-country organization refers to a company or entity that is based outside of the European Union (EU), excluding organizations within EU member states. This term is used throughout the report and has consistent application. This includes those that are based in across multiple developing countries (e.g. low-income countries, lower-middle income countries, upper-middle income countries, high income countries), and developed countries.

Executive Summary

Ai & Partners conducted extensive market research, taking into account findings, such as a GDPR preparedness survey report from Deloitte[2], to anticipate the preparedness of organisations based outside of the EU with the requirements mandated by the EU Act[3], given that those exposed to GDPR are more than likely to be in-scope of EU AI Act given the link between data and AI: **data is the gasoline, and AI systems are the combustion engine**. The objective of this research was to ascertain the EU AI Act readiness process and the overall alignment towards trustworthy AI by third-country organisations. The report details many aspects such as the expected awareness of the third-country organisations, how the EU AI Act would be applicable to them, how they can prepare for it, and what are few of the most potentially applicable leading practices used by third-country organisations to adhere with the requirements laid down by the regulation.

Our estimations are that near one third of organisations in-scope of GDPR offer services and have presence in the EU. As compared to large third-country organisations (with employee count in excess of more than 10,000), a majority of third country small & medium enterprises are likely to start their EU AI Act readiness journeys in 2024. From sector perspective, IT/BPM, Health and E-commerce are likely to be the frontrunners of the EU AI Act readiness journey. Based on the survey results it is evidence that the primary driving factor for EU AI Act readiness can be avoiding legal & contractual liabilities, fines & penalties followed by gaining a competitive advantage through EU AI Act compliance. Another related aspect that was identified is for organisations to have a dedicated AI team with increase in AI laws and regulations around the world. As an initial step towards adopting a trustworthy AI culture, organisations are likely to prioritize training and hiring the right AI workforce to manage and implement the requirements of the EU AI Act and defining AI system classification policies and procedures.

Further the survey results indicate that third-country organisations may prefer to establish a clear and appropriate purpose for deploying AI systems in a structured and lawful manner. It was observed that AI systems are being identified mostly in the forms of metadata, whereas high-risk AI systems are not being specifically targeted.

Majority of the third-country organisations consider "Principles relating to responsible AI (Ref: Recital 14a, EU AI Act)" as an enabler of a trustworthy AI-oriented ecosystem in an organisation and not a hindrance. However, a few requirements such as an individual's subject's right to explanation of individual decision-making and other restrictions on AI system deployment pose a challenge to the current setup of third-country organisations.

Few more challenges for maintaining concurrence with EU AI Act such as record keeping, Fundamental Rights Impact Assessment ("FRIA") etc. are also discussed. Since complying to EU AI Act is not a one-time activity, organisations will have to adhere to certain obligations on a regular basis. Amongst such obligations, maintaining records for AI system deployment activities proved to be more tedious for organisations having substantial number of employees or deploying, using, and/or marketing large amounts of AI systems.

[2] Deloitte, (2017), 'GDPR Preparedness Survey Report', accessible at https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-riks-gdpr-preparedness-survey-report-noexp.pdf (last accessed 17th February 2024)

[3] European Parliament, (2024), 'Proposal for a regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts 2021/0106(COD) (COM(2021)0206 – C9-0146(2021) – 2021/0106(COD))', accessible at https://www.ai-and-partners.com/_files/ugd/2984b2_d973c1fc464740da9985c5de8fbe97bb.pdf (last accessed 17th February 2024)

Another viewpoint that was posited was with respect to appointment of a AI Officer ("AIO") which was relative to size of an organisation. Large organisations are likely to appoint / or keen to appoint a AIO preferably having a legal qualification whereas small organisations are likely to appoint /or keen to appoint their business head or chief information office ("CIO") as a AIO.

With respect to breach notification requirements under Article 68e, the data indicates that the organisations functioning as deployers are more likely to focussed on procedural arrangements for responding to a breach at the earliest while users are concerned about making a breach notification.

The report concludes by highlighting the leading state-of-the-art trustworthy AI measures used across third-country industries, with human-centric measures such as quality management systems, internal governance technologies, automated log management, and data protection and privacy likely to be more prevalent now than later, whereas these measures are likely to be slowly adapted as the society becomes more aware and vigilant towards trustworthy AI.

1. Introduction

Background

The world is witnessing a transformative era driven by various resources, with AI' emerging as a pivotal asset for organizations. Technological advancements such as Internet of Things ("IoT"), blockchain, metaverse, etc., are driving a global digital revolution, necessitating robust management of associated digital risks. One such risk revolves around the utilization of AI systems, which could potentially pose harm to individuals' safety, health, and fundamental rights. In response to the escalating risks associated with AI system usage, marketing and deployment, governments and regulators worldwide are actively enhancing AI legislations. One of the most notable and recent developments in this domain is the imminent entry into force of the EU AI Act, which mirrors the significance of GDPR in the realm of AI governance.

The EU AI Act, in a similar, yet different fashion to GDPR, is designed to safeguard the safety, health, and fundamental rights of individuals, particularly concerning the deployment, use and marketing of AI systems. It establishes stringent regulations to ensure transparency, fairness, and accountability in AI usage, aiming to mitigate risks and protect the fundamental rights of individuals. The act imposes obligations on organizations utilizing AI systems, both within and outside the EU, underscoring the importance of responsible AI deployment globally. Given its extraterritorial scope, organizations worldwide are compelled to comply with its provisions when deploying AI systems to EU residents. Moreover, when countries like the United Kingdom ("UK") and Turkey use CE marks, the AI Act applies. E.g. if you want to put a toy using a large language model ("LLM") on the market, a firm must comply with the AI Act.

In light of these regulatory developments, this report was produced to ascertain the potential preparedness of third-country organizations in adhering to the requirements set forth by the EU AI Act. Many multinational organizations based outside the EU, but operating within the European Economic Area ("EEA") or having business interests in the region, are proactively addressing queries and concerns related to AI governance raised by stakeholders, including vendors, employees, and clients. The report findings indicate a potential growing awareness and adoption of leading practices among third-country organizations to align with the provisions of the EU AI Act and manage associated risks effectively.

Subsequent sections delve into the insights gleaned from the survey responses, shedding light on the diverse approaches adopted by organizations to ensure compliance with the EU AI Act.

Methodology

The report, prepared by AI & Partners, employed a rigorous research methodology to gain deeper insights into third-country organizations' readiness concerning the EU AI Act. The methodology encompassed a situational analysis, identification of information needs, qualitative and quantitative research, and correlation analysis of Variables of Interest ("VoIs") related to AI governance. Moreover, it draws insights – and makes inferences – from existing publicly available research on GDPR preparedness given its analogous nature to EU AI Act.

Survey participants

The report elicited insights from range of participants representing organizations of various sizes and sectors, including Information Technology ("IT")/Business Process Management ("BPM"), Banking Financial Services and Insurance ("BFSI"), Telecommunications, Manufacturing, Pharmaceuticals, Healthcare, and Oil & Energy. These participants provided valuable perspectives on the readiness of third-country organizations to comply with the regulatory framework established by the EU AI Act.

Objectives

The report is designed to address the following objectives:

1. To study the anticipated readiness of third-country organisations against the EU AI Act.
2. To check potential awareness amongst third-country organisations about GDPR.
3. To provide key insights on various trends and correlations between EU AI Act requirements and overall AI postures of third-country organisations.
4. To provide an overview of recommended practices that can be followed by organisations.

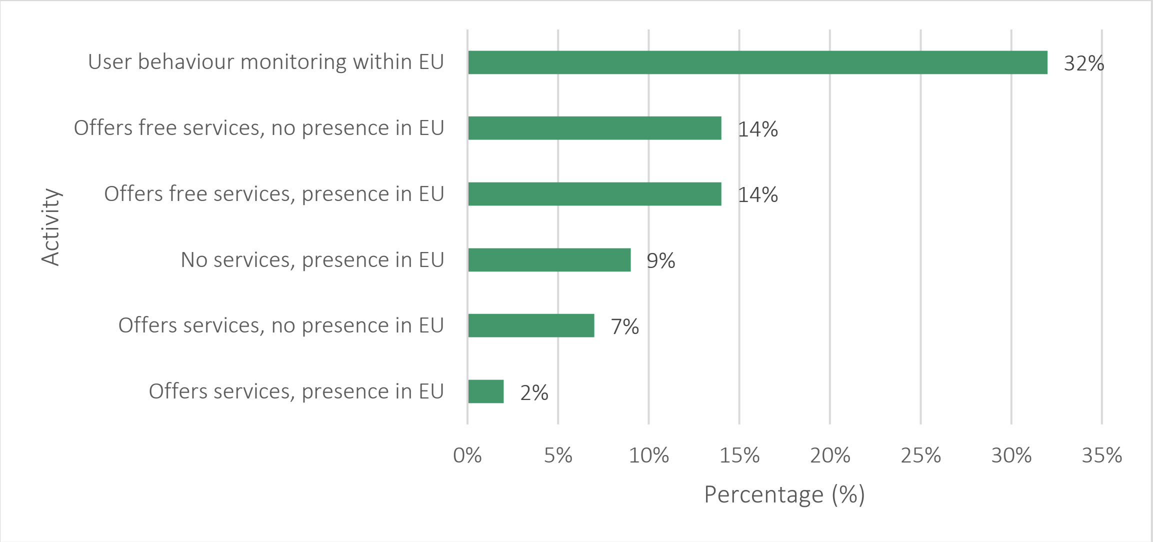
2. Applicability of EU AI Act to Third-Country Organisations

As discussed in Chapter 1, the extraterritorial reach of the EU AI Act affects organizations outside the EU, including those situated in third countries deploying AI systems to EU individuals. Throughout the research, it became apparent that certain third-country organizations were uncertain about the applicability of the EU AI Act to their operations. In such instances, the initial crucial step involves comprehending the criteria determining the applicability of the EU AI Act and simplifying its relevance to organisations deploying AI systems regardless of their physical presence (inside or outside the EU). Analysis of the research findings revealed that approximately 55% of third-country organizations may be subject to the EU AI Act due to their local presence in the EU (which includes organizations offering free services or no services in the EU).

2.1 Applicability as per activities of an organisation

Most prevalent activities in organisations are likely to be:

Figure 1: Likely prevalent activities in organisations



The EU AI Act operates beyond borders and is anticipated to be overseen by a network of supervisory authorities/regulators within the EEA. Consequently, even if a third-country organization lacks local operations in a specific EEA country, the EU AI Act may still be relevant. Below are illustrative scenarios:

- Third-country organizations with a physical presence in the EEA, registered with the local supervisory authority/regulator, may be obligated to comply with notices and undergo site inspections by the authority.
- Third-country organizations without a physical presence in the EEA, but directly offering customer services to individuals in the EEA, might necessitate an EU representative. This representative would act on behalf of the third-country organization before the local regulator and facilitate channels for enforcement and compliance requirements.
- Third-country organizations without a physical presence in the EEA, yet indirectly offering AI-related services to individuals in the EEA, may encounter enforcement of the EU AI Act through binding clauses outlined in service contracts, especially if operating as authorised representatives or deployers to an EU-based provider.
- Third-country organisation without a physical presence in the EEA wants to put an AI-embedded product on the market, regardless of whether or not it's a standalone AI product.

‘A global race for AI trustworthiness has begun’, Arkstons Advisory

The EU AI Act will shape global AI regulations by enforcing compliance from companies worldwide, even outside the EU. Its transparency requirements will boost user trust and accountability by mandating clear communication about AI operations. This push for transparency could lead to more ethical AI development and influence other nations to adopt similar regulations.

Once applicability is established, it is important to assess the organisation’s role i.e. a provider[4], deployer[5] or authorised representative[6]. Data results estimate indicate that ~51% of third-country organisations will operate as deployers.

In the context of the EU AI Act and using GDPR preparedness as an indicator of EU AI Act readiness by third-country organisations, the roles equivalent to those found under the GDPR can be identified as follows:

1. Controller (under GDPR): The closest equivalent in the EU AI Act is the "provider" of an AI system. The provider is responsible for ensuring compliance with the Act's requirements, including the development or putting into service of high-risk AI systems [Article 25] [3].
2. Processor (under GDPR): The EU AI Act introduces the role of the "deployer" who uses or operates AI systems under their authority. Deployers are responsible for certain obligations, such as compliance with registration obligations for high-risk AI systems [Article 29] [3]. Additionally, this can also include the “provider” of an AI system. See **Annex A** for details.
3. Sub-processor (under GDPR): While the EU AI Act does not directly define a role equivalent to a sub-processor as understood under GDPR, the closest concept may involve entities like "authorised representatives" (for providers outside the Union) who perform tasks on behalf of the provider, including ensuring compliance with the Act's requirements [Article 25][3]. Additionally, entities involved in the conformity assessment or testing of AI systems could be seen as fulfilling a supportive role similar to sub-processors, though their responsibilities are more specific to ensuring AI systems' compliance with the Act not processing data [Article 39][3].

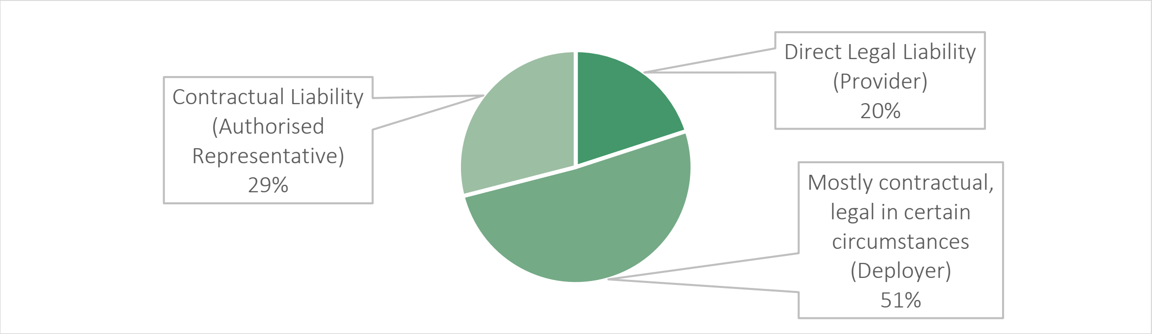
[4] a natural or legal person, public authority, agency or other body that develops an AI system or a general purpose AI model or that has an AI system or a general purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge.

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

[6] any natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation.

2.2 Roles of Organisations W.R.T. EU AI Act

Figure 2: Likely roles of organisations under EU AI Act



Majority of third-country organisations are likely to be deployers.

The data highlighted that 20% of the respondents are likely to operate as a provider since they have a direct legal liability for all activities involving its AI system deployment. A deployer has mostly contractual liability and a legal liability in some circumstances, whereas a authorised representative has solely a contractual liability.

Focusing on this result further, the table below represents potential sectoral coverage of organisations operating as Authorised Representative. Deployer, and Provider.

Table 1: Potential sectoral coverage of key roles under EU AI Act

Direct Legal Liability (Provider)	Contractual Liability (Authorised Representative)	Mostly contractual, legal in certain circumstances (Deployer)
Third-country multinational corporation (operating in EU) (60%) Business process management ("BPM") (67%) Call centre (60%)	Engineering services (43%) Internet platforms (67%) Consulting (39%)	IT services (42%) MNC IT services (50%) Global in-house centre (67%) KPO (50%) Technology product (47%)

'AI regulatory sandboxes incubate global ethics leaders', AZLYC - Aznar Legal & Compliance

Third-country organizations can become global AI ethics leaders by leveraging regulatory sandboxes to adopt the EU AI Act early. Through collaboration with governance bodies, developing transparent AI systems, leading training initiatives, and publishing reports, they can shape global standards and foster trust in responsible AI innovation.

AI Regulatory sandboxes 'critical' in upholding global AI governance

"Third-country organizations can use the EU AI Act and regulatory sandboxes to lead in ethical AI, fostering trust, driving innovation, and influencing future global standards for responsible AI governance."

Enrique Aznar, *Founder*, AZLYC - Aznar Legal & Compliance

AZNAR LEGAL & COMPLIANCE

Trustworthy AI – A ‘D&I Catalyst’

"Trustworthy AI applications not only drive innovation but also serve as a powerful catalyst for Diversity and Inclusion, not just locally or regionally but globally. Safeguarding an individual's well-being and fundamental rights aligns perfectly with Article 1 of the Charter of Fundamental Rights of the European Union. Third-world preparedness is essential in ensuring that standard of governance.”

Lavinia Osbourne, *CEO*, Unbiasfy

2.3 Myths around applicability

It has been observed that organizations in Business Process Management (“BPM”), call centres, and Business Process Outsourcing (“BPO”) sectors often perceive themselves as providers. However, this perception is a myth, as these organizations can function as deployers. They do not determine the purpose and methods of AI system deployment to EU individuals. Instead, they operate under service contracts with their clients (likely to be providers), deploying AI systems according to specified sequences/steps and sharing the deployment results.

It is imperative for third-country organizations to accurately assess their role under the EU AI Act, whether as a provider, deployer, or both. This distinction is essential as regulatory requirements for a provider may differ from those applicable to a deployer.

´Apple Intelligence won't come to most European countries due to Apple's disagreements with E.U. law´

“The EU act sets the bar high and that can also mean missing out on the innovation wave of AI. With all technology we know that regulation in the end has to be put in place to avoid abuse. The EU Act Framework is a very good start and it will be a great export product from Europe to show the necessity to have a framework that is ethical with the boundaries of human rights. A blueprint any country will be able to use and improve their AI readiness.”

Michael Boevink*,* *Founder*, Boevink Group

To conclude, the results in this chapter clearly indicate that EU AI Act, although a European regulation, is likely to significantly impact third-country organisations. The next chapter analyses when such third-country organisations are likely to start their EU AI Act readiness journey and what factors can influence it.

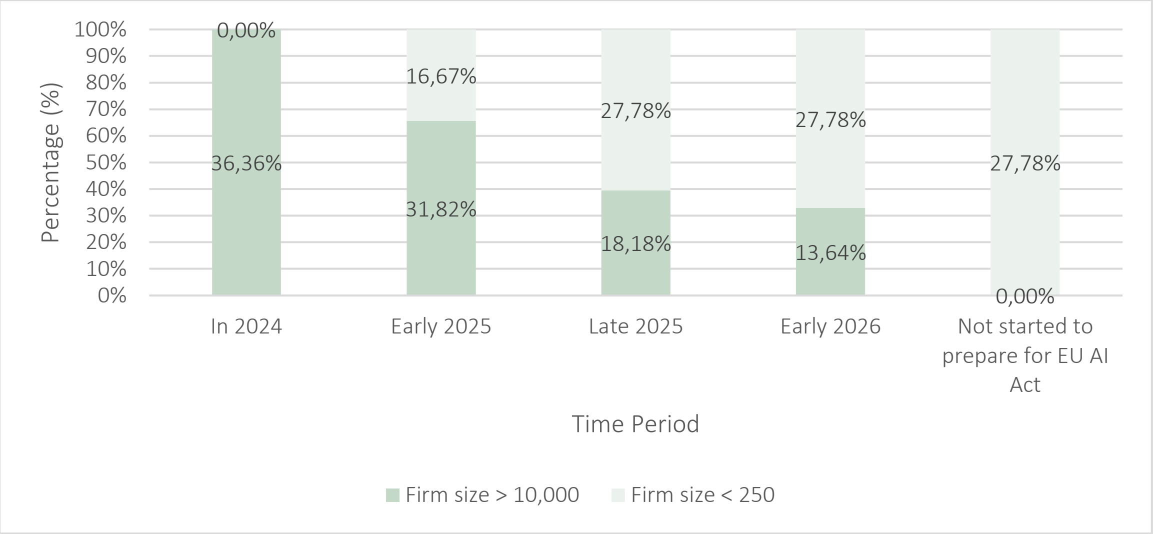
3. Early starters

In 2021, the EU proposal for EU AI Act was published by the European Commission ("EC"). The EU AI Act entered into force on 1st August 2024[7] and become the world's first legislative attempt to establish a unified AI law across Europe. Organizations around the world are set to be granted a two-year period to prepare themselves before the EU AI Act becomes applicable on 2nd August 2026.

The data unveils varying potential reactions to the EU AI Act among organizations based outside of the EU. Approximately 21% of third-country organizations may initiate their AI Act readiness journey in 2024, while 17% may not yet commence their preparations. Notably, it can be surmised that only large organizations (with over 10,000 employees) are likely early adopters, embarking on their AI Act readiness journey as early as 2024, in contrast to small organizations (with less than 250 employees), which are likely to begin their preparations in 2025-2026.

3.1 Size of the organisation versus the likely EU AI Act journey

Figure 3: Likely journey towards EU AI Act



'Equilibrium between compliance and innovation necessary', Edmund Group

To effectively navigate AI governance, it is imperative for firms to strategically balance innovation with legal and regulatory requirements. This equilibrium would not only ensure compliance but also foster sustainable development and cultivate global trust in AI technologies; a key pillar in facilitating international cooperation and harmonising cross-border standards.

Safeguarding public trust fosters AI innovation

"AI governance isn't just about compliance; it's about crafting frameworks that foster innovation while safeguarding public trust and upholding ethical standards globally."

Elliott Day, *Senior Compliance & Financial Crime Consultant*, Edmund Group

EDMUND

[7] European Commission, (2024), 'AI Act enters into force', accessible at https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en (last accessed 19th August 2024)

Majority of third-country SMEs are likely to start their journey late as compared to large third-country organisations.

By early 2025, all large organisations (size > 10,000) are expected to have started their EU AI Act readiness journey, with majority (36%) of large organisations initiating it in the year of EU AI Act entry into force itself (2024). On the other hand, around 28% of the small organisations are likely to not have yet initiated their journey towards EU AI Act as they face issues due to many reasons such as lack of dedicated AI team or insufficient/no budget allocation for the readiness program, etc.

It was also observed that apart from organisational size, the sector in which organisation operate also determined the likely start time for their readiness journey. The sectors that are set to lead EU AI Act readiness efforts were IT/BPM, Health, Ecommerce, Manufacturing and Pharma. It is inferred that sectors which deployed fewer amounts of AI systems are not very prompt and comparatively are likely to have a slow start towards EU AI Act readiness.

‘Rules around AI governance help drive workplace optimisation’, KLIEMT.Arbeitsrecht

AI is still in its infancy, if the experts are to be believed, and yet it is changing our world by the minute. The changes will affect all areas of our lives, and this will be particularly noticeable in the world of work. From a German perspective, both existing laws such as the Works Council Constitution Act and the GDPR as well as new laws such as the AI Act must be observed.

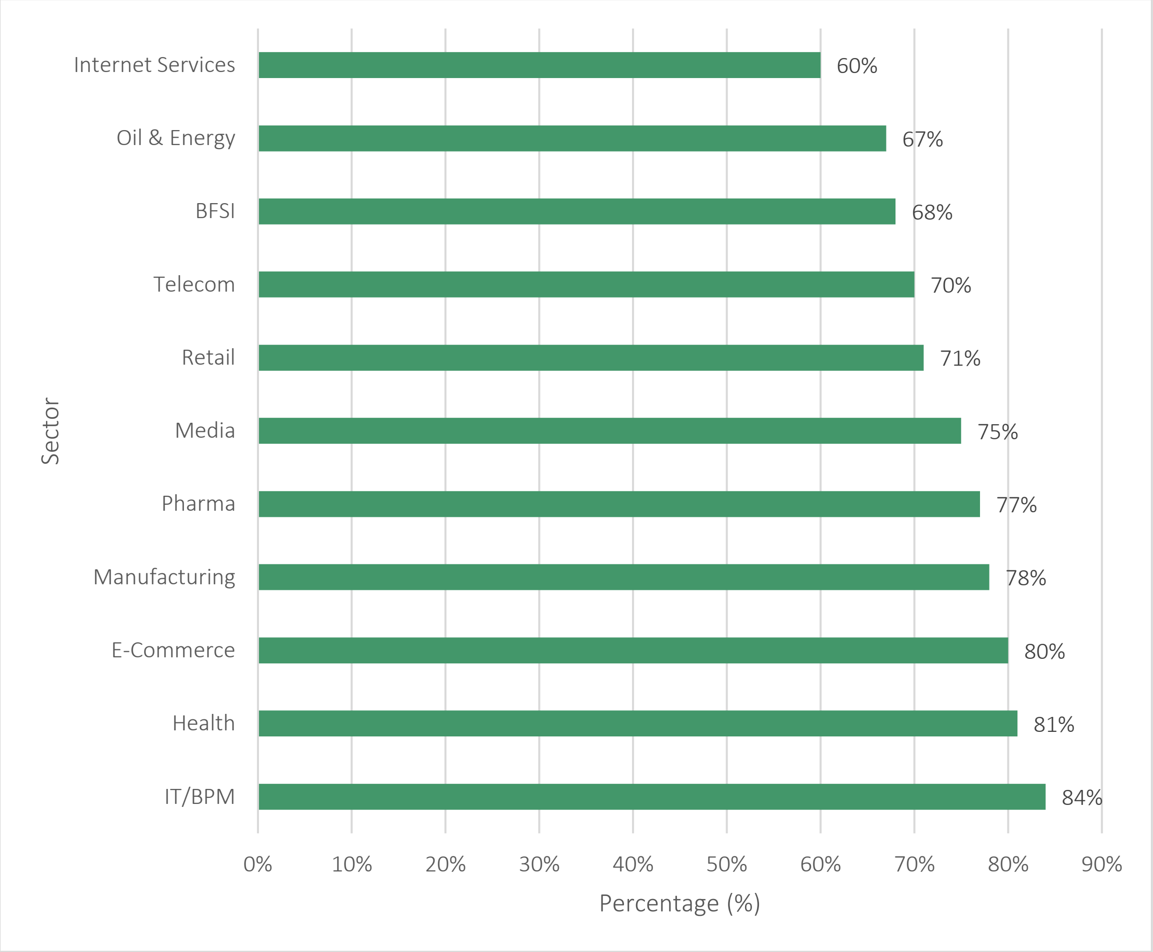
AI Regulation – Alleviating concerns over AI risks

"AI equals the invention of the railway for our century; it will incredibly change the way we work. But we have to make sure that people are not afraid of AI, as they were of the railway.”

Jakob Friedrich Krüger, *Counsel*, KLIEMT.Arbeitsrecht

3.2 Initiation of EU AI Act – sector wise

Figure 4: Anticipated sectoral depiction of organisations that have started their EU AI Act journey August 2026



IT/BPM, Health and E-commerce are probably frontrunners of the EU AI Act readiness journey.

The Sectoral depiction clearly indicates that IT/BPM sector is anticipated to be the most responsive sector in terms of taking any steps towards EU AI Act readiness with 84% of IT organisations projected to have started their readiness journey. This is followed by health and E-commerce sectors with 81% and 80% organisations respectively initiating their process.

Responsible AI – 'Continuous Obligation'

"Ensuring responsible, human-centric AI will be an ongoing challenge requiring constant vigilance, as the technology advances and our work and lives become ever-more reliant on algorithms that are nowhere seen, but everywhere felt."

Charles Epstein, *Co-Founder and Manager*, AIX (AI Exchange)

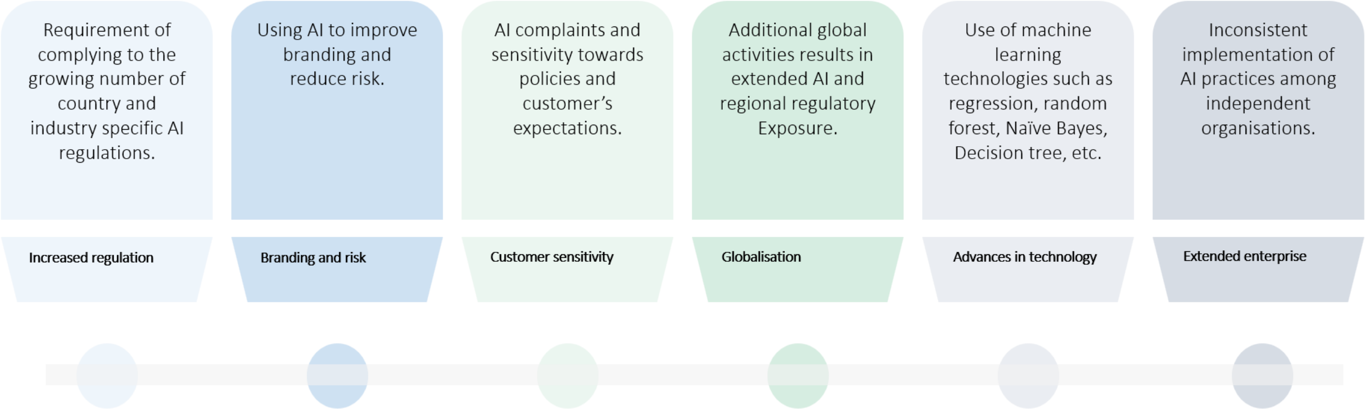
AI EXCHANGE
POWERED BY HR.COM

To conclude, the size and sector are two factors that are likely to determine prompt or slow response of third-country organisations towards EU AI Act readiness. The subsequent chapter, emphasizes the imperative for third-country organisations to be EU AI Act ready.

4. Drivers to be EU AI Act Ready

Subsequent to the EU AI Act applicability date, which is set for 2nd August 2026, more and more organisations from every sector are likely to look to be EU AI Act ready; however, across organisations, the motives may vary.

Investing in EU AI Act readiness and, further, in trustworthy AI, is motivated by some of the following factors:



Requirement of complying to the growing number of country and industry specific AI regulations.

Increased regulation

Using AI to improve branding and reduce risk.

Branding and risk

AI complaints and sensitivity towards policies and customer's expectations.

Customer sensitivity

Additional global activities results in extended AI and regional regulatory Exposure.

Globalisation

Use of machine learning technologies such as regression, random forest, Naïve Bayes, Decision tree, etc.

Advances in technology

Inconsistent implementation of AI practices among independent organisations.

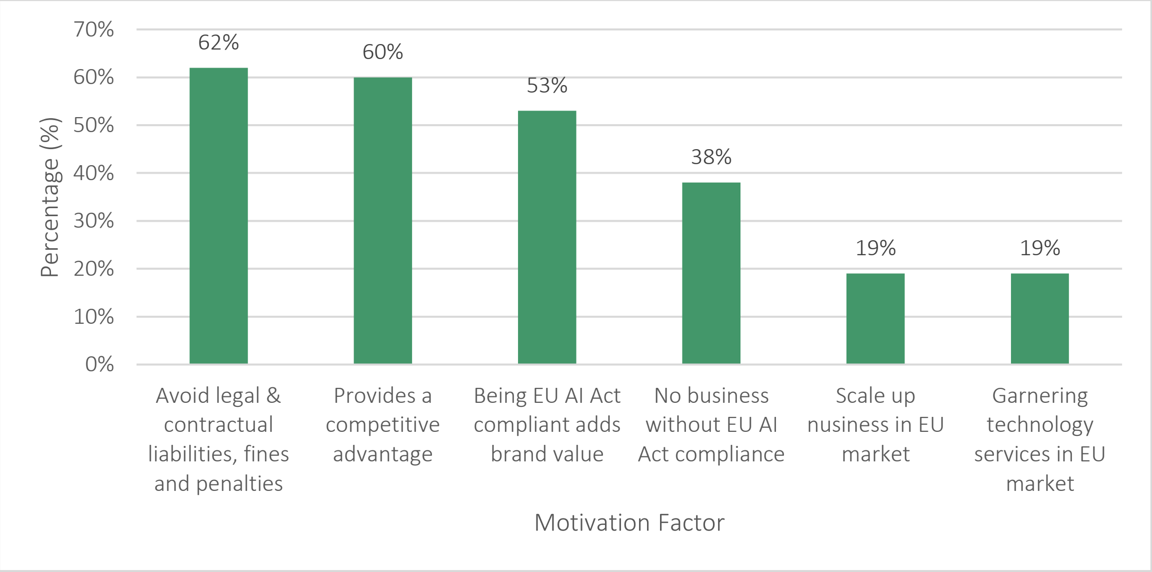
Extended enterprise

The data provided participants with multiple potential objectives and reasons to be EU AI Act ready. With the option to select all applicable reasons, the top three anticipated reasons for third-country organisations to be EU AI Act ready are:

1. **62%**: Avoiding legal & contractual liabilities, fines and penalties is the key focus.
2. **60%**: EU AI Act compliance provides a competitive advantage in the market.
3. **53%**: Being EU AI Act compliant adds to your brand value.

4.1 Anticipated motivation factors for EU AI Act readiness

Figure 5: Anticipated motivation factors for EU AI Act readiness



Leading potential factors towards EU AI Act readiness are likely to be 'avoid legal & contractual liabilities, fines and penalties' and to have a 'competitive advantage'

Most organisations are forecast to have an objective to avoid legal & contractual liabilities, fines & penalties (62%), or to get a competitive advantage (60%).

It is no surprise to note that most of the organisations are expected to consider administrative fines as the reason to be EU AI Act ready. However, it was encouraging to note that many organisations are expected to consider EU AI Act as a value proposition for brand and an enabler for competitive advantage.

Organisations that are EU AI Act ready are expected to gain a competitive advantage as they will be able to use AI systems in their innovations and digitization to provide a better delivery to their clients through the following measures:

- **60%**: Provide better customer experiences.
- **54%**: Enhance productivity of internal operations.
- **47%**: Personalisation of product & service deliveries.
- **46%**: Creation of new products and services.

'Maintaining competitive advantage underpins regulatory adherence', AFAQ AI by OmanPay

AFAQ AI by OmanPay emphasizes the critical need for AI systems to adhere to rigorous quality standards, particularly in markets with less stringent regulations. By prioritizing risk mitigation and aligning with global best practices, AFAQ AI ensures that its AI solutions not only meet but exceed international benchmarks, providing unparalleled reliability and a distinctive market advantage.

AFAQ AI by OmanPay emphasizes the critical need for AI systems to adhere to rigorous quality standards, particularly in markets with less stringent regulations. By prioritizing risk mitigation and aligning with global best practices, AFAQ AI ensures that its AI solutions not only meet but exceed international benchmarks, providing unparalleled reliability and a distinctive market advantage.

Adherence to regulatory standards 'solidifies competitive advantage'

"In an underregulated market, adhering to the highest quality standards in AI development is essential. It ensures risk mitigation, aligns with global benchmarks, and secures a unique, competitive position in the industry."

Osama Al-Zadjali, *CEO and Founder,* AFAQ AI by OmanPay

‘Third-country well prepared for compliance challenge’, Cyber Security Unity

Third-country organisations face significant challenges in aligning with the EU AI Act, which may impact their operations within the EU market, however many organisations are well prepared for the EU AI Act when it comes into place.

Adherence to regulatory standards ‘solidifies competitive advantage’

“Organisations are expected to recognize the EU AI Act not just as a regulatory requirement, but as a strategic opportunity to enhance customer experiences. Embracing compliance will offer them a strong competitive edge, with strategies to ensure readiness and capitalise on this. It is heartening to see such a positive response to the EU AI Act in this important White Paper.”

Lisa Venture MBE, *Founder,* Cyber Security Unity

An opportunity to build stronger, more transparent client relationships

“The EU AI Act implications of this legislation on sales and marketing strategies are profound. While some may view the regulations as a hurdle, we see them as a competitive edge & opportunity to build stronger, more transparent relationships with clients. By ensuring that AI-driven tools and techniques comply with these new standards, we are not only protecting our customers' data but also enhancing the trust they place in firms.”

Payal Raina, *Founder,* FinTech B2B Marketing Community

To conclude, organizations are forecasted to have a variety of reasons to be EU AI Act ready. The data implies that most organizations may view EU AI Act beyond its regulatory requirement and regard this preparedness as an advantage to provide better customer experiences. The next chapter highlights various potential strategies that can be adopted by an organization to be EU AI Act ready.

5. Strategy and Governance

Once organisations decide to undergo the readiness journey, it is recommended to follow a structured approach aligned with expected industry practices. Amongst many aspects of a structured approach, this chapter details the aspects related to awareness, accountability, AI teams, and designated roles.

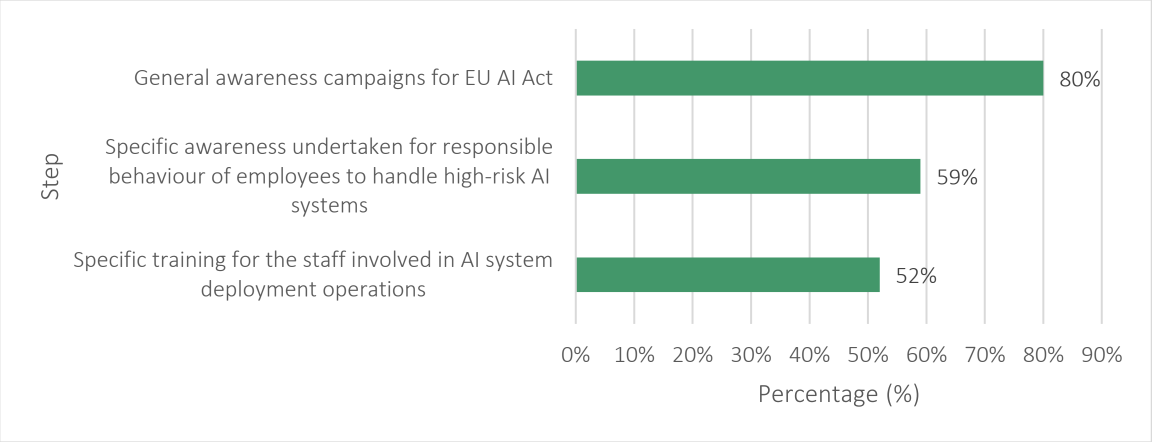
Some of the anticipated leading practises to be followed by organisations are:

- Clearing understanding of existing roles & responsibilities with respect to AI in the organisation
- Structured thinking of the processes that develop and deploy AI systems
- Catalogued AI system elements captured over its lifecycle
- Culture of AI deployed throughout the organisation
- High level of awareness relating to AI throughout the business

Survey data indicate that ~72% organisations are likely to take steps towards AI awareness and training requirements of EU AI Act and ~80% of such organisations may recognize "General awareness campaigns for EU AI Act" as a step taken to spread awareness.

5.1 Awareness & training requirements

Figure 6: Potential steps to be taken towards EU AI Act readiness



Many third-country organisations are expected to conduct general awareness campaigns as their key step for EU AI Act readiness.

Out of the organisations that are expected to have taken action for EU AI Act readiness, 80% may also conducted general awareness campaigns for all their relevant stakeholders to identify their processes which use or deploy AI systems. This will help them streamline their efforts towards EU AI Act readiness. Additionally, while training is not absolutely required, it would be difficult for an organisation, if assessing by internal control, to ignore competency requirements in conformity assessment standards, such as those laid down by ISO/IEC DIS 42006[8].

[8] International Organisation for Standardisation (ISO), (2024), "ISO/IEC DIS 42006Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems", accessible at https://www.iso.org/standard/44546.html (last accessed 29th August 2024)

Third-country organizations must implement programs for their employees to raise awareness regarding the EU AI Act and its associated responsible AI practices. It is essential to cultivate a culture of responsible AI within every organization, as emphasized by the EU AI Act, which stresses not only AI culture but also accountability and demonstration. Certain ways of instilling trustworthy AI within an organization's culture are outlined below.

Every employee, particularly those involved in the use, development, deployment and marketing of AI systems, should possess knowledge of the rules and restrictions pertaining to handling AI systems. Organizations should organize workshops for employees and subcontractors to educate them about the rules and regulations concerning the EU AI Act.

Since individuals play a crucial role in the successful implementation of trustworthy AI and related strategies, it is imperative to establish a robust AI team to promote the AI culture within the organization.

While there are no specific requirements for any professional to evaluate and ensure the readiness of an organization for compliance with the EU AI Act, individuals often pursue certifications to become AI professionals (capable of making decisions, understanding business priorities and limitations, delivering training, assisting with risk assessment, and project management), AI technologists (integrating AI into early stages of IT products and services for cost control and accuracy), AI managers (developing the organization's vision and structure for the AI team and implementing a AI program framework), etc. The data indicates a potential general consensus among respondents as depicted below.

'Sufficient preparation minimises risks', Wriben Consultancy Services Ltd

Correct implementation of Awareness & Training Requirements are crucial for GDPR and the EU AI Act compliance as they ensure that organisation's understand and implement necessary data protection and AI regulations, fostering transparency, accountability, and ethical AI use. This minimizes risks, protects individual rights, and builds public trust.

Robust training a key success driver

"Having worked with multiple global organisations I am acutely aware of how robust training and awareness can make dramatic differences in a company's status in their industry."

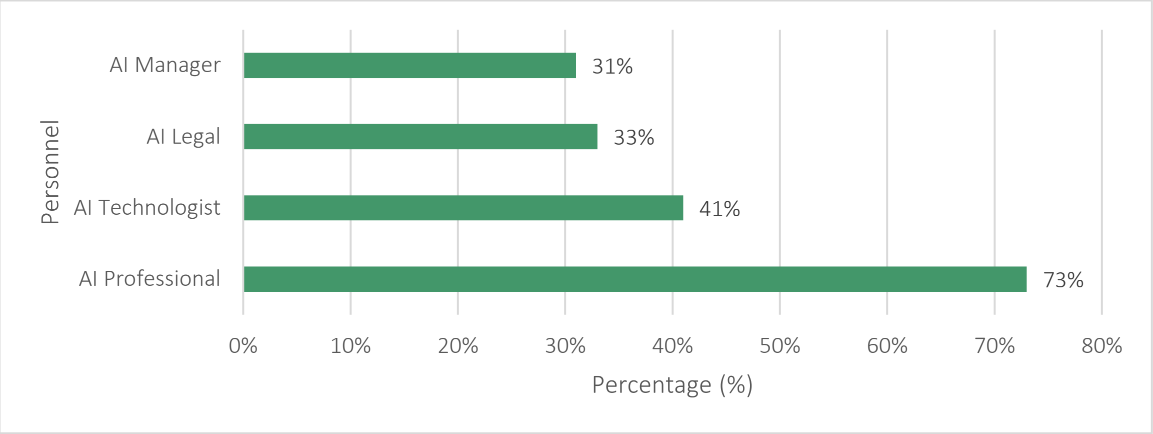
Jeff Bennison*, Director,* Wriben Consultancy Services Ltd

Wriben Consultancy Services

Expert AI, information and cyber security advisor experienced in guiding Boards on organisational risk and improvement opportunities.

5.2 Potential preferences for AI team

Figure 7: Most potentially preferred personnels for AI team



AI professionals are likely to be preferred by majority of third-country organisations for their AI team

73% of our respondents indicate potential demand for an AI professional to be added to their AI team for EU AI Act readiness.

Considering numerous challenges that organisations are likely to experience with EU AI Act readiness, compliance and demand for AIOs, organisations should prioritize training and hiring the right AI individuals to manage and implement the requirements of EU AI Act.

The data suggests that organisations are likely to identify specific roles to drive EU AI Act readiness journeys. The projected top-rated roles accountable / designated for the EU AI Act compliance were AI Officer or / Chief AI Officer (responsible for the vision, strategy, and program regarding use of AI systems) (~32%) and Chief Information Security Officer (responsible for the vision, strategy, and program to ensure protection of AI systems assets, and technologies) (~ 20%). It is also observed that the majority of small organisations may identify their Business Owner or CIO as the person-in-charge.

‘Global enterprises have an opportunity to lead in ethical AI development’, BOARD OS

Drawing from GDPR's transformative impact, AI & Partners research’ anticipates the EU AI Act setting new international standards for AI governance. It encourages a forward-looking business readiness strategy where global enterprises don't just comply, but lead in ethical AI deployment. This proactive stance fosters a global business ecosystem where innovation thrives alongside stringent compliance, ensuring that integrity becomes a cornerstone of technological advancement worldwide.

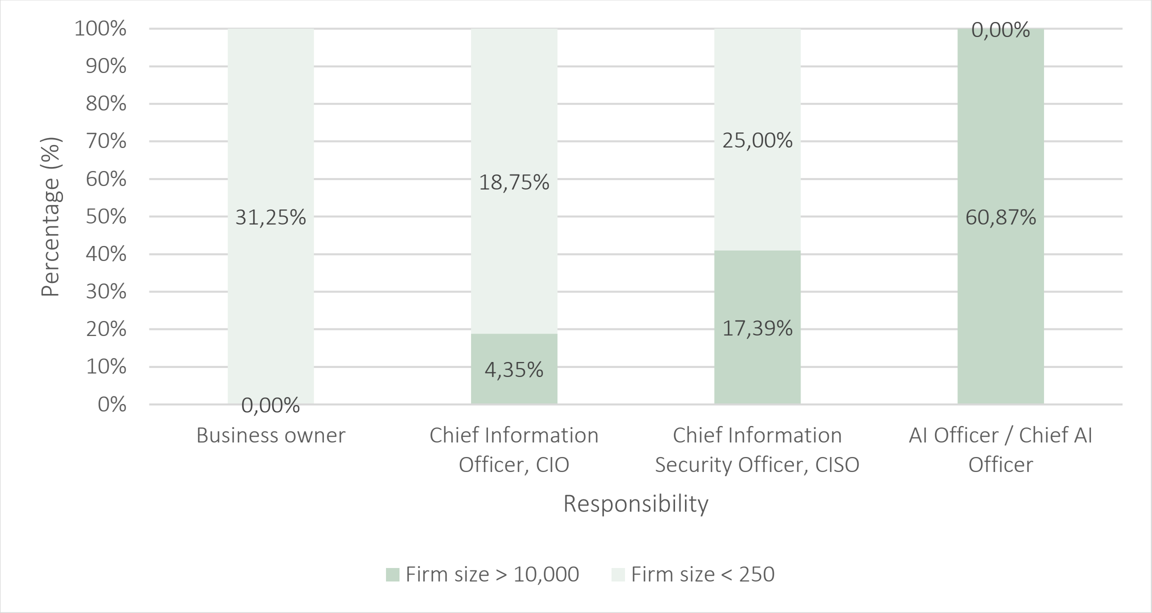
Global Strategy, Local Adherence: Board Leadership in Third-Country EU AI Act

"Boards in third countries bear the critical responsibility of architecting and transforming the EU AI Act from a regulatory checklist to a strategic asset. By cultivating and empowering AI teams that deeply understand and implement these standards, they turn regulatory alignment into a distinctive advantage, propelling their companies to the forefront of ethical innovation on the global stage and robust market access.”

Steven PAUL, CDir FIoD, *Founder and MD*, BOARD OS

5.3 Likely responsibility for ensuring EU AI Act compliance in an organisation

Figure 8: Likely responsibility for ensuring EU AI Act compliance in an organization



Many third-country SMEs are likely to have Business Owners in charge of compliance whereas large third-country organisations may hand over the responsibility to the Chief Privacy Officer ("CPO").

Many SMEs are likely to keep their business owner or CIO as the person in-charge whereas large enterprises / or organisations are likely to prefer a separate AI as the head of their AI team. One of the key reasons to appoint a AIO is regular and systematic monitoring of AI systems on a large scale or deploying high-risk AI systems on a large scale as "core activities".

> **Researching non-EU organizations' preparedness for the EU AI Act is crucial**
>
> *"Understanding the challenges and strategies employed by these entities can inform effective compliance measures and identify potential competitive advantages for EU-based companies."*
>
> **Richard Chiumento,** *Director,* Rialto

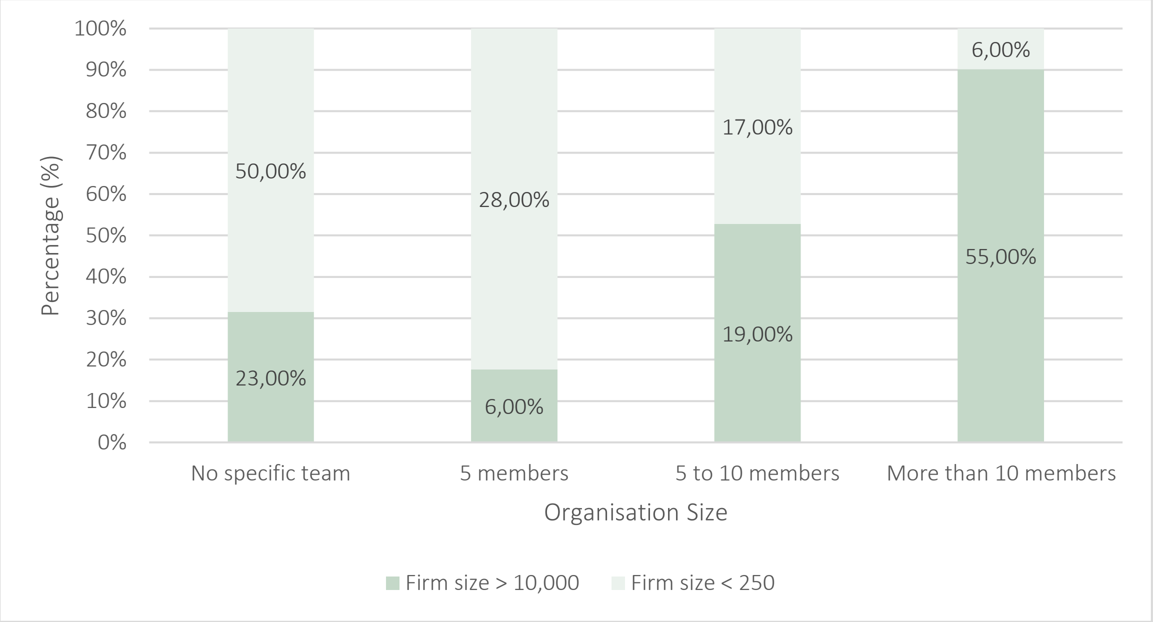
rialto
ACCELERATED IMPACT

Since the responsibility of driving compliance in an organisation should not reside with one individual, organisations are likely to increase and expand their AI teams in order to deal with the ever increasing AI laws and requirements. Key management in addition to HR, Legal, Marketing and security need to be involved. Organisation's senior employees, must work together to ensure a smooth path to achieving compliance. Organisations cannot be fully compliant without board involvement.

Further, it is predicted that the size of a AI team is relative to the size of the organisation. AI teams within an organisation are tasked with AI governance, AI system lifecycle management, etc. and will be continuously challenged to provide clearer, more proactive oversight on AI system storage, journeys, lineage and other requirements of EU AI Act. Therefore, the size of the AI team should be substantial in comparison with the size of the organisation.

5.4 Likely size of AI team

Figure 9: Expected organization size versus AI team size



The size of an AI team of an organisation is expected to be directly proportional to the size of the organisation.

55% of large organisations are expected to have more than 10 members in their AI teams.

'Leading practices to be established in upcoming months', Dr. Ilesh Dattani

The EU AI Act has extraterritorial reach, meaning it can apply to organizations and individuals outside the EU under certain circumstances:

- **Providers**: If a provider, regardless of their location, places an AI system on the EU market or puts it into service within the EU, they are subject to the Act.
- **Deployers**: If AI systems are deployed within the EU, even if developed elsewhere, the deployers must adhere to the regulations.
- **Output Used in the EU**: Even if the provider or deployer is located outside the EU, if the output produced by the AI system is used within the EU, the Act applies.

How Third-Country Organizations Can Prepare for the EU AI Act

- **Understand the Act**: Thoroughly familiarize themselves with the Act's requirements, particularly the classification of AI systems into risk categories and the obligations associated with each.
- **Conduct Conformity Assessments**: If offering high-risk AI systems, implement conformity assessment procedures, potentially involving notified bodies, to ensure compliance.
- **Implement Technical and Organizational Measures**: Establish robust technical and organizational measures to address risks and ensure compliance, including data governance, risk management, and quality management systems.
- **Maintain Documentation**: Prepare and maintain technical documentation, including risk assessments, conformity assessments, and user manuals.
- **Appoint a Representative**: If not established in the EU, designate an authorized representative within the EU to act as a liaison with authorities and fulfill certain obligations.

Leading Practices for Compliance

- **Privacy by Design**: Embed privacy considerations into the design and development of AI systems from the outset.
- **Transparency and Explainability**: Ensure that AI systems are transparent and their decision-making processes can be explained, especially for high-risk systems.
- **Human Oversight**: Implement appropriate human oversight measures to monitor and control AI systems, especially for high-risk applications.
- **Robustness, Accuracy, and Security**: Ensure AI systems are technically robust, accurate, and secure to minimize risks and prevent unintended harm.
- **Data Governance**: Implement strong data governance practices, including data quality management and bias mitigation.
- **Collaboration**: Actively engage with stakeholders, including users, to understand their needs and concerns and ensure that the AI system is designed and deployed responsibly.

Cross-collaboration necessary across AI system lifecycle

"The EU AI Act introduces a complex landscape for AI supply chains, particularly those involving third-country organizations. It mandates that any AI system, regardless of origin, must comply if placed on the EU market or its output is used within the EU. This necessitates careful risk assessments, compliance checks, and potential collaboration with EU-based entities throughout the AI development and deployment lifecycle."

Dr. Ilesh Dattani, *CEO and Founder,* Assentian

To conclude, AI team and dedicated AI roles are expected to play a critical role in EU AI Act readiness journey. The next chapter provides an insight into a proposed implementation approach adopted by third-country organisations.

6. EU AI Act implementation for third-country organisations

Implementing EU AI Act requires a plan in which it is important to know which elements of EU AI Act are already in place at an organisation and which are not. These are identified by executing gap assessment. The extent of time and effort to put into a gap assessment is largely determined by the level of detail that it requires. A high degree of detail can be obtained by performing deep dives with relevant stakeholders.

Deep dives involve significant time and effort, and thus require clear scoping and co-ordination. The scoping required is determined based on the structure of the organisation and the expected current state of AI adherence.

Table 2: Expected leading sectors in third-countries that deploy or use AI systems

Input Data	Biometric Data	Input Data / Biometric Data
Telecom (55%)	Retail (71%)	IT/BPM (38%)
BFSI (52%)	Pharmaceutical (64%)	Oil (33%)
Media (50%)	Health (62%)	Internet Service (31%)

The EU AI Act, as outlined in the provided references, does not explicitly define equivalents to the GDPR-specific terms such as "online identifier," "directly identifying data," and "location data" in a direct one-to-one correspondence.

However, it does introduce concepts and definitions that encompass data types and processing activities which could relate to these GDPR terms. Based on the references provided:

1. **Online Identifier (under GDPR)**: The EU AI Act does not specifically mention "online identifiers." However, the Act discusses "input data[9]," which means data provided to or directly acquired by an AI system on the basis of which the system produces an output [Reference 1: Article 3(32)]. This broad definition could encompass online identifiers when they are used as input for AI systems.
2. **Directly Identifying Data (under GDPR)**: While the EU AI Act does not use the term "directly identifying data," it does refer to "biometric data"[10] as personal data resulting from specific technical processing related to the physical, physiological, or behavioural characteristics of a natural person, such as facial images or dactyloscopic data [Reference 1: Article 3(33)]. This type of data can directly identify an individual and thus could be considered equivalent to directly identifying data under GDPR.
3. **Location Data (under GDPR)**: The EU AI Act does not explicitly address "location data" as a distinct category. However, the Act's broad definitions of "input data" and the inclusion of "biometric data" suggest that location data could be included within the scope of data processed by AI systems, especially if it contributes to the identification or inference of information about natural persons [Reference 1: Article 3(32)][Article 3(33)].

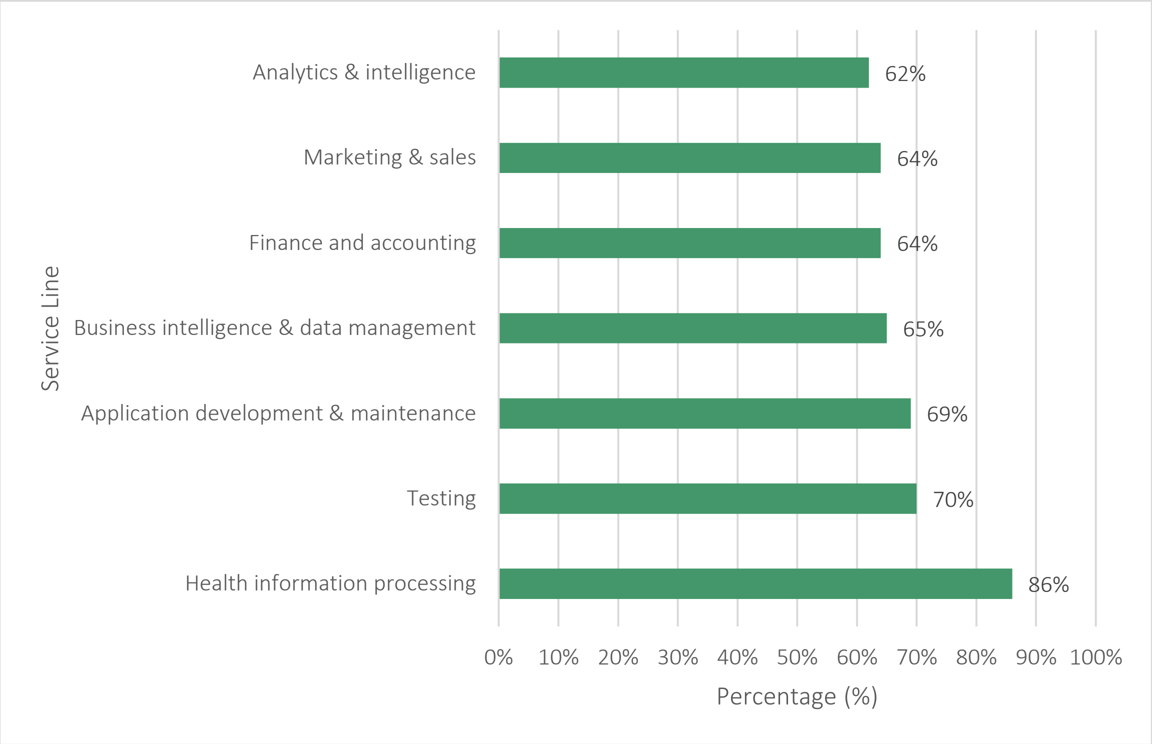
[9] data provided to or directly acquired by an AI system on the basis of which the system produces an output;

[10] personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data.

This table is indicative of the fact that AI system deployment collection is likely not limited to a few sectors. This broadly suggests how an organisation comes under the applicability of EU AI Act as it deploys AI systems in some way or the other.

6.1 Expected lines of service dealing with AI systems

Figure 10: Expected lines of service dealing with AI systems



During research activities, it was noted that 'health information processing' service line is likely to deal with the most AI systems, containing fields such as genetic data, biometrics, health information, and sexual orientation which can be traced back to an individual. Similarly, other organisations offering services such as 'testing', 'application development and maintenance', etc. also extensively indulge in usage of AI systems as deployers to various EU organisations (providers) to provide business solutions.

As per the research, anticipated leading sectors in third-countries that use and/ or deploy AI systems are the IT/BPM, BFSI and Health care sectors. Majority of high-risk AI systems are likely to reside in processing or using biometrics or health data in these sectors.

Organizations must have policies and procedures in place to identify the type of AI systems being used and/or deployed, and the relevant controls required to protect it. At all times, the AI systems At all times, the AI system lifecycle should be clearly visible to the organisation. Thus, via this research, organisations are anticipated to begin asking about their practices to maintain visibility over high-risk AI systems & prohibited AI systems. The anticipated most selected option (~63%) was "AI system classification policy has been defined and notified". This following represent the top 3 such expected leading practices.

- **63%**: AI system classification policy defined and notified.
- **45%**: Routine exercises to discover AI systems.
- **39%**: Defined responsibilities for notifying use of AI systems.

‘Implementation challenges compounded by multiple external factors’, Access Partnership

The EU AI Act, like GDPR, will inspire AI policies and governance frameworks globally, setting standards for ethical AI use across sectors. However, implementation challenges may arise, compounded by countries’ varying economic priorities, interests, and digitalization goals, leading to inconsistencies across jurisdictions.

EU AI Act – a ‘global blueprint’ for AI regulation

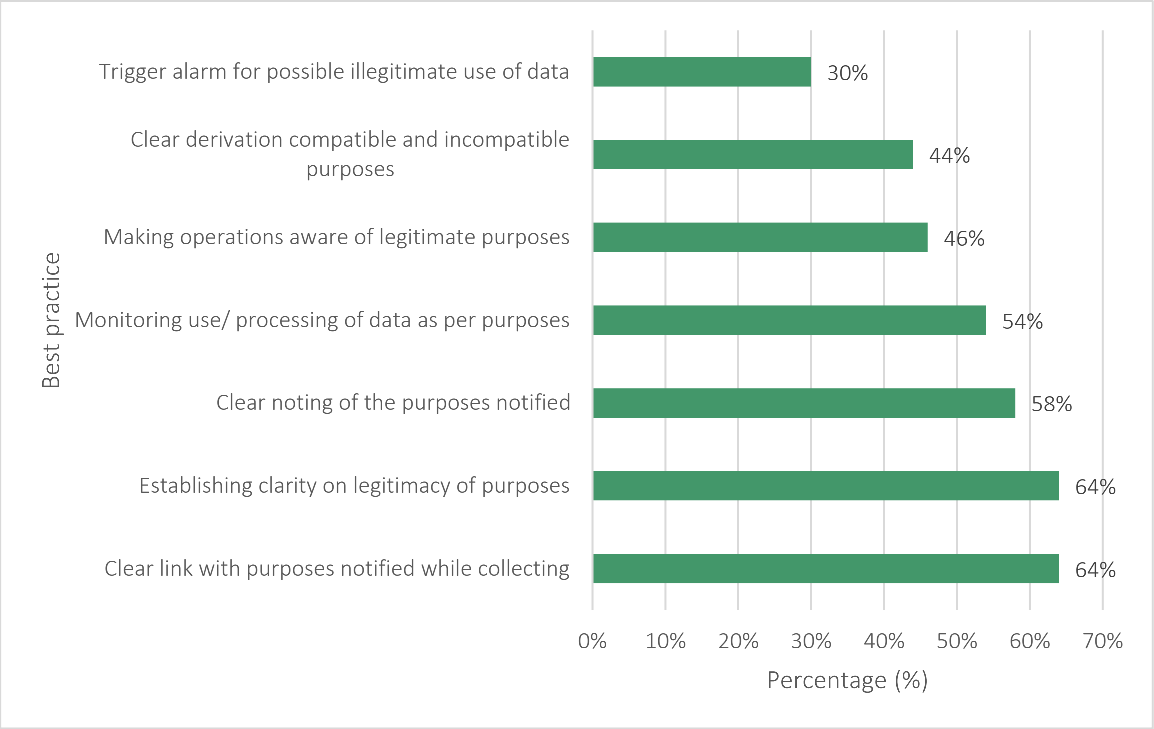
“The EU AI Act will likely inspire AI policies, regulations, and laws around the globe, encouraging ethical AI development and accelerating harmonized AI governance along the way.”

Jonathan Gonzalez, *Senior Manager,* Access Partnership

Access Partnership

6.2 Expected best practices for processing personal data within AI regulatory sandboxes

Figure 11: Expected best practices for processing personal data within AI regulatory sandboxes



Intend to convey a clear and legitimate purpose for collecting and processing personal data. Use it only for the purpose it was collected.

The most prevalent practice that seems likely is to convey a clear, legitimate purpose for collecting and processing personal data that would link to the intended use of this data (i.e. for use in an AI regulatory sandbox). Apart from the aforementioned activity, awareness amongst all operations dealing with personal data is encouraged, and triggering an alarm when it is being used illegitimately are some of the expected preferred practices by various third-country organisations.

‘Interesting battleground for non-EU firms to take into consideration’, gunner*cooke*

Third party preparedness is going to be the interesting battleground for jurisdictions such as the UK. Whilst Brexit has meant that the EU AI Act has no direct application, this means that the legislation effectively has extra-territorial impact, and raises the question of whether non-EU firms will effectively be forced by their EU counterparts to comply with the legislation, giving it a “viral” global impact.

Extra-territorial impact felt throughout AI value chain

“This paper is of ubiquitous interest for everyone in AI, as it ensure that all those outside the EU are captured, not only of they have clients in the EU, but also if those clients have clients.”

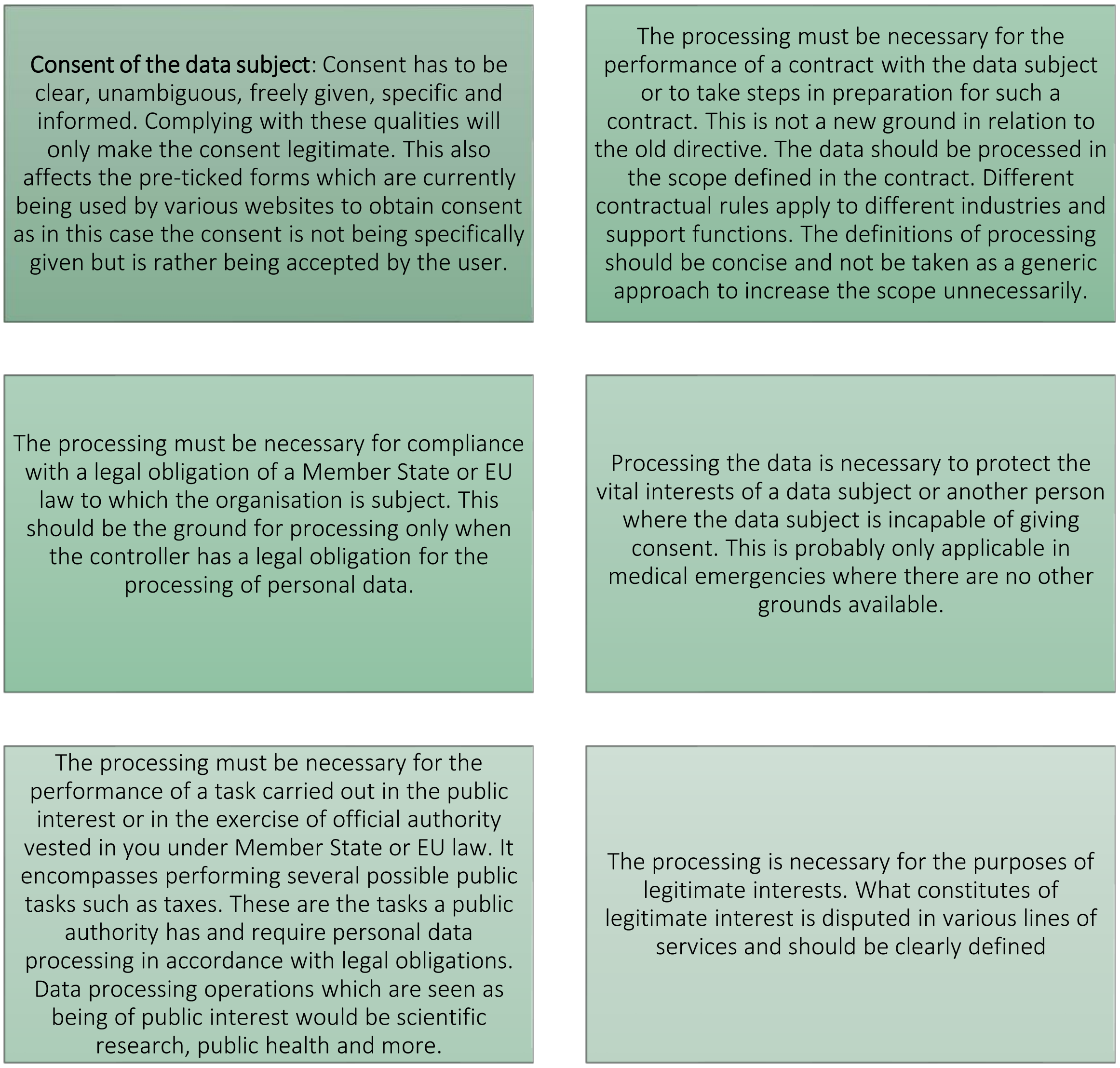
James Burnie, *Partner,* gunner*cooke*

gunner*cooke*

6.3 Expected grounds for processing personal data in AI regulatory sandbox

A closely-related expected requirement is to have legitimate grounds for processing personal data in an AI regulatory sandbox. As per the salient requirements of EU AI Act, organisations have to satisfy the following conditions:

Figure 12: Expected grounds for processing personal data in Ai regulatory sandbox



Consent of the data subject: Consent has to be clear, unambiguous, freely given, specific and informed. Complying with these qualities will only make the consent legitimate. This also affects the pre-ticked forms which are currently being used by various websites to obtain consent as in this case the consent is not being specifically given but is rather being accepted by the user.

The processing must be necessary for the performance of a contract with the data subject or to take steps in preparation for such a contract. This is not a new ground in relation to the old directive. The data should be processed in the scope defined in the contract. Different contractual rules apply to different industries and support functions. The definitions of processing should be concise and not be taken as a generic approach to increase the scope unnecessarily.

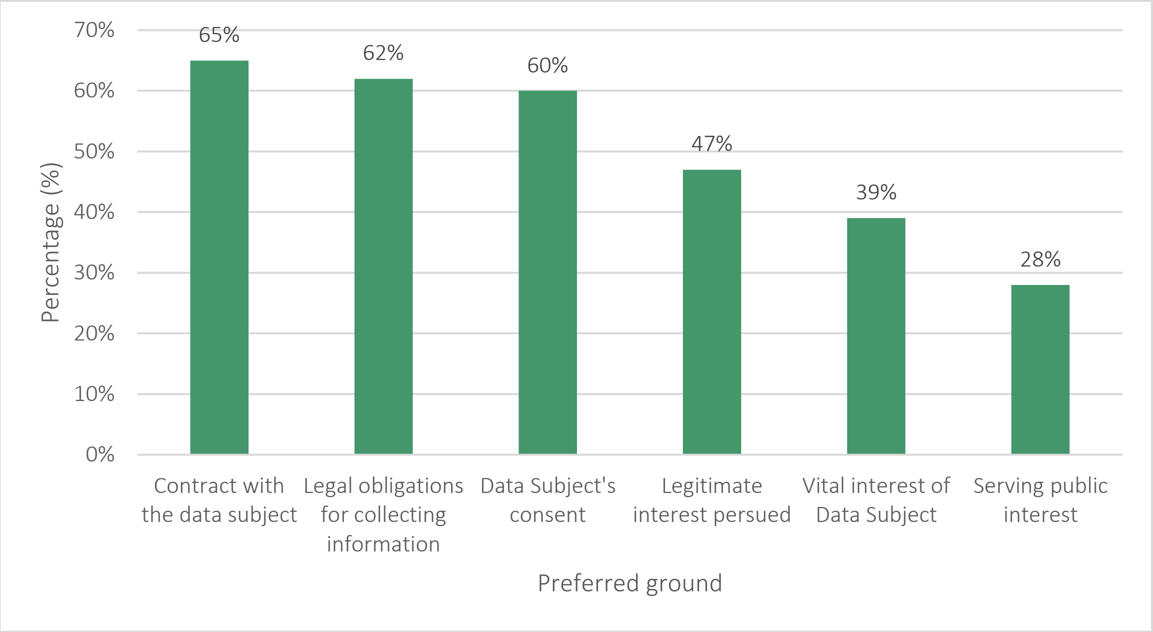
The processing must be necessary for compliance with a legal obligation of a Member State or EU law to which the organisation is subject. This should be the ground for processing only when the controller has a legal obligation for the processing of personal data.

Processing the data is necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent. This is probably only applicable in medical emergencies where there are no other grounds available.

The processing must be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in you under Member State or EU law. It encompasses performing several possible public tasks such as taxes. These are the tasks a public authority has and require personal data processing in accordance with legal obligations. Data processing operations which are seen as being of public interest would be scientific research, public health and more.

The processing is necessary for the purposes of legitimate interests. What constitutes of legitimate interest is disputed in various lines of services and should be clearly defined

Figure 13: Expected preferred grounds for processing



In the third-country context, Contractual agreement is expected to be the most preferred ground for processing personal data

Amongst these expected conditions to process personal data, the most opted forecasted condition (~65%) was "Performance of Contract with the data subject" followed by "Legal obligations demanding collection of information [e.g. KYC]" (~62%) and "Data Subject's Consent" (~60%).

6.4 Expected grounds for obtaining consent

As 'Data Subject's Consent' is expected to be one of the top conditions for envisaged lawful processing, the respondents' responses regarding the means of complying with procedural requirements associated with consent have also been provided. Majority (78%) of the respondents responses include "Identifying all possible collection & processing points where consent is required" as being key.

Forecasted conditions regarding how consent should be used for processing personal information for an AI regulatory sandbox can be strengthened. Key potential considerations include the following:

- Organisations will have to provide a genuine consent;
- The consent must be purpose-limited;
- The terms of consent should be such that the data subject is allowed withdrawal of consent at any given time.

Consent is an expected widely used ground for processing. This must have a clear form–online or offline, with clear and unambiguous language to convey the purpose and scope of processing the personal data. The terms and conditions should be clearly mentioned and presented in a visible format to the data subject. Obtaining consent can be performed in different ways as summarized later on.

'Enterprises should keep GDPR in mind for EU AI Act compliance', SumSub

European regulations with extraterritorial reach are not new for companies based outside the Union. The General Data Protection Regulation (GDPR), enforced since 2018, set a global benchmark for data privacy practices. This means that non-EU companies must keep the GDPR in mind while familiarizing themselves with the EU AI Act.

The EU AI Act, particularly in Recital 10, makes it clear that its effects, along with those of the GDPR, are cumulative rather than conflicting, meaning that these two regulations will often overlap.

As companies are already aware, the GDPR applies to any processing of personal data. The AI Act, on the other hand, applies exclusively to AI systems and General Purpose AI (GPAI) models, which are likely to involve personal data processing. In other words, the GDPR and the EU AI Act regulate different objectives.

From a compliance perspective, there are four possible scenarios:

1. **Only the EU AI Act is applicable**: For example, a company provides or deploys AI systems or GPAI models covered by the Act, but these applications do not process personal data.
2. **Only the GDPR is applicable**: For instance, the company does not provide or deploy any AI systems or GPAI models covered by the Act.
3. **Both the EU AI Act and the GDPR are applicable**: For example, a company provides or deploys AI systems or GPAI models covered by the Act, and these applications process personal data at any stage of their life cycle, such as during training, testing, or operation.
4. **Neither the EU AI Act nor the GDPR is applicable**: For instance, the company does not provide or deploy any AI systems or GPAI models covered by the Act, and these systems also do not process personal data at any stage of their life cycle.

The good news is that in scenarios where both regulations apply, compliance with the GDPR facilitates compliance with the EU AI Act. This is for two key reasons:

(i) Complementary Regulations: Policymakers intentionally drafted the Act to complement the GDPR. For example, for “high risk” systems, which need a “EU Declaration of Conformity” to indicate compliance with the Act, full compliance with the GDPR is one of the boxes to be mandatory checked.

(ii) Overlapping Provisions: The GDPR already addresses some aspects of AI regulation, particularly regarding automated decision-making and profiling. The EU AI Act builds on this by specifically targeting AI systems, introducing additional layers of compliance. For instance, AI systems that process personal data must comply with GDPR requirements for data minimization, transparency, and user rights, while also adhering to the specific obligations under the AI Act.

In summary, while the GDPR and the EU AI Act are distinct, they are highly complementary. Companies outside the EU must be aware of both regulations, as compliance is essential for any business interacting with EU markets.

sumsub

6.5 Expected explicit consent for Sensitive data

Sensitive data is a category of personal data for which taking consent explicitly is mandatory as per GDPR guidelines. Given the cross-overs between EU AI Act and GDPR, examining sensitive data is key. Explicit consent can be taken through various mediums. Data collected indicates that the prevalent practices likely to be followed in the industry is to obtain explicit consent.

Expected methods of obtaining explicit consent includes:

- **69%:** Filling an electronic form
- **60%:** Written form
- **38%:** Logging data subjects' actions
- **33%:** Sending an email
- **27%:** Scanned document carrying a signature
- **27%:** Opt-in mechanism

It is noted that filling electronic and written forms are expected to be the most widely used methods to gain explicit consent.

While the data that 78% of the organisations are likely dealing with any type of sensitive data, they consider 'consent' as their grounds for processing, 69% are expected to believe that filling an electronic form is the most widely accepted method of providing consent.

'Setting a standard for responsible data management in telecommunications industry', TelcoSolve

TelcoSolve integrates GDPR principles into the core of our ICT solutions, ensuring data privacy and protection are paramount. This approach not only enhances compliance but also builds trust with users, setting a standard for responsible data management in the telecommunications sector.

Enhanced data privacy, higher digital resilience

"At TelcoSolve, we empower telecommunications with robust ICT solutions that enhance data integrity and operational efficiency, ensuring resilience in the face of evolving digital challenges."

Shivaprasad M (Shiva), *Co-Founder and CEO,* TelcoSolve

TelcoSolve™

To conclude, it is envisaged that the processing of personal data in an AI regulatory sandbox, as per the requirements of both EU AI Act and GDPR, will not only help organisations conduct business with ease in the EU and EEA, but also help their customers, vendors and suppliers consider them as trustworthy. The next chapter provides a view on how organisations can prepare their extended teams (vendors, contractors, etc.) for EU AI Act readiness.

7. Maintaining concurrence with EU AI Act

Implementation of EU AI Act in an organisation is not a one-time activity but a constant process which has to be embedded in the culture of the organisation to face any challenges that might arise in the future. According to Title III / Chapter 3 of EU AI Act, there are certain obligations that have to be abided by the providers and deployers of high-risk AI systems. These obligations are fulfilled by implementing appropriate technical and organisational measures to comply with the procedural requirements of EU AI Act. A deployer should use only those providers who comply with the requirements (and vice-versa), and the engagement between them should be governed by a contract. The contract contains the subject-matter and the duration of the deployment. Other requirements should also be mentioned in the contract such as record keeping activities, fundamental rights impact assessment ("FRIA"), etc.

With the future enforcement of EU AI Act, many organisations will have to revise these contracts to reflect upon the new arrangements of liability sharing and the clauses within these contracts.

Prior to EU AI Act, contracts that were signed between organisations regarding deployment and sharing the liability were not mandatory. From the data, a change is foreseen regarding this scenario as more and more organisations will now have comprehensive discussions on the sharing of liability. A blanket policy is a policy which covers a plethora of liabilities. With EU AI Act enforcement on the horizon, it is likely that the conditions that come under blanket policies will be pushed by the clients to increase liabilities on service organisations. The requirements and obligations to be fulfilled with respect to EU AI Act are covered in the sections below.

7.1 Records of events

As per Article 12, EU AI Act expects organisations to ensure that high-risk AI systems maintain records relating to the automatic recording of events over the duration of the lifetime of the system.

Any organisation irrespective of its size is expected to adhere to this requirement if they handle vast amounts of AI systems, regardless of their risk classification, as referred to in Article 5 and/or 6. According to the data, organisations with less than 250 employees are likely to strongly believe that they have central visibility over all AI system activities and so this requirement (records of high-risk Ai systems) may not apply. Organisations with more than 10,000 employees are likely to believe that policies and format for maintaining records is an important step for them.

Figure 14: Expected changes in contracts due to EU AI Act

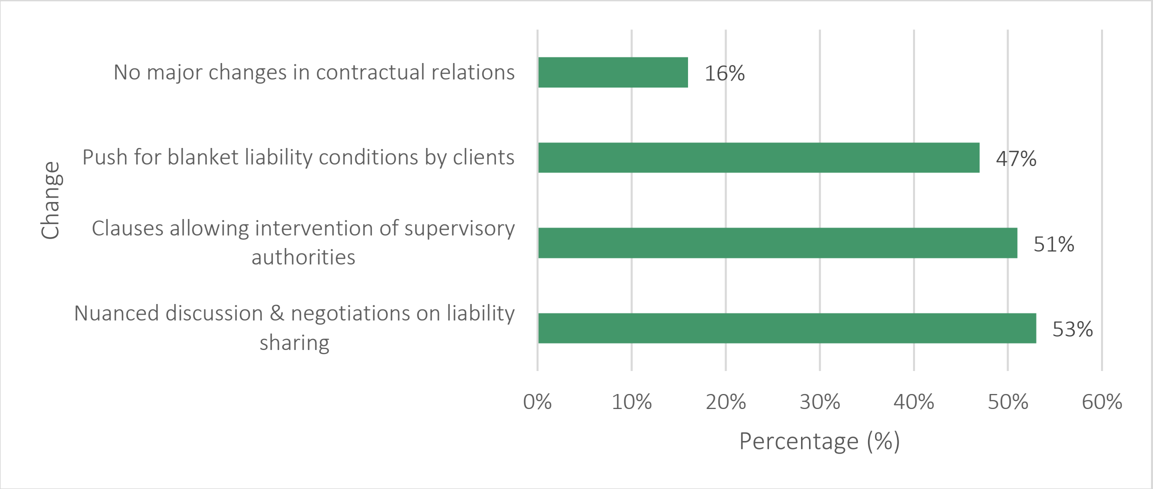


Table 3: Likely steps to take for record-keeping

Likely steps taken for record-keeping		
Firm Size < 250	Central visibility over all AI system activities (47%)	This requirement is not applicable to my organisation (27%)
Firm Size > 10,000	Organisational policy, guidance & format for maintaining record of the AI system activities (58%)	Obligation on business operations to inform the deployment of AI systems (47%)

7.1.1 Trustworthy AI by design

The standardized and repeatable process of trustworthy AI by design and by default ensures that the organisations understand the appropriate AI controls as a project begins, rather than only considering AI governance as a checkbox exercise. This enables not only AI teams, but also security teams to help provide advice, guidance, and review the process from the beginning itself.

'EU AI Act – Paradigm shift for AI Governance', DLT Hub

The EU AI Act's extraterritorial scope highlights the critical need for organizations to adopt a socially responsible approach to AI. By integrating ethical considerations and community-focused solutions, we can ensure that emerging technologies not only comply with regulations but also drive positive social impact across global communities.

Preparedness requires enterprise positioning at forefront of ethical AI deployment

"The EU AI Act represents a paradigm shift for AI governance. Preparedness is not just about compliance; it's about positioning your organization at the forefront of ethical AI deployment."

Ozgur Kaplan*, Founder/CVO,* DLT Hub

7.1.2 Security of Processing

Taking into account the sensitivity of the personal data processed in an AI regulatory sandbox, the provider and the deployer can implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks involved:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

The provider and the deployer must also take steps to ensure that any person who has access to personal data under their authority does not process it unless required by the law or instructed by them.

7.1.3 AI System Lifecycle Management:

AI risk management intersect with other AI system lifecycle management programs within an organisation. A good management program must continually assess and review who needs access to what types of information.

- Organize the collected AI systems: The AI systems that are used by the organisation must be logged and maintained in a secure place. Its access should only be on a need-to-know basis;
- An authorization structure should be in place to prevent misuse of AI systems;
- There must be deletion and retention rules in place for the deployed AI systems that no longer serves the business purpose.

7.1.4 Fundamental Rights Impact Assessment (FRIA):

FRIAs should be conducted as soon as a new technology comes into effect, so as to incorporate the measures identified by it, into the updated policies of the organisation. In order to enhance compliance with the EU AI Act where AI system operations are likely to result in a high risk to the safety, health, and fundamental rights of individuals, the provider should be responsible for carrying out a FRIA to evaluate, in particular, the origin, nature, particularity and severity of that risk. It should be conducted as soon as a new technology comes into effect, so as to incorporate the measures identified by it, into the updated policies of the organisation.

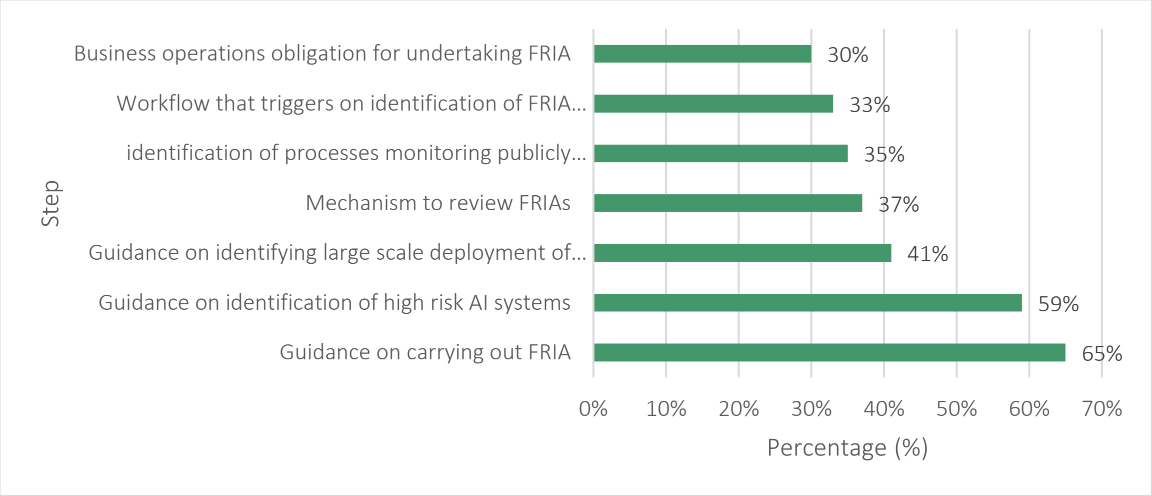
In such cases, the provider of an organisations needs to define the circumstances under which a FRIA is to be conducted. That impact assessment should include the measures, safeguards and mechanisms envisaged for mitigating the risks, ensuring the trustworthiness of AI systems and demonstrating compliance with EU AI Act.

A FRIA is especially required in the following cases:

- A systematic and extensive evaluation of personal aspects relating to natural persons which is based on AI system deployment and/or use, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
- Deployment of AI systems on a large scale.
- A systematic monitoring of individuals in a publicly accessible area on a large scale using AI systems.

7.2 Fundamental Rights Impact Assessment (FRIA)

Figure 15: Anticipated steps taken towards FRIA



65% organisations are likely to issue internal guidance to conduct the FRIA

FRIAs are expected to help organisations identify, assess, and mitigate or minimize AI risks with AI system activities. They are particularly relevant when a new AI systems are deployed or related processes, systems, or technologies are being introduced. However, FRIAs are of limited applicability. They apply only to deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III.

The likely guidance issued by organisations include assessment measures and procedures. An FRIA assesses the impact on fundamental rights that the use of a high-risk AI system may produce. Specifically, a FRIA involves:

1. A description of the deployer's processes in which the high-risk AI system will be used, aligning with its intended purpose.
2. A description of the period and frequency of the high-risk AI system's intended use.
3. The categories of natural persons and groups likely to be affected by its use in the specific context.
4. The specific risks of harm likely to impact the identified categories of persons or groups, taking into account information provided by the AI system's provider.
5. A description of the implementation of human oversight measures, according to the instructions of use.
6. The measures to be taken in case of the materialization of these risks, including arrangements for internal governance and complaint mechanisms [Reference 2: Article 29a].

The FRIA is not mandatory when the deployment of an AI system is not high-risk, for instance, the deployment of an AI system for use in a non-professional, personal capacity.

FRIA also are likely to identify the trustworthy AI solutions that will mitigate the risks. The decisions taken after the assessment should be documented as part of the FRIA process. Where necessary, the provider will carry out a review to assess if deployment is performed in accordance with the FRIA at least when there is a change of the risk represented by deployment operations.

As per the data, the support that organisations are likely to require for conducting FRIAs are as below:

Table 4: Likely steps to take for FRIA

Likely steps taken for record-keeping	
Provider	Business Operations obligation for undertaking FRIA on requires circumstances (55%)
Deployer	Guidance on identification of high risk AI systems (74%)

7.2.1 Appointing a Data Protection Officer (DPO)

To effectively perform the duty of maintaining the AI function of an organisation, large corporations, government bodies, organisations in the health and social care sectors, financial institutions, and most organisations based in the EU are likely to, but are not mandated to, appoint a AIO who would be responsible for formulating AI strategy and make the organisation compliant with EU AI Act requirements.

EU AI Act names multiple entities involved in the deployment of data, including the developer, deployer and appointed representative. The main task of the AIO is likely to be working closely with these AI system deployment entities and ensure their compliance with the EU AI Act requirements. He/she also should play a passive role in trustworthy AI by training staff and raising awareness on data protection.

EU AI Act potentially advocates the following tasks of AIOs which are:

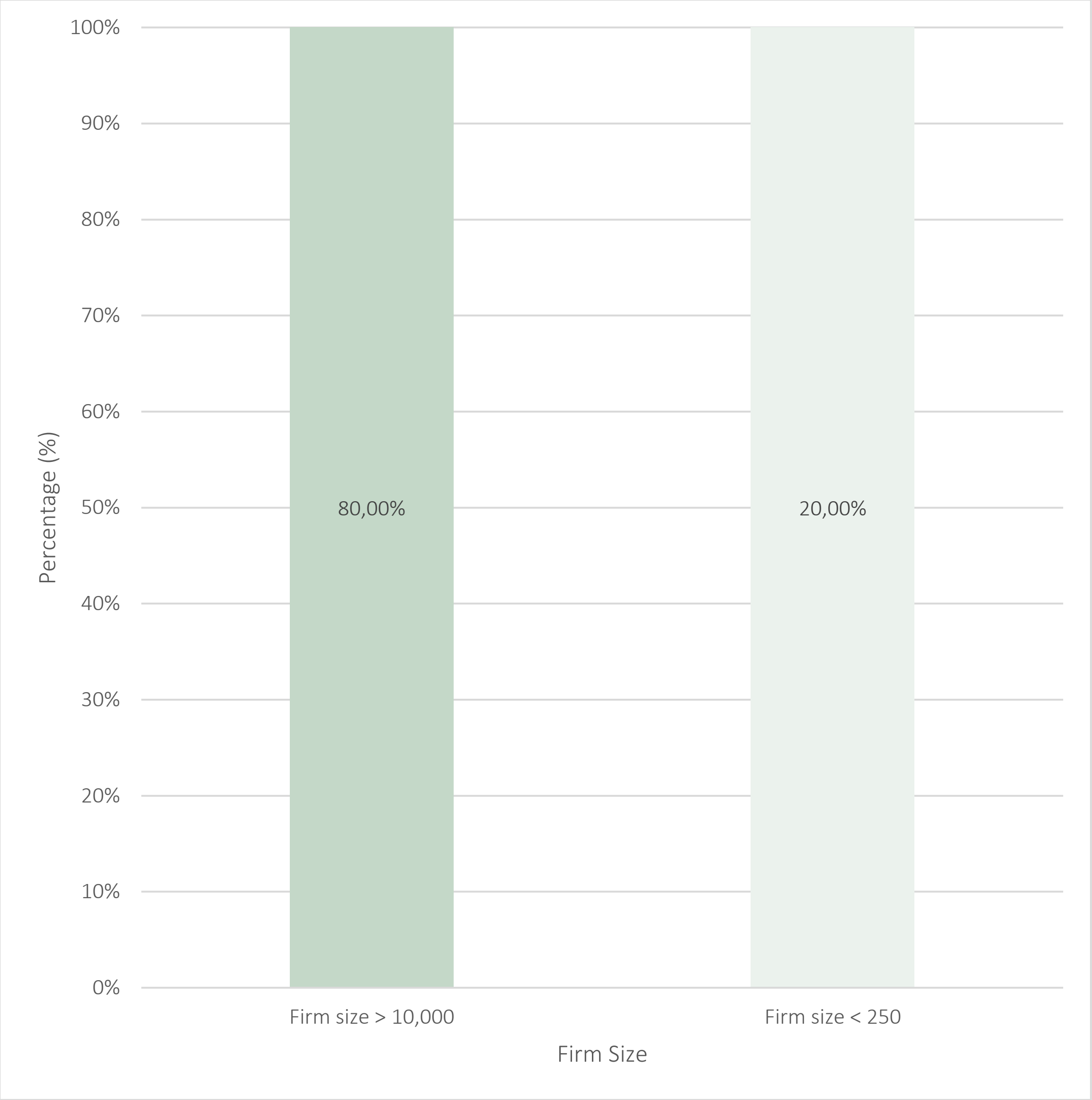
- To inform and advise the provider and the deployer of their obligations to the Regulation.
- To monitor compliance with the regulation.
- To provide advice where requested about trustworthy AI.
- To cooperate with the supervisory authority.

Potential cases for appointment of a AIO are mentioned below:

- The deployment is carried out by a public authority or body, except for courts acting in their judicial capacity.
- The core activities of the deployer or the provider consist of high-risk AI systems which require regular and systematic monitoring on a regular basis.

7.3 AIO Appointment

Figure 16: Expected firm size vs. AIO appointment

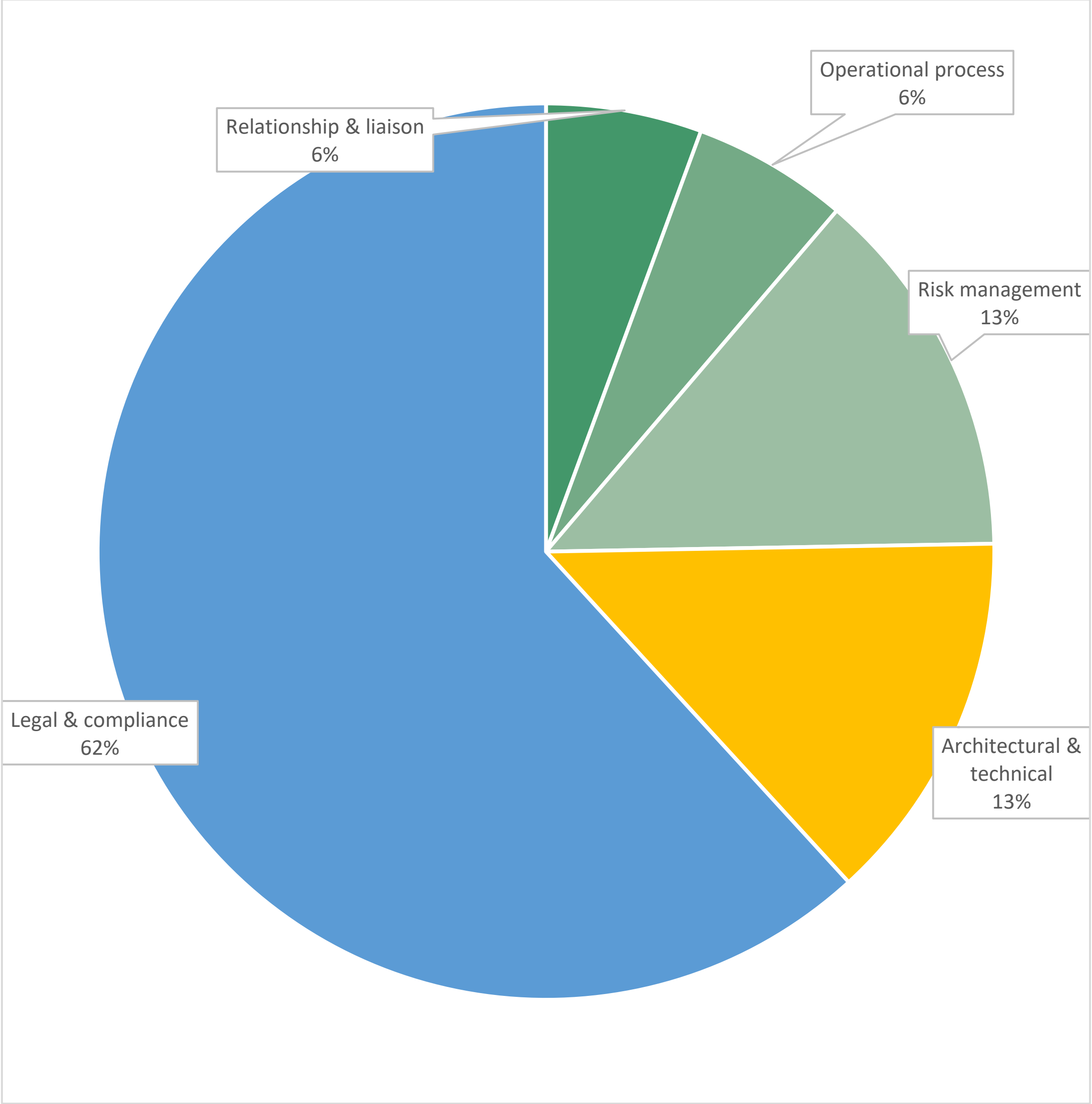


80% of large third-country are likely to choose to appoint a AIO, on the other hand, only 20% of SMEs are expected to appoint a AIO.

Large third-country firms are anticipated to appoint a AIO proactively as a part of their readiness activities as compared to third-country SMEs.

Talking about the anticipated qualifications of AIO, the degree of risk of an AI system that an organisation is deploying and using should be directly proportionate to the expertise and skills of the AIO that they appoint. They should be able to fulfil their duties which are required out of him.

Figure 17: Anticipated preferred skills in an AIO



55% of third-country organisations are expected to indicate legal & compliance as their most preferred skill set while appointing a AIO.

Organisations are expected to appoint AIOs who have a background on the Legal and Compliance requirements.

8. Caveats to the Report

There are inherent limitations to the Report that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most ex-ante based research reports based on forthcoming legislation.

- **Divergence in Regulatory Intent**: While the GDPR may share similarities with the EU AI Act, it is essential to recognize potential differences in regulatory goals and objectives. Variances in legislative intent or policy priorities could lead to divergent outcomes despite surface-level similarities.
- **Contextual Disparities**: The socio-economic, political, and cultural contexts surrounding the GDPR and EU AI Act are likely to differ significantly. These contextual variations can influence stakeholder behaviour, enforcement mechanisms, and overall regulatory effectiveness, thereby impacting the validity of direct comparisons and inferences.
- **Evolution of Stakeholder Dynamics**: Stakeholder dynamics, including the composition, interests, and influence of relevant parties, may have evolved between the implementation of the GDPR and the EU AI Act. Changes in stakeholder engagement strategies or power dynamics can alter the regulatory landscape and its outcomes.
- **Methodological Limitations**: Any inferences drawn from the Study must be tempered by an acknowledgment of its methodological limitations. Factors such as sample size, research design, data quality, and the generalizability of findings could impact the reliability and applicability of conclusions to the current EU AI Act regulatory environment.
- **Unforeseen External Factors**: External variables that were not accounted for in the Study may exert significant influence on the outcomes of the EU AI Act. These could include technological advancements, shifts in market dynamics, or unforeseen events such as global pandemics, all of which may shape regulatory implementation and outcomes in unforeseen ways.
- **Dynamic Regulatory Environment**: Regulatory frameworks are subject to continuous evolution and adaptation in response to changing societal needs, political priorities, and emerging challenges. Therefore, while insights from the GDPR can provide valuable guidance, it is imperative to recognize the dynamic nature of regulatory environments and exercise caution when extrapolating findings to inform future regulatory decisions.

Annex A – EU AI Act GDPR Equivalents: Actors

This section outlines the potential cross-overs between these two EU pieces of legislation to emphasize how making inferences can inform insights for the other (and vice-versa).

Table 5: Comparison between EU AI Act and GDPR in terms of in-scope actors

EU AI Act	GDPR	Comment
Provider	Data Controller or Data Processor	The 'provider' under the EU AI Act is akin to both 'data controller' and 'data processor' in GDPR. A 'data controller' determines the purposes and means of processing personal data, while a 'data processor' processes personal data on behalf of the controller. Both roles involve developing, deploying, or operating systems AI systems in the EU AI Act and data processing systems in GDPR) under their authority.
Deployer	Data Controller	The 'deployer' in the EU AI Act closely resembles the 'data controller' in GDPR, as both are entities that use the system (AI or data processing) under their authority for specific purposes, except for personal or household activities.
Authorised Representative	Concept of Representation	The concept of an 'authorised representative' in the EU AI Act, who acts on behalf of a provider, is somewhat mirrored in GDPR by the requirement for non-EU entities to appoint a representative within the EU to interact with supervisory authorities and data subjects.
Importer	Concept of Representation or Data Importer	The 'importer' role, specific to bringing AI systems from outside the EU into the Union market, can be loosely compared to GDPR’s concept of data importers or representatives of non-EU data controllers/processors who must ensure compliance with EU data protection standards when importing data.
Distributor	No direct equivalent	The 'distributor' role in the EU AI Act, which involves making AI systems available on the Union market, does not have a direct equivalent in GDPR. However, any entity involved in the distribution chain could be considered a data processor if they process personal data on behalf of a data controller.
Operator	Data Controller or Data Processor	The 'operator' encompasses several roles (provider, product manufacturer, deployer, authorised representative, importer, or distributor) in the EU AI Act, similar to how both 'data controllers' and 'data processors' cover various entities involved in data handling under GDPR.

Annex B – EU AI Act GDPR Equivalents: Activities

This section outlines the potential cross-overs between these two EU pieces of legislation to emphasize how making inferences can inform insights for the other (and vice-versa).

Table 6: Comparison between EU AI Act and GDPR in terms of in-scope activities

EU AI Act	GDPR	Comment
Making available on the market	Data processing	Akin to the GDPR's concept of 'Data Processing'. While the EU AI Act discusses the supply of AI systems for commercial activity, GDPR regulates the processing of personal data, which can include the distribution or use of data processing systems or services.
Putting into service	Data Collection and Use	Resembles the GDPR's 'Data Collection and Use'. This term refers to the initial use of data or systems for processing personal data, aligning with the GDPR's focus on how personal data is collected and used for its intended purpose.
Instructions for use	Privacy Notices or Data Protection Notices	Can be compared to the GDPR's 'Privacy Notices' or 'Data Protection Notices'. These notices inform data subjects about the purpose and methods of data processing, similar to how instructions for use inform users about the intended purpose and proper use of an AI system.
Recall of an AI system	'Right to Erasure'	No direct equivalents in GDPR, as they specifically pertain to the physical or functional removal of AI systems. However, they conceptually align with GDPR's 'Right to Erasure' (also known as the right to be forgotten), which allows data subjects to have their personal data erased under certain conditions.
Withdrawal of an AI system	'Right to Erasure'	No direct equivalents in GDPR, as they specifically pertain to the physical or functional removal of AI systems. However, they conceptually align with GDPR's 'Right to Erasure' (also known as the right to be forgotten), which allows data subjects to have their personal data erased under certain conditions.
Informed consent	Consent	Closely mirrors the GDPR's concept of 'Consent'. GDPR defines consent as a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, through a statement or a clear affirmative action, signify agreement to the processing of personal data relating to them. This definition aligns with the notion of informed consent for participation in testing, emphasizing the importance of voluntariness and awareness of the testing's aspects.

Annex C – EU AI Act GDPR Equivalents: Principles

This section outlines the potential cross-overs between these two EU pieces of legislation to emphasize how making inferences can inform insights for the other (and vice-versa).

Table 7: Comparison between EU AI Act and GDPR in terms of overarching principles

EU AI Act	GDPR	Comment
Human Agency and Oversight	Accountability	The EU AI Act emphasizes the importance of human oversight for high-risk AI systems, ensuring they can be effectively overseen by natural persons during their use. This aligns with the GDPR's principle of accountability, where data controllers must ensure and demonstrate compliance with data protection principles.
Technical Robustness and Safety	Integrity and Confidentiality	The EU AI Act requires high-risk AI systems to be developed based on training, validation, and testing data sets that meet quality criteria. GDPR does not directly address technical robustness but mandates the security of personal data processing through appropriate technical and organizational measures (Article 32, GDPR).
Privacy and Data Governance	Data Minimisation, Purpose Limitation and Accuracy	The EU AI Act specifies conditions for processing personal data for bias detection and correction in high-risk AI systems, including technical limitations and state-of-the-art security measures. GDPR's core focus is on the protection of personal data, with principles such as data minimization, purpose limitation, and ensuring data accuracy (Articles 5-6, GDPR).
Transparency	Lawfulness, Fairness and Transparency	The EU AI Act mandates that high-risk AI systems be designed to ensure their operation is transparent, enabling deployers to interpret the system's output and use it appropriately. GDPR emphasizes transparency in the processing of personal data, requiring clear communication to data subjects about how their data is used (Articles 12-14, GDPR).
Diversity, Non-Discrimination and Fairness	Lawfulness, Fairness and Transparency	The EU AI Act requires examination of possible biases in training, validation, and testing data sets and measures to prevent and mitigate these biases. GDPR addresses non-discrimination implicitly through the principles of fairness and accuracy in data processing and explicitly in the context of automated decision-making and profiling (Article 22, GDPR).

Table 7: Comparison between EU AI Act and GDPR in terms of overarching principles (continued)

EU AI Act	GDPR	Comment
Societal and Environmental Well-Being	No direct equivalent	While the EU AI Act does not explicitly mention environmental well-being in the provided references, it addresses societal impacts by facilitating the development of AI systems in regulatory sandboxes with safeguards to protect fundamental rights and society. GDPR does not directly address societal or environmental well-being but contributes to societal trust by enforcing strict data protection standards.
Accountability	Accountability	The EU AI Act includes provisions for record-keeping and documentation to justify the processing of special categories of personal data for bias detection and correction. GDPR establishes the principle of accountability, requiring data controllers to implement measures that ensure and demonstrate compliance with the regulation (Article 5(2), GDPR).

Annex D – EU AI Act GDPR Equivalents: Rights

This section outlines the potential cross-overs between these two EU pieces of legislation to emphasize how making inferences can inform insights for the other (and vice-versa).

Table 8: Comparison between EU AI Act and GDPR in terms of rights for individuals

EU AI Act	GDPR	Comment
Right to explanation	Right of access by the data subject	The EU AI Act does not directly replicate the GDPR's right of access by the data subject. However, Article 68c provides a right to explanation for individuals affected by decisions made by high-risk AI systems, which could be seen as a form of access to information about how personal data is used in decision-making.
No direct equivalent	Right to rectification	The EU AI Act does not explicitly include a right to rectification akin to the GDPR. The focus of the AI Act is more on the systemic requirements for AI systems, including documentation, transparency, and safety measures, rather than individual rights to modify personal data.
No direct equivalent	Right to erasure ('right to be forgotten')	Similar to the right to rectification, the EU AI Act does not directly address the right to erasure. However, the Act mandates that personal data processed for bias detection and correction in high-risk AI systems must be deleted once the bias has been corrected or the data has reached the end of its retention period.
No direct equivalent	Right to restriction of processing	The EU AI Act does not provide a direct equivalent to the GDPR's right to restriction of processing. The Act's provisions are more focused on the conditions under which AI systems can process data, especially for bias detection and correction, rather than allowing individuals to limit such processing.
No direct equivalent	Right to data portability	The EU AI Act does not include a provision equivalent to the GDPR's right to data portability. The Act's scope is centered on the regulation of AI systems' development, deployment, and use, rather than on the rights of individuals to transfer their data between controllers.
No direct equivalent	Right to object	There is no direct equivalent to the GDPR's right to object in the EU AI Act. However, the Act does provide mechanisms for oversight and enforcement by national authorities, including the ability to request documentation and conduct testing of high-risk AI systems to ensure compliance with fundamental rights obligations.

Annex E – EU AI Act GDPR Equivalents: Dates

This section outlines the potential cross-overs between these two EU pieces of legislation to emphasize how making inferences can inform insights for the other (and vice-versa).

Table 8: Comparison between EU AI Act and GDPR in terms of dates

EU AI Act	GDPR	Comment
Entry into Force		
At August 2024	At May 2016	The regulation shall enter into force on the twentieth day following its publication in the Official Journal of the European Union.
Transition Period		
August 2024 – August 2026	May 2016 – May 2018	The regulation shall apply from 24 months following its entry into force. This period allows Member States, institutions, and AI system providers and deployers to prepare for compliance. • Titles I and II, concerning prohibitions, will apply from six months following the entry into force of the regulation. • Title III Chapter 4, Title VI, Title VIIIa, and Title X, covering various regulatory aspects including penalties, will apply from twelve months following the entry into force. • Article 6(1) and corresponding obligations will apply from 36 months following the entry into force 2. Regulatory Sandboxes: By the date of general application (24 months after entry into force), at least one regulatory sandbox per Member State shall be operational, or the Member State must participate in the sandbox of another Member State.
Entry into Application		
At August 2026	At May 2018	See above.

About AI & Partners

AI & Partners – 'AI That You Can Trust'

Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialize in providing comprehensive and tailored solutions for companies subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organizations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Contacts

Sean Donald John Musch, Founder/CEO, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, Founder/CEO, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Acknowledgements

Corporate Partners

We are grateful to our network of corporate partners for their invaluable contributions:

OP

AF
AFAQ AI

TelcoSolve™

CYBERSECURITY UNITY
be safe, be sure, BE SECURE

rialto
ACCELERATED IMPACT

Wriben
Consultancy
Services
Expert AI, information and cyber security advisor experienced in guiding Boards on organisational risk and improvement opportunities.

sumsub

ARKSTONS

Access
Partnership

gunnercooke

BOARD OS
BOARD OPERATING SYSTEM

Kliemt.
ARBEITSRECHT

AIX
AI EXCHANGE
POWERED BY HR.COM

DLT
HUB
CIC

jc legal
bespoke solutions

EMPOWERING B2B MARKETERS
FinTech
MARKETING

EDMUND

AZ
AZNAR LEGAL & COMPLIANCE

unbiasfy

Individual Partners

We are also grateful to our network of individual supporters for their invaluable contributions:

Adam Leon Smith, Adam Leon Smith is an expert in AI regulation and technical standards and works on research and strategy projects in that area. He is Deputy Chair of the UK's national AI standards committee and has delivered multiple technical AI standards. Before involvement in quality infrastructure, Adam spent 20 years in senior technology roles, delivering verification and validation solutions for highly complex or high-risk industry challenges. He was the Editor and Contributing Author of the BCS book AI and Software Testing. He also worked with ISTQB to develop their AI Software Testing Certification and trained several organisations in AI testing concepts. He is also chair of BCS's F-TAG Committee, which advises BCS on technology policy. In 2024, the University of Bath awarded Adam an honorary doctorate in recognition of his work and its impact on the profession, including standards-making.

Binesh Balan, A seasoned investment specialist and strategist with extensive experience in venture capital, mergers and acquisitions, private equity, and impact investments. He is the General Partner of Arkstons Global Ventures, a US-based venture capital fund, and leads the Arkstons Group of Companies, a global investment banking advisory firm with offices in Bahrain, the UK, and India. He maintains strong relationships with prominent family offices, business groups, high-net-worth individuals, venture capital, and private equity funds across the Middle East, Europe, the US, and Asia. His achievements have earned him multiple recognitions as an 'Innovative Business Leader'.

Charles Epstein, Charles Epstein, co-founder and manager of AIX (AI Exchange), a learning community developed in association with HR.com that provides HR professionals with expert and peer-to-peer answers, guidance, and support on the myriad challenges poised to disrupt HR and workforce dynamics.

Dr Ilesh Dattani, Dr Ilesh Dattani is the CTO and Founder of Assentian - a Cyber Security and AI Lab based in the UK, USA and Ireland. Ilesh has spent the last 25 years leveraging emerging technologies like Artificial Intelligence into disruptive new innovations aimed at transforming and optimising mission and business critical systems and services across a diverse array of sectors and applications including financial services, civil aviation, construction, nuclear energy, supply-chain management and Cyber Security. He is an investor in and mentor to AI start-ups in Europe, the United States, Kenya, Singapore and Australia. Ilesh is a Certified Information Security Auditor, a Chartered Engineer and has a first degree and masters in Mathematics and a Phd in Artificial Intelligence.

Elliott Day, Elliott Day is a Senior Compliance & Financial Crime Consultant at Edmund Group, a UK consultancy specialising in risk, compliance & financial crime prevention.

Enrique Aznar, Enrique Aznar is a legal and compliance expert with extensive experience in corporate governance, business ethics, and tech-law. A professor of business ethics, he has led compliance programs for multinational organizations, ensuring alignment with global regulations and fostering ethical practices in the tech industry and beyond.

Jakob F. Krüger, Jakob F. Krüger advises national and international companies. He specialises in the preparation of dismissals and subsequent litigation. He also advises clients on the drafting of employment, cancellation and severance agreements as well as on issues of works council constitution law. Jakob F. Krüger is an active member of the International Practice Group for Data Privacy at Ius Laboris, the association of leading international labour law firms, and frequently advises on the interface between labour law and data protection, e.g. on the introduction of IT systems.

Jonathan Gonzalez, Jonathan has 17 years' experience working with multilateral organisations (World Bank, Asian Development Bank, OECD, UNESCO, APEC, and ASEAN) and leading technology companies to develop whitepapers and reports on a wide range of policy issues, including the digital transformation of governments and the impact of AI in Asia's digital economies.

Lavinia Osbourne, Lavinia Osbourne is the co-founder and CEO of Unbiasfy, an AI Data Management provider, training & sourcing data sets to be unbiased.

Lisa Ventura MBE, Lisa Ventura MBE is an award-winning cyber security specialist, published writer/author, and keynote speaker. She is the Founder of Cyber Security Unity, a global community organisation that is dedicated to bringing individuals and organisations together who actively work in cyber security to help combat the growing cyber threat. As a consultant Lisa also works with cyber security leadership teams to help them work together more effectively and provides cyber security awareness and culture training, and training on the benefits of hiring those who are neurodiverse. She has specialist knowledge in the human factors of cyber security, cyberpsychology, neurodiversity and AI in cyber, and is also a Co-Founder of International Imposter Syndrome Awareness Day. More information about Lisa can be found on www.lisaventura.co.uk.

Michael Boevink, Michael Boevink has more than 20 years management experience in the fintech and banking industry and is founder of his own investment company Boevink Group. Mr. Boevink specialises in capital raising, scaling and executing go-to-market strategies and business development growth in global markets and is engaged in companies as Raimac Financial Technology - Raimac.io - a programmable payment solution. He holds an MBA from the University of Bradford.

Steven PAUL CDir, FIoD. Steven Paul a Chartered Director and Transformation leader brings over 2 decades of global leadership across over 30 countries, driving strategic transformations and building enterprise value in diverse sectors. As a seasoned board director and executive leader, Steven's profound expertise in business transformation, mergers, and Gen AI-driven strategies has been instrumental in steering organisations towards sustainable growth and innovation. His leadership extends beyond traditional boundaries, encompassing a robust commitment to developing authentic leaders and impactful boards especially in the era of Gen AI, making him a trusted advisor and architect of change in the international business landscape. Steven is educated at Harvard and is a Fellow of the Institute of Directors. For further information, https://linktr.ee/steven.paul.

Vibhav Mithal, Vibhav Mithal is an Associate Partner at Anand and Anand and is practicing as an intellectual property litigator for over 8 years. Vibhav has been a part of many path breaking litigations such as the Aloys Wobben dispute (Supreme Court, 2014); Roche v. Cipla (Delhi High Court, 2015); Shree Nath v. ABD (Delhi High Court, 2015); Monsanto dispute (Supreme Court, 2019), Ferid Allani (Delhi High Court, 2019 &amp; Intellectual Property Appellate Board, 2020) and Armasuisse (Delhi High Court, 2023). Vibhav regularly contributes to leading IPR publications such as Managing Intellectual Property magazine, Computer and Telecommunications Law Review, Asia Business Law Journal, the Intellectual Property Law Review and Patent Litigation Review and has also co-authored the India Chapter in Global Patent Litigation (3rd Edition, 2019) published by Bloomberg Law. Vibhav has also been recognized by Managing Intellectual Property as a Rising Star, 2022 and 2023.

Important notice

This document has been prepared by AI & Partners B.V. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of AI & Partners B.V. to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V.