AI & Partners

Amsterdam – London - Singapore

EU VS. US

Race to Compliance

Examining the potential state of compliance of organisations based in the United States (US) and European Union (EU) with the requirements of the EU Artificial Intelligence (AI) Act following its entry into force on 1st August 2024.

October 2024

AI & Partners

Amsterdam – London - Singapore

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, following the EU AI Act's entry into force on 1st August 2024, many companies may not meet the compliance deadline following the two-year transition period, although this depends on how they learn from the lessons brought by similar regulatory regimes, such as GDPR. Moreover, many companies may be behind schedule in implementing the risk management, governance and compliance processes needed to ensure that they meet the EU AI Act's requirements and obligations if they do not take necessary measures.

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 compliance for companies in the United States and Europe given its analogous nature.

Contents

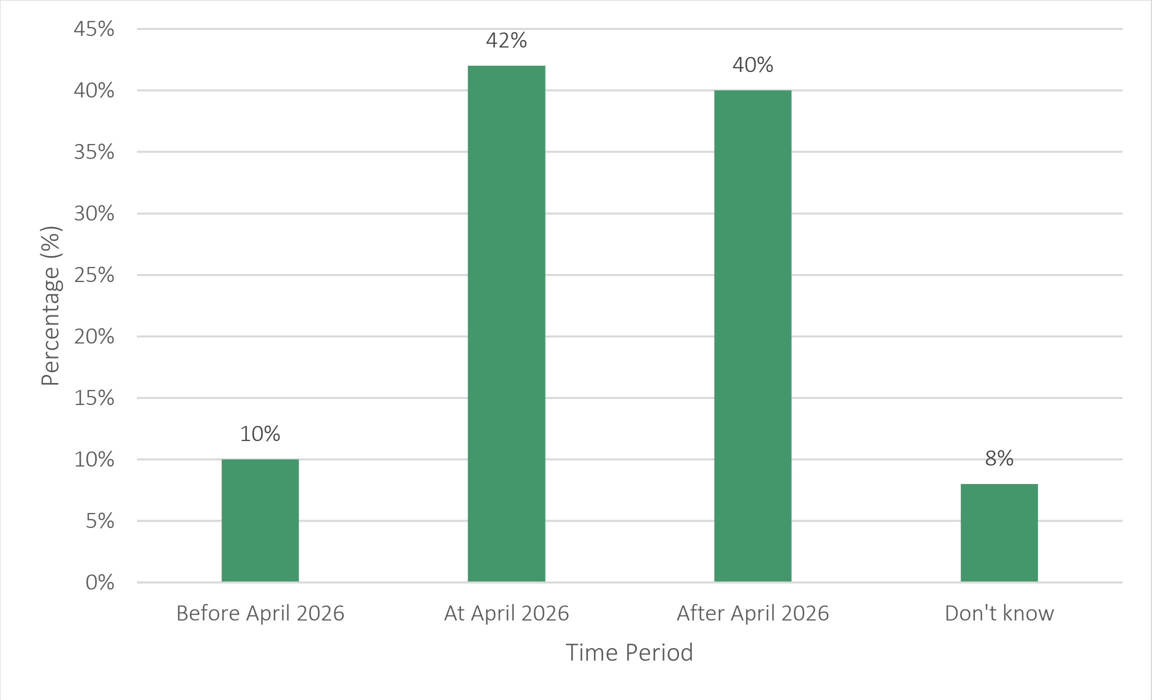
Part.1 Introduction

The race to achieve compliance with the European Union's ("EU") Artificial Intelligence ("AI") Act (the "EU AI Act") has gone beyond its starting position following its entry into force on **1st August 2024**. Many companies in both in the US and EU are potentially behind track in terms of ex-ante preparations in implementing the risk management, governance and compliance processes needed to ensure they meet the regulation's requirements and obligations, some of which apply within the two-year transition period under a staggered approach to compliance.

This report makes inferences from a study of GDPR compliance for more than 1,000 companies in the United States ("US") and EU[1] (the "Study"), that was sponsored by McDermott Will and Emery LLP, given an analogous relationship between these two pieces of European legislation. This study was deemed relevant from which to draw inferences based on its coverage of people in a variety of departments including information technology ("IT"), IT security, compliance, legal, data protection office and privacy. Moreover, 90% of respondents said that their company is subject to GDPR, while 10% were unsure, so this showcases a strong benchmark for both comparison and insight gathering.

This report indicates suggests that half of companies represented in the Study are either unlikely to meet the **2nd August 2026** deadline (or staggered deadlines during the transition period) or are unlikely to know. Moreover, this report suggests that compared to other regulations compliance with EU AI Act is anticipated to either be more or equally difficult to comply with. As shown in **Figure 1**, 40% of respondents are likely to achieve compliance after August 2026, and 8% may unaware of when they will achieve compliance.

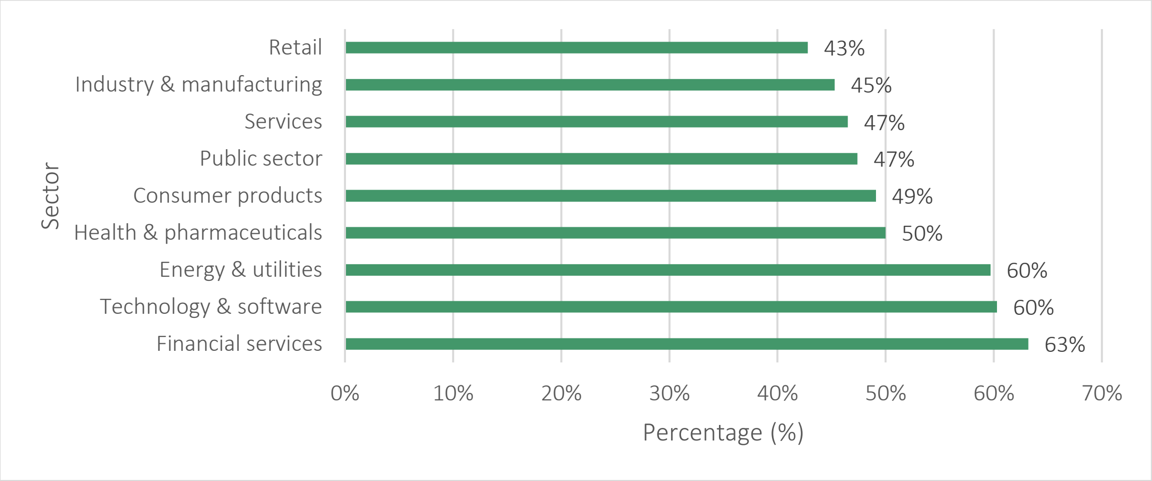
Figure 1: When are companies likely to expect to be in compliance with EU AI Act



[1] McDermott Will and Emery LLP, (2019), 'The Race to GDPR: A Study of Companies in the United States & Europe', accessible at https://s3-us-east-2.amazonaws.com/mwe.media/wp-content/uploads/2019/04/15202019/Race-to-GDPR.pdf (last accessed 18th February 2024)

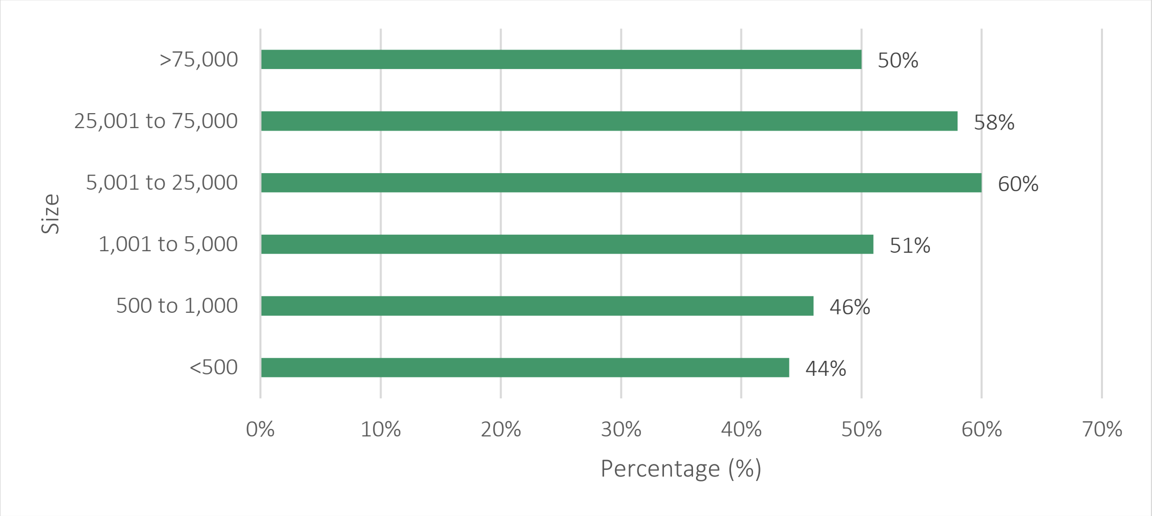
Industry sector and company size are expected to be important factors in EU AI Act readiness. As can be seen, financial service organizations are anticipated to report the highest readiness level, followed by companies in technology and software and energy and utilities. In contrast, companies in retail, industrial manufacturing and services are predicted to report the lowest readiness level.

Figure 2: Industry effects: When are companies likely to expect their organisation will be satisfied with its efforts to be in compliance with EU AI Act (at or before August 2026)



Smaller companies and very large companies are likely to see themselves as less likely to be in compliance with EU AI Act by the effective date than do mid-size companies. Figure 3 reveals an projected inverted U-shaped relationship between EU AI Act readiness and organizational size. As can be seen, smaller-sized organizations are anticipated to report the lowest readiness level, while companies with 5,000 to 25,000 employees are envisaged to report the highest readiness level. Large companies with more than 25,000 employees are expected to have a lower level of readiness than middle-sized organizations.

Figure 3: Size effects: When are companies likely to expect their organisation will be satisfied with its efforts to be in compliance with EU AI Act (at or before August 2026)



Part.2 Key Findings

In this section we provide an analysis of expected aspects of EU AI Act compliance based on the Study. Unless indicated otherwise, we present the consolidated findings for the US and EU to draw potential insights from. A special section, as noted below, will describe the most salient, expected differences between respondents in the US and EU. We have organized the report according to the following topics.

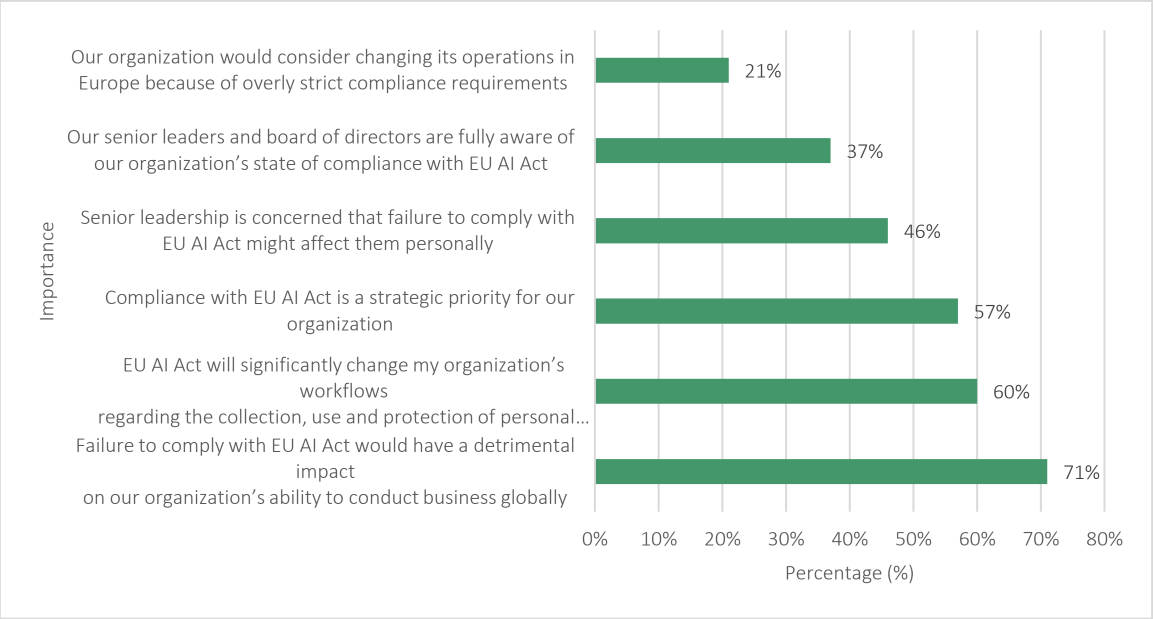
- The potential impact of EU AI Act on business practices
- The likely state of readiness to comply with AI system breach notification obligations
- The anticipated risk of non-compliance
- EU AI Act's future potential impact on companies
- The expected EU AI Act budget
- A comparison of likely US and EU respondents

The potential impact of EU AI Act on business practices

Compliance with EU AI Act is likely to be considered critical but daunting. EU AI Act is expected to compel companies to make significant changes in their global operations. As shown in Figure 4, 71% of respondents are projected to say that failure to comply with EU AI Act would have a detrimental impact on their organizations' ability to conduct business globally and 60 % of respondents are projected to say it will significantly change workflows regarding the use, marketing and deployment of AI systems. Despite their potential issues in achieving compliance, only 21 percent of respondents are expected to say their organizations would change their operations because of the overly strict compliance requirements.

It is expected that organisations believe that EU AI Act will have a significant impact on their companies' operations and 57% of respondents may say that compliance is a strategic priority. However, only 37% of respondents might say their senior leaders and board of directors are fully aware of their organizations' state of compliance with EU AI Act.

Figure 4: Likely perceptions about the importance of compliance with EU AI Act



Many companies are expected to not understand what is required to be in compliance. 47% percent of respondents may say that they do not know where to begin their path to compliance. Of the 53% of respondents who potentially understand compliance requirements, 92% are likely to say that their organizations have appointed an AI Officer and 62% of respondents are likely to report that their companies are conducting an assessment of their ability to comply with regulations.

'Understand the fundamentals AI risk management', Data Privacy & AI

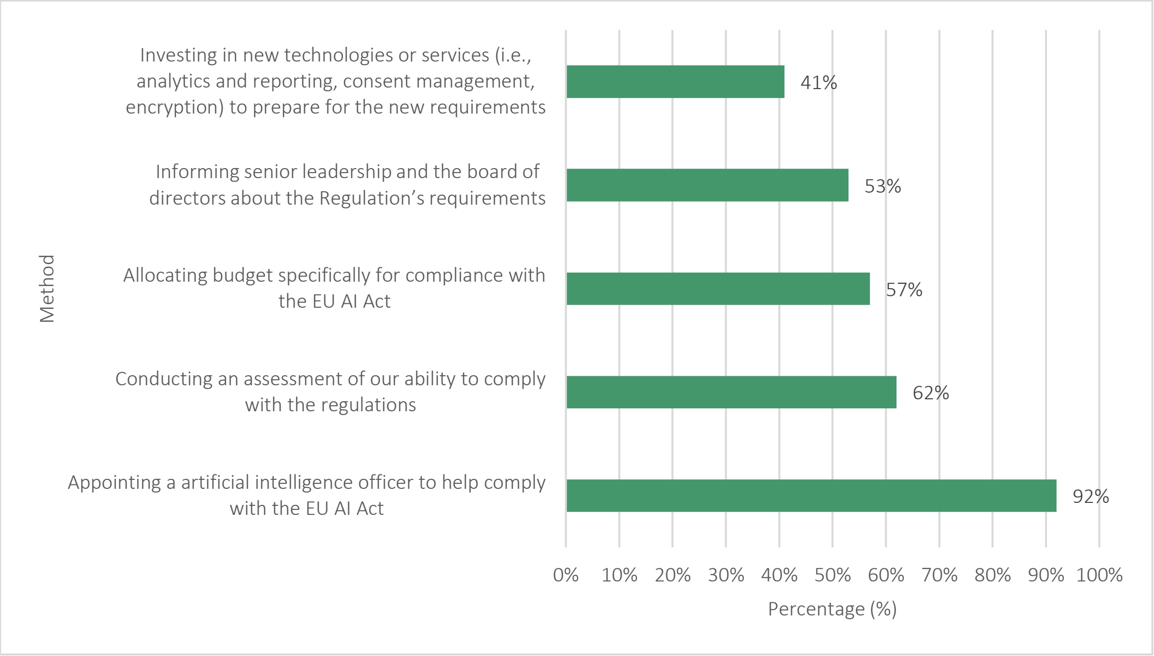
The solution to understand to get compliance with the regulations for AI, is the management approach, based on ISO/IEC42001 AIMS (AI Management System). It can guide and steer all necessary requirements, frameworks, standards and guidelines by embedding these into the business processes when developing or using AI and can be understand as steering wheel for trustworthy and ethical way with AI.

AI is the 'transformer'

"AI is the transformer to understand data as stardust in gold."

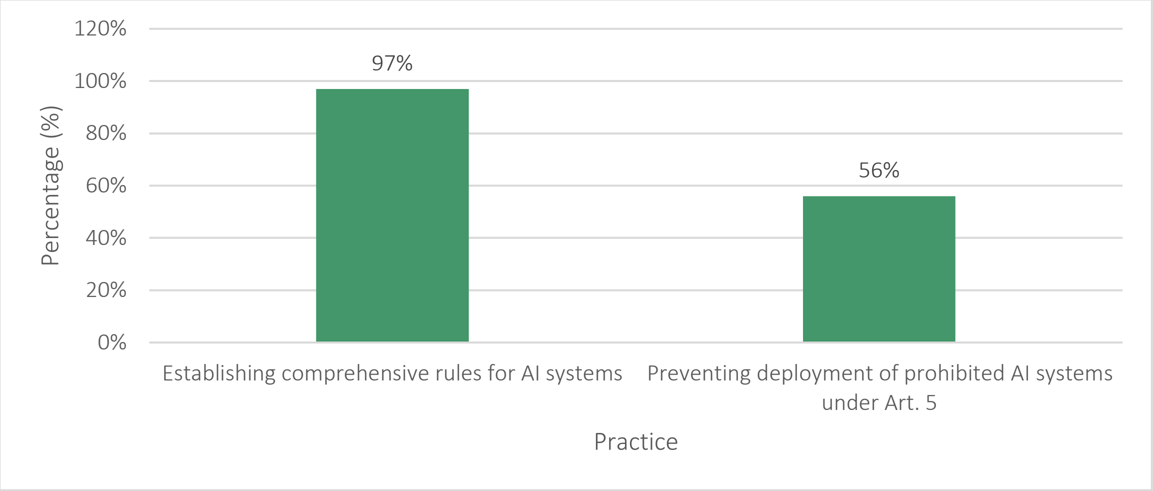
Ina Schöne*, CEO | Founder Data Privacy & AI,* Data Privacy and AI

Figure 5: How are companies likely to prepare for compliance with EU AI Act



Who potentially has to comply with EU AI Act? Companies are expected to be required to comply with EU AI Act if they offer goods or services relating to AI systems or interact with individuals involving AI systems in the EU. As shown in Figure 6, 97% of respondents are likely to say their organizations offer goods or services to EU data subjects for sale or for free and 56 percent of respondents say their companies track or observe the behaviour of data subjects in the EU by using cookies or other methods.

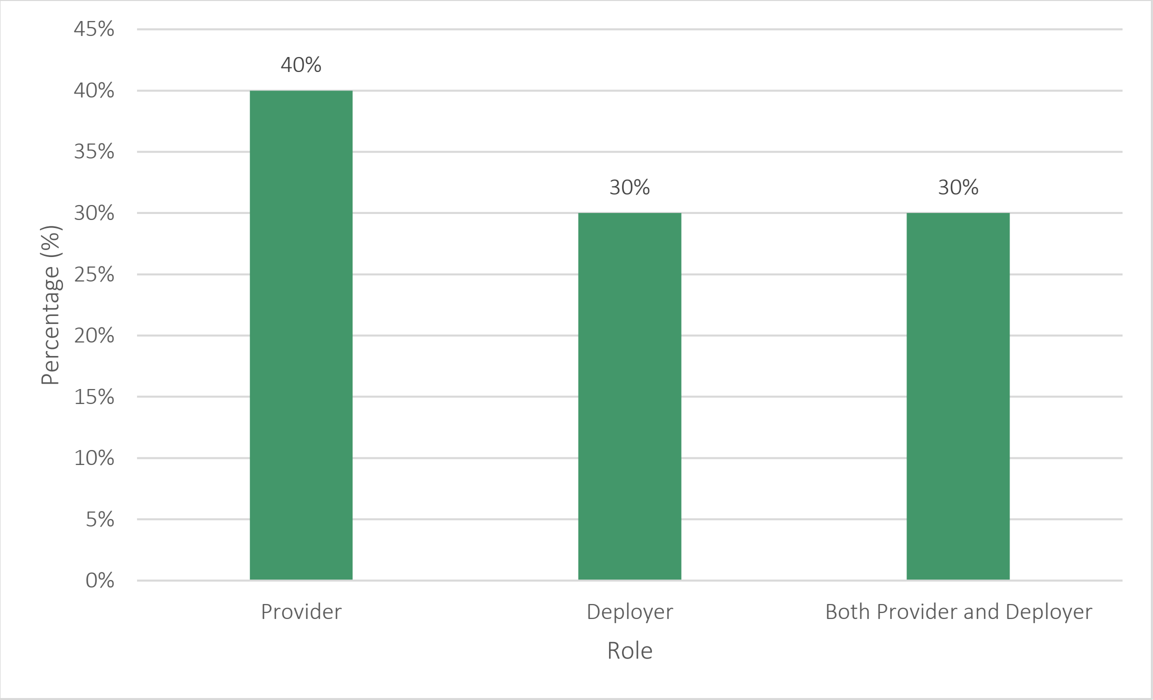
Figure 6: What are the expected practices of companies in the EU?



More companies are expected to be providers. Under EU AI Act, the provider determines the deployment, deployment and operation of AI systems to customers and third parties based on EU or Member State law. The deployer deploys AI systems on behalf of the provider.

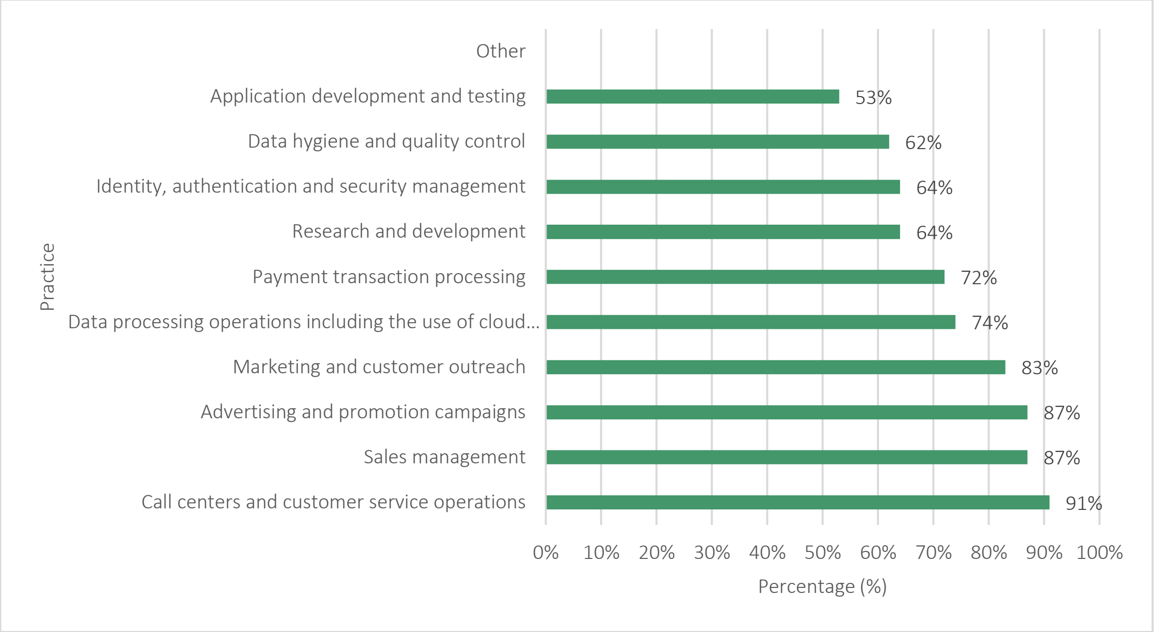
As shown in Figure 7, 40% of respondents are likely to say their companies are providers, 30% of respondents are likely say they are deployers and another 30% of respondents are expected to say their organizations are both. In their expected efforts to comply with EU AI Act, 37% of deployers are anticipated say they will change their status to provider.

Figure 7: What are organisations expected to consider themselves to be



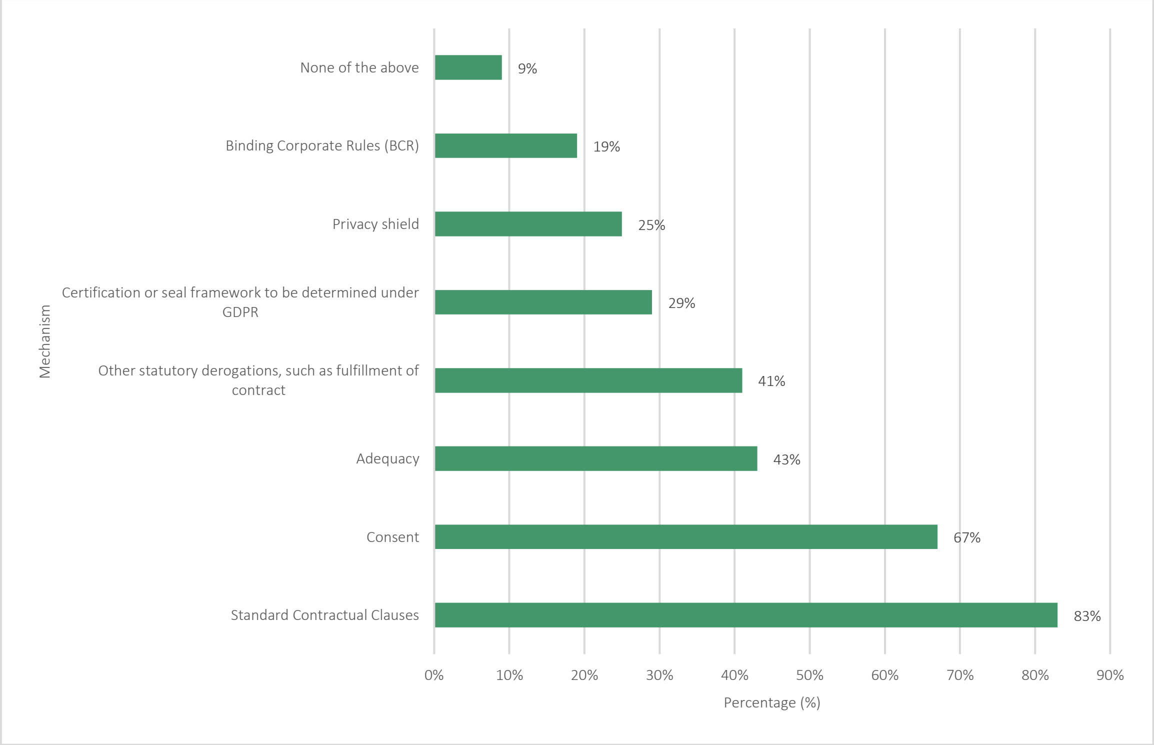
According to Figure 8, expected common practices of companies are call centres and customer service operations (91% of respondents), sales management (87% of respondents) and advertising and promotion campaigns (87% of respondents).

Figure 8: What expected practices do organisations conduct with their offices and third-parties throughout the world



Companies are expected to use a variety of mechanisms to transmit EU personal data outside of the EU. Eighty-three% of respondents are expected to say their companies use Standard Contractual Clauses ("SCCs") to transmit EU personal data outside of the EU for the purpose of testing high-risk AI systems in real-world conditions. This is followed by consent (67% of expected respondents), adequacy (43% of expected respondents) and other statutory derogations, such as fulfilment of contract (41% of expected respondents), as shown in Figure 9.

Figure 9: Expected mechanisms to transmit personal data outside of EU for the purposes of testing high-risk AI systems in real-world conditions



‘International alignment around standards for ethical and trustworthy AI’, Boevink Group

It has to be clear we need international standards to create ethical and trustworthy AI around the globe and the EU and US are aligned with this view...The challenge is the balance between innovation and regulation as the speed of AI models goes far beyond the regular growth market, where regulation and compliance always are behind but can catch up. With AI....regulation has to be a fundamental basic framework which requires continuous monitoring and update to keep up with the rapid changing landscape.

EU’s focus on fundamental rights protection offers a different approach

“The United States has always been more high risk in the investment space and boosts AI research and use cases in all technology waves there has been from the computer to the internet and now AI. European policy has focused more on protecting human rights, it is really a different angle to support the humans affected by AI.”

Michael Boevink, *Founder,* Boevink Group

US firms remain unprepared for regulatory requirements

“In our engagement with companies in some of the key U.S technology hubs (Silicon Valley, New York, Boston) we are seeing that by and large companies are not prepared for the EU AI Act. They can prepare by conducting thorough audits of their AI systems, ensuring transparency and compliance with risk management standards. Establishing governance frameworks, enhancing data privacy practices, and fostering cross-functional teams to monitor evolving regulations will ensure readiness for compliance.”

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

‘Risk classification of AI systems a ‘cornerstone’ of EU AI Act compliance’, Arkstons Advisory

To comply with the EU AI Act, U.S. firms should classify AI systems by risk level, conduct a gap analysis to address noncompliance, and establish governance frameworks with training and transparency. They must maintain detailed technical documentation and stay updated on evolving regulations, seeking legal counsel when necessary to navigate complexities.

‘Trustworthy AI for predictive AI decision-making are critical’, Q4BS GmbH

In Life Sciences, trustworthy AI for Predictive AI Decision-Making are critical to advancing patient safety. By integrating EU AI Act compliance driven by risk mitigating visualization of AI based certainty, risk, and uncertainty analysis, small and mid-sized organizations can advantage their EU marked participation through agility and innovation mindset.

Hybrid intelligence to drive more informed decision-making

"Hybrid Intelligence will transform business decision-making by enabling better choices and uncertainty deconstructed, guided by the EU AI Act compliance and advanced human-centricity will risk mitigate global business."

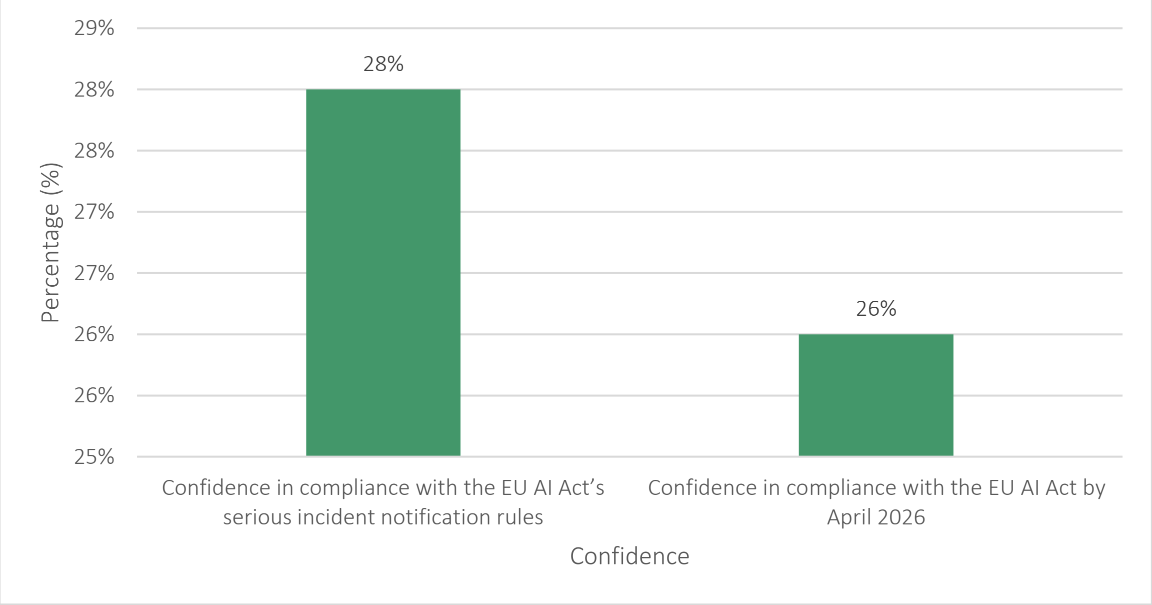
Dr. Dietmund Peters, *Managing Partner*, Q4BS GmbH

Q4BS BUSINESS SOLUTIONS

The likely state of readiness to comply with AI system breach notification obligations

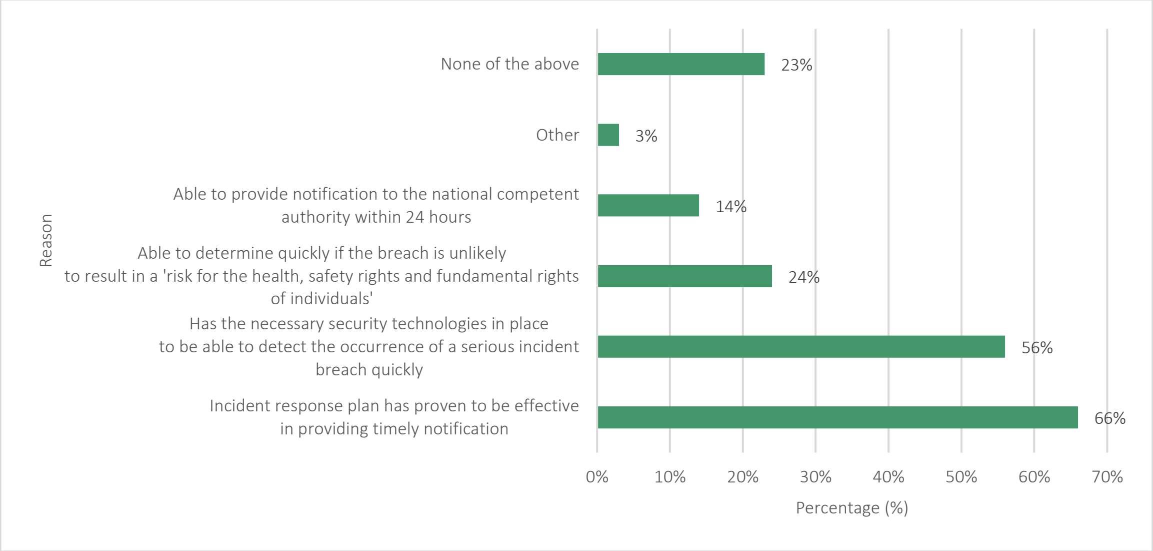
Likely confidence in meeting the deadline and serious incident breach notification rules is low. Respondents are likely to rank their confidence in complying with EU AI Act’s serious incident notification rules and with EU AI act on a scale of 1 = low confidence to 10 = high confidence. Figure 10 shows that only 26% are likely to have a high level of confidence in meeting the deadline and only 28% are anticipated to be confident in their ability to comply with the serious incident notification rules.

Figure 10: Expected confidence in compliance by August 2026 and in compliance with serious incident notification rules



Incident response plans that have proven to be effective are likely to be important to achieving compliance with the EU AI Act's serious incident notification rules. Of the 28% of respondents who are perceived to say their organizations are highly confident in their ability to comply with the EU AI Act's serious incident notification rules, it is because their organizations' incident response plans result in providing timely notification (66% of respondents) or they have the necessary security technologies in place to be able to detect the occurrence of a serious incident quickly (56% of respondents), as shown in Figure 11.

Figure 11: Anticipated reasons for organisations to be confident in compliance with EU AI Act's serious incident notification rules



A serious incident breach is anticipated to have severe financial consequences. If their companies had a serious incident, 53% of respondents are likely to believe fines would be the worst consequence followed by other significant financial harms, as shown in Figure 12.

Figure 12: Anticipated reasons for organisations to be confident in compliance with EU AI Act's serious incident notification rules

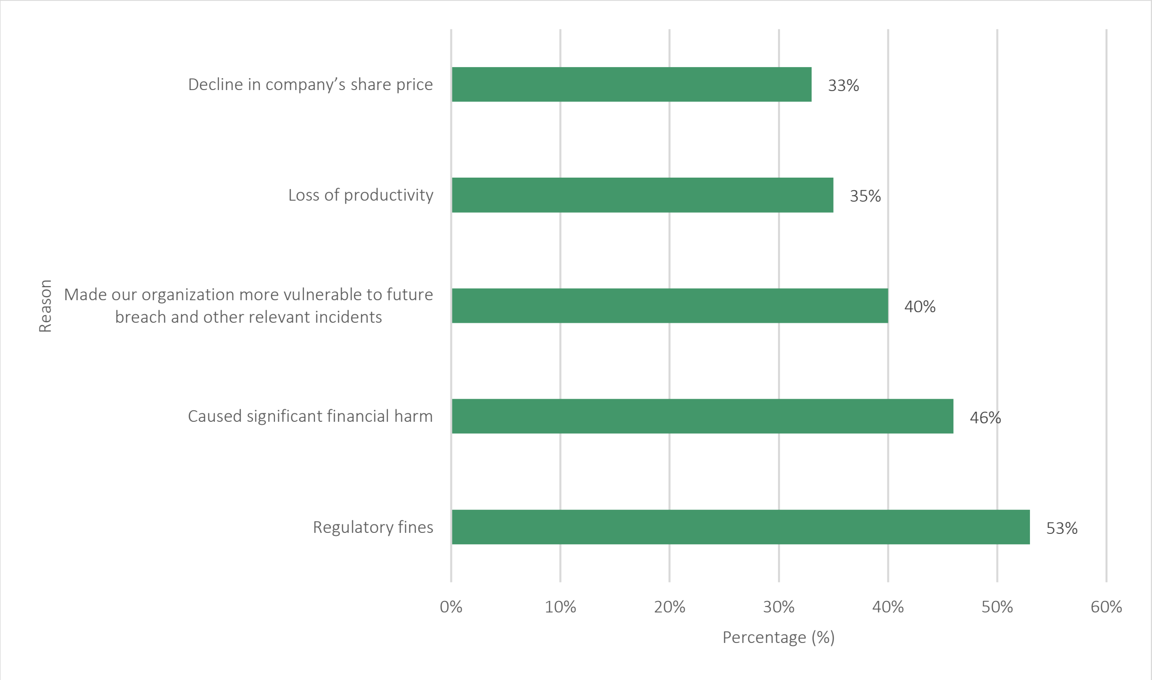
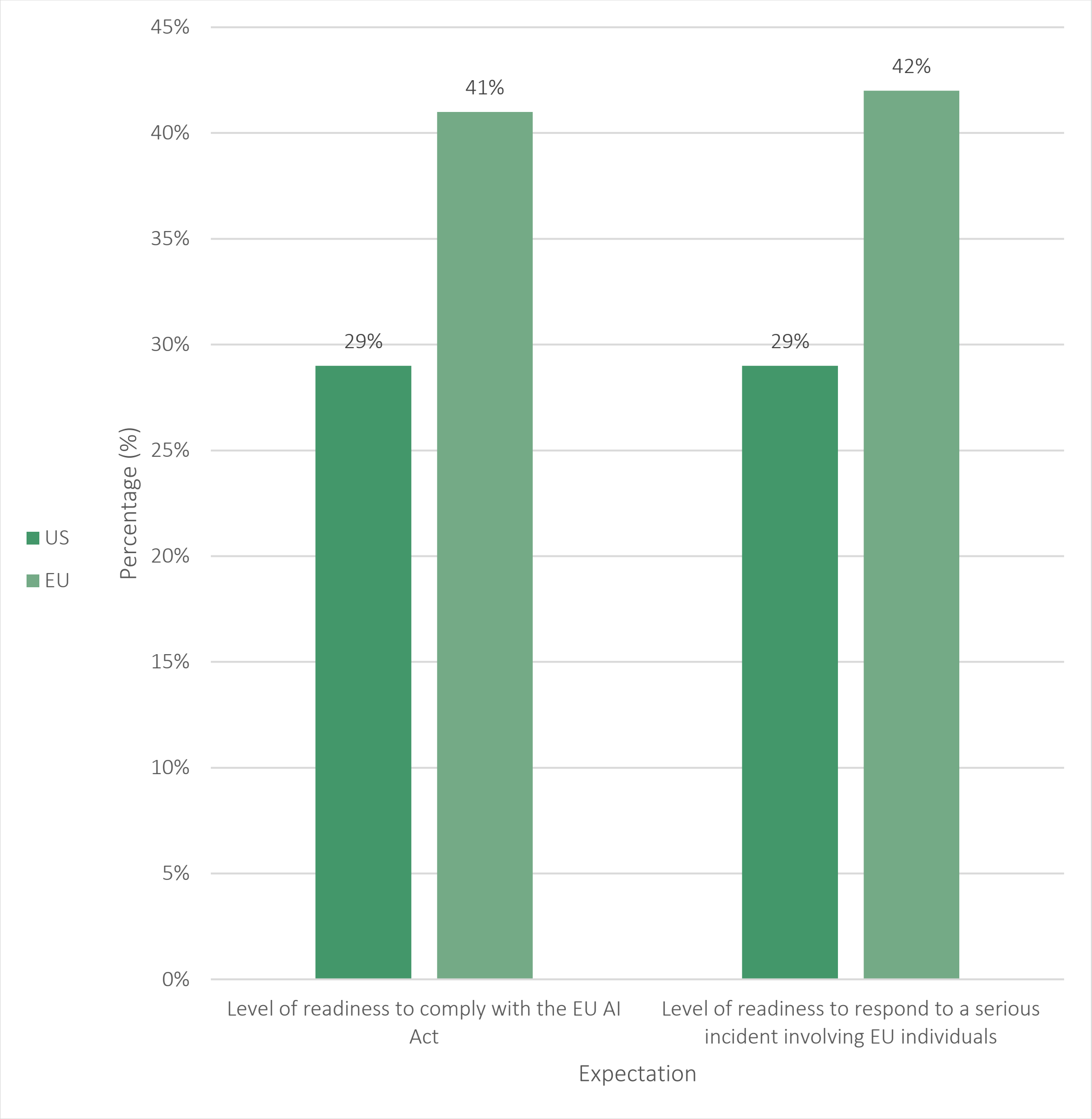


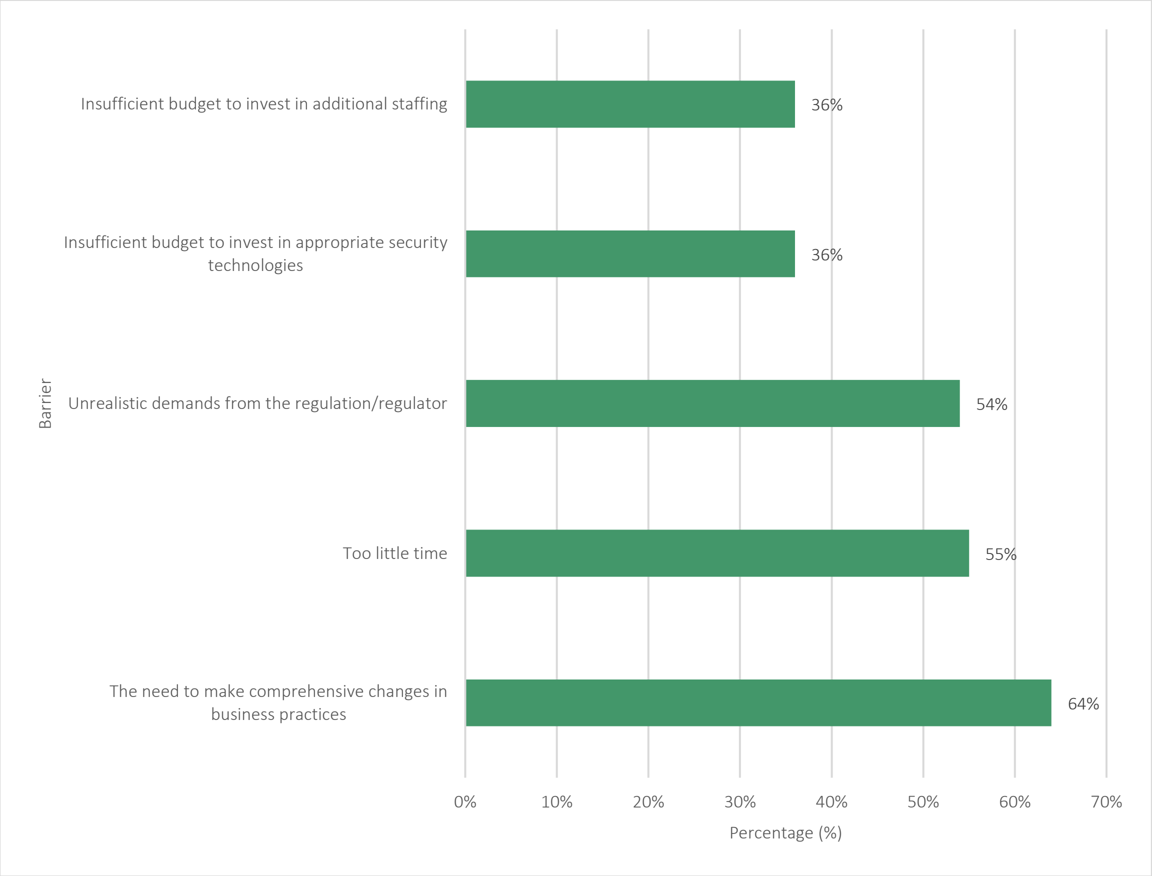
Figure 13 presents the findings of those respondents who are expected to report a high level of readiness (7+ on the scale of 1 to 10) to comply with the EU AI Act and respond to a EU serious incident. Only 29% of US respondents are expected to say they are very ready to comply with the EU AI Act and respond to a EU serious incident. While still low, more respondents in Europe are anticipated to believe they will achieve compliance with EU AI Act (41% of respondents) and, in the event it occurs, are ready to respond to a EU serious incident (42% of respondents).

Figure 13: Expectations on whether companies are ready to comply with EU AI Act and respond to an EU serious incident



The need to make comprehensive changes to business practices is expected to be the biggest barrier to compliance. As previously discussed, 60% of respondents are expected to recognize that EU AI Act will significantly change their organizations' workflows regarding the use, development, deployment and marketing of AI systems. As shown in Figure 14, 64% of respondents are anticipated say they are concerned about the need to make comprehensive changes in business practices before achieving compliance. 55% of respondents are expected to say there is too little time and 54% of respondents are envisaged to say regulators and the regulation have unrealistic demands.

Figure 14: What are the expected barriers to EU AI Act compliance



‘Proactive readjustment by enterprises to ensure regulatory alignment’, Savion Ray

As the EU AI Act reshapes the landscape of artificial intelligence, businesses need to proactively adapt their strategies to meet the new regulatory requirements. At Savion Ray — a Brussels-based public affairs agency — we believe that integrating AI and necessary compliance frameworks, let it be even a simple internal code of conduct, early ensures not only adherence but also strengthens the foundation for innovative AI solutions within the organization.

End-user mindset shift required alongside provider technical adjustments

“Compliance with the EU AI Act requires not only technical adjustments on the side of providers but a mindset shift on the side of end users. Organizations that embrace AI will lead the way in ensuring both innovation and responsible AI development.”

Bisera Savoska*, CEO,* Savion Ray

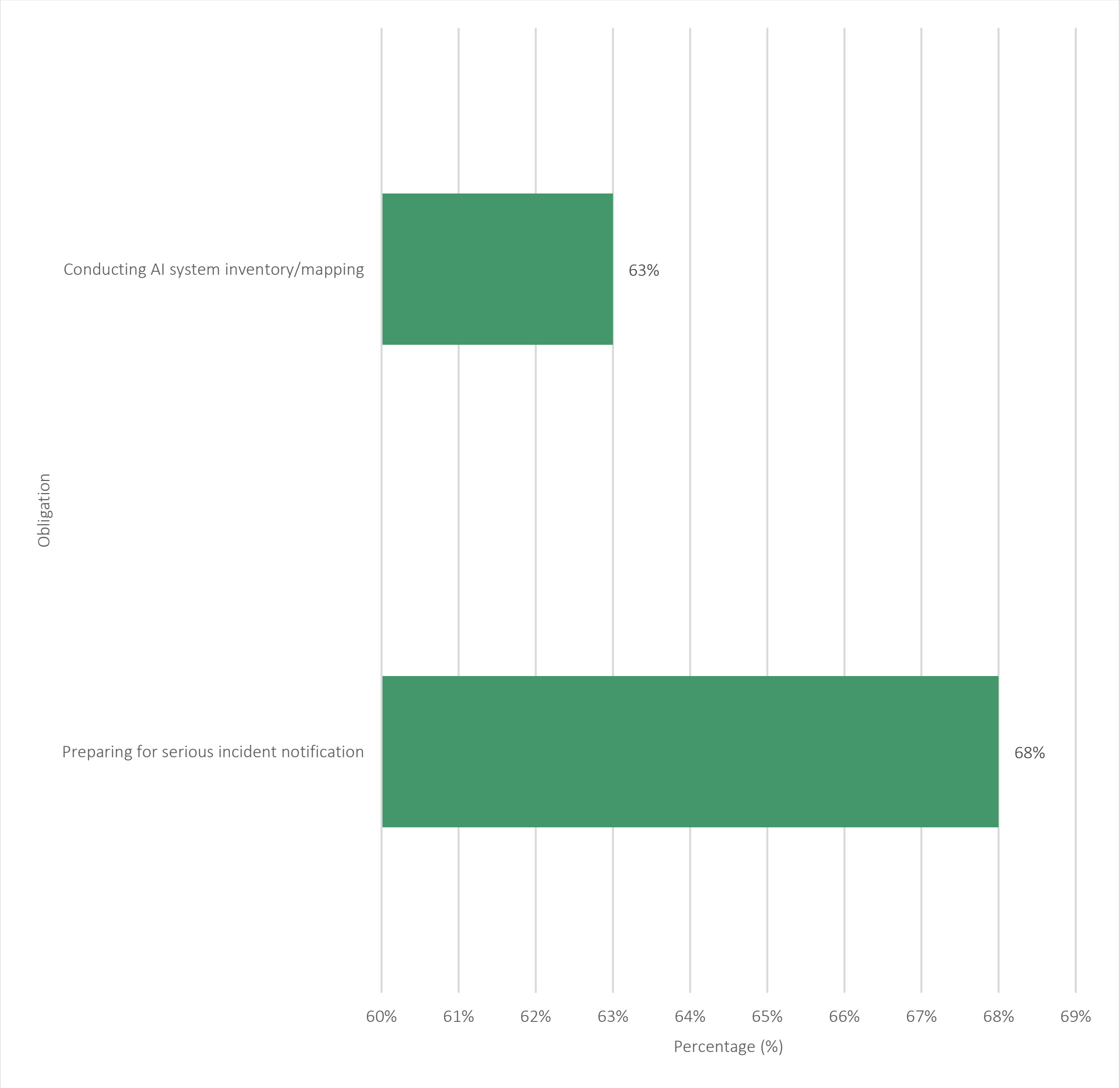
savion ray

The anticipated risk of non-compliance

Companies are expected to be concerned about the risk of noncompliance with certain EU AI Act obligations. 84% of respondents are forecasted to believe their organizations are at greater risk for potential fines and regulatory action because of their profile with regulators. They are also anticipated to believe their organizations are at a high risk if they fail to comply with specific EU AI Act obligations.

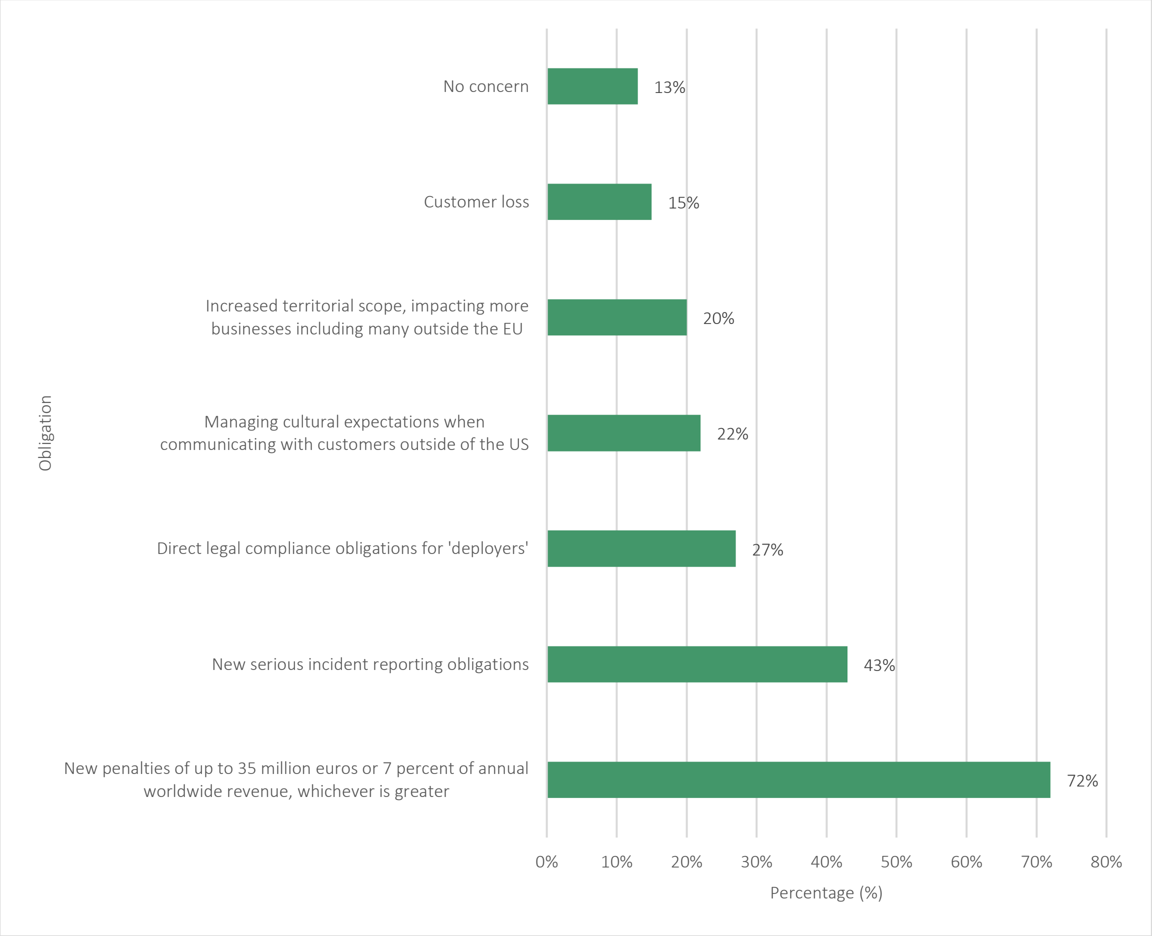
Figure 15 shows the five expected EU AI Act obligations respondents are estimated to believe pose the greatest risk for fines and regulatory action (7+ on a scale of 1 to 10) if they are not in compliance. These are: preparing for serious incident notification (68% of respondents), conducting AI system inventory/mapping (63% of respondents).

Figure 15: The expected EU AI Act obligations that pose the greatest risk of non-compliance



Companies are likely to be most concerned about the risk of incurring financial penalties. As shown in Figure 16, 72% of respondents are likely to be most worried about the financial penalties if their companies are found in non-compliance. This is expected to be followed by the new serious incident reporting obligations according to 43% of respondents.

Figure 16: The expected EU AI Act obligations that pose the greatest risk of non-compliance



‘Aligned HR strategies necessary for positive AI impact on workforce’, Hybridge Consulting

Hybridge Consulting supports HR teams in navigating AI adoption, focusing on data compliance, particularly the EU AI Act and EU Pay Transparency Act, AI-powered HR tech adoption via tools like Microsoft Viva and Copilot, and aligning HR strategies with AI’s impact on the workforce

Strategic focus on data governance necessary for AI adoption

“With the EU AI Act classifying HR systems and data as high-risk, the role of HR has never been more pivotal. HR leaders must adopt a comprehensive, purposeful strategy for data management that not only aligns with AI governance but also considers the implications of the EU Pay Transparency Act, as well as GDPR. This requires an integrated approach to data governance, ensuring compliance, ethical practices, and the safeguarding of employee rights while leveraging AI to its fullest potential.”

Fanni Kadocsa, *Managing Partner,* Hybridge Consulting

‘Firms’ biggest challenge is risk categorising AI systems’, Empasco

The most significant impact of the EU AI Act on most businesses will be the ability to risk-categorise AI systems and pinpoint high-risk AI systems for additional risk management, oversight & monitoring. While supporting innovation will be delivered from a business’ natural desire to innovate, creating a robust, transparent & explainable framework for determining how a model should be categorised will key complex

For most businesses, there will be major disruption in three areas:

1. **Roles**: Defining & implementing the roles mentioned in the EU AI Act and training staff into them
2. **Processes**: New procedures for AI Instructions, Recall / Withdrawal, and Informed consent will need to be defined in the context of how AI systems are built & operated within the business
3. **Governance**: While Data Governance is already challenging because of the separation between business, IT & Data teams, the ability to ensure Human Agency & Oversight during development & into production of AI systems will require specific skills and positions to be created

To conclude, it is unlikely that organisations have even a conceptual understanding of the above, let alone the ability to execute detailed changes & strategies to ensure compliance.

empasco CONSULTING

‘EU touchpoint drives compliance obligation’, Karushkov

The EU AI Act shall apply to providers or deployers of AI systems or models irrespective of whether these are located or established within the EU and irrespective of the sector[2]. The core issue of exterritorial reach of the AI Act is whether the AI system is used in or have effect on the EU.

> **Cross-functional application to affect all businesses**
>
> *“The global reach of the EU AI Act shall result in compliance measures at corporate, design, contractual and business level for all stakeholders targeting EU market.”*
>
> **Mitko Karushkov,** *Founder,* Karushkov Legal Solutions

K! KARUSHKOV LEGAL SOLUTIONS

EU AI Act’s future potential impact on companies

EU AI Act is likely to require ongoing investments in technologies and governance practices. As shown in Figure 17, 72% of respondents are likely to say their organizations will have to make investments in new technologies or services (i.e., analytics and reporting, consent management, encryption) to maintain compliance. Other ongoing practices will include assessments of the ability to comply with regulations (65% of respondents), evaluation of relationships with third-party vendors (58% of respondents) and the creation of a new accountability framework (52% of respondents).

[2] Save to defense, national security, and some research endeavors

‘Driving significant investment in technology and governance’, Sumsub

While the EU AI Act will drive significant investment in technology and governance, businesses should be prepared for evolving legal landscapes globally. The vetoed landmark, yet controversial, California's SB1047 bill highlights the growing complexity of global AI regulation. This bill, aimed at facilitating compliance with the EU AI Act for U.S. companies, signals that more stringent regulations may soon follow in the U.S.

Stringent regulations likely to follow in the US

"As AI technology continues to advance, new laws are likely to emerge, further complicating compliance for organizations. This uncertainty adds pressure, especially as key areas like generative AI-led scams and fraud—which caused $12.3 billion in damage to businesses in 2023—remain insufficiently addressed. Staying ahead of future regulatory requirements will require swift adaptation and well-equipped compliance teams."

Natalia Fritzen, *AI Policy and Compliance Specialist,* Sumsub

sumsub

‘Redefining global AI Governance standards’, 5Tech Lab

The EU AI Act’s extraterritorial impact mirrors the GDPR, and its requirements are poised to redefine global AI governance standards. US-based organizations cannot afford to take a passive approach. Those that move early to establish robust compliance frameworks, particularly in areas like risk management, transparency, and AI ethics, will secure a competitive edge in the European market.

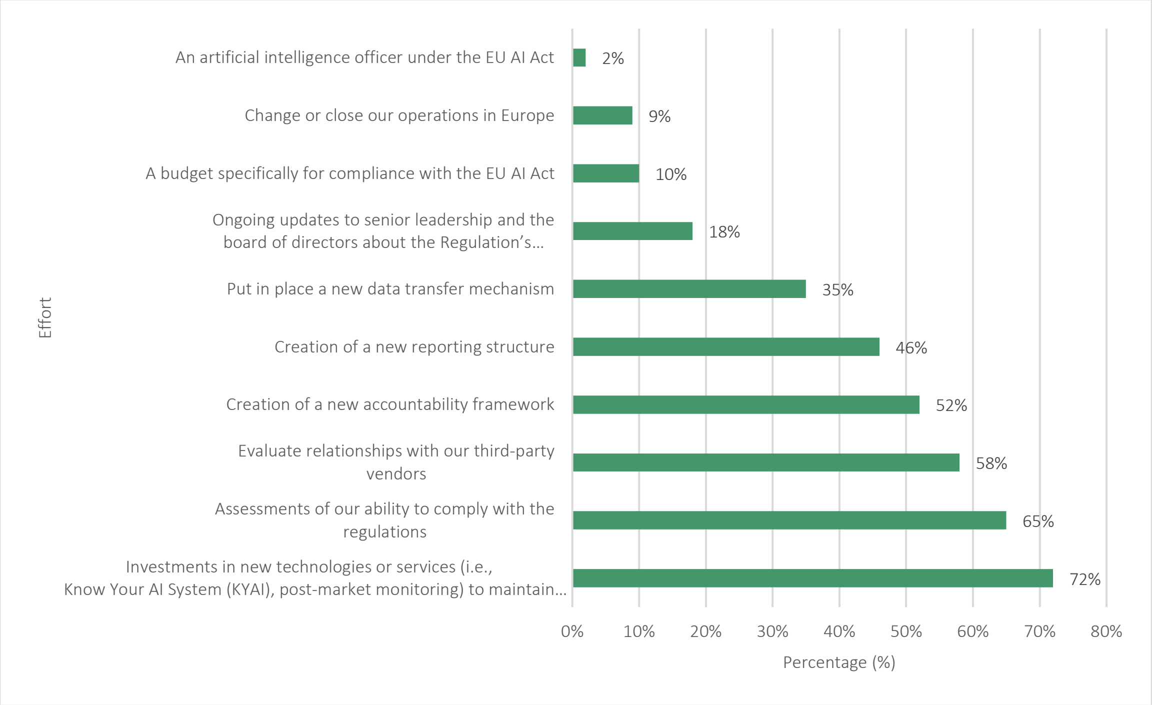
Offering a blueprint for trustworthy AI development

“The key lies in recognizing that the Act doesn’t just impose legal obligations but also offers a blueprint for trustworthy AI deployment. By embracing this opportunity, businesses can align technological innovation with regulatory foresight.”

Arjun Prasad, *General Partner,* 5Tech Lab

5TECHLAB

Figure 17: Anticipated areas that require significant efforts after August 2024



More fundamental rights impact assessments ("FRIAs") will be conducted after August 2024. As shown in Figure 18, prior to the August 2024 deadline 50% of respondents are expected to say that they conducted only one (if any) FRIA and 29% of respondents are expected to say they didn't conduct any. Following the August 2024 deadline, 57% of respondents are anticipated to say they will conduct at least 3 (44%) and more than 5 (13%).

'Non-compliance detrimental to competitive advantage', Cyber Security Unity

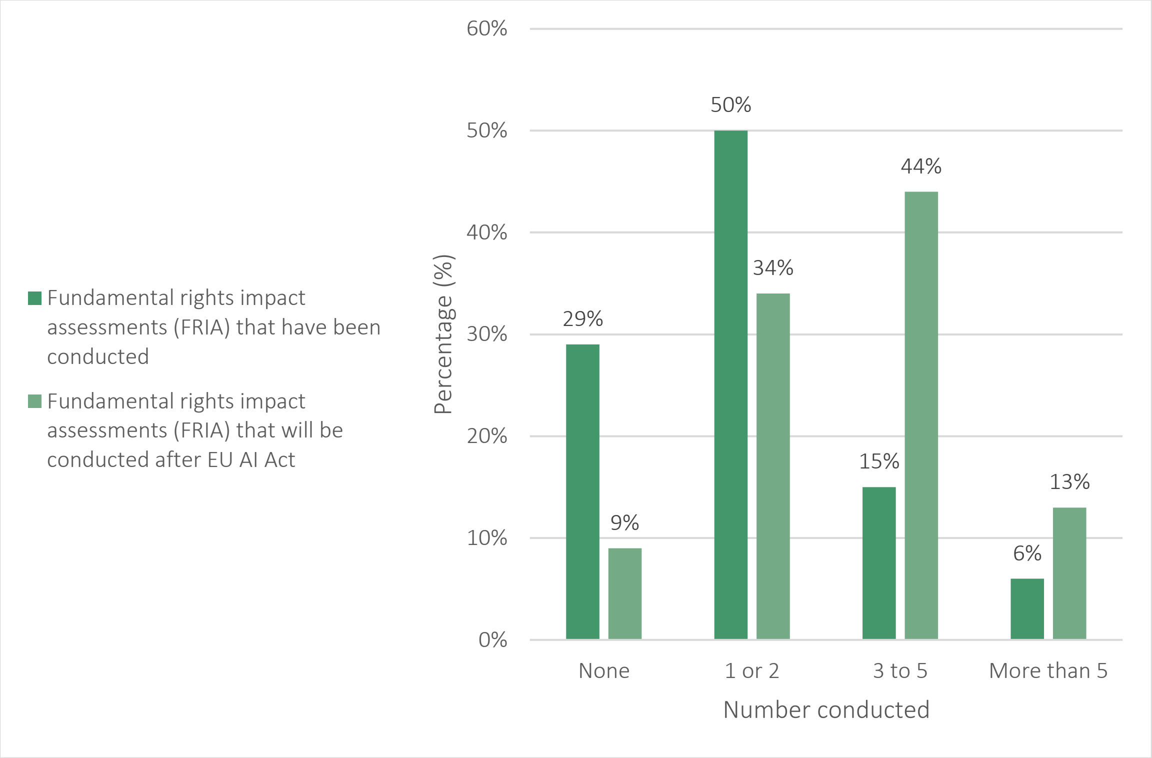
While the race to achieve compliance has been considered critical but daunting up to now, AI is here to stay, whether we like it or not. AI is considered to be a bit of a wild west when it comes to compliance with the new EU AI Act, but it is an act that is sorely needed, and I hope it will spur organisations on to make changes to cope with it in their global operations. These survey results show that failure to comply with the EU AI Act will have a detrimental impact on the ability to conduct business globally. It is something that no organisation can afford to ignore today if they wish to remain competitive in their marketplaces.

Race for compliance matches AI's anticipated long-term impact-

"While the race to achieve compliance has been considered critical but daunting up to now, AI is here to stay, whether we like it or not."

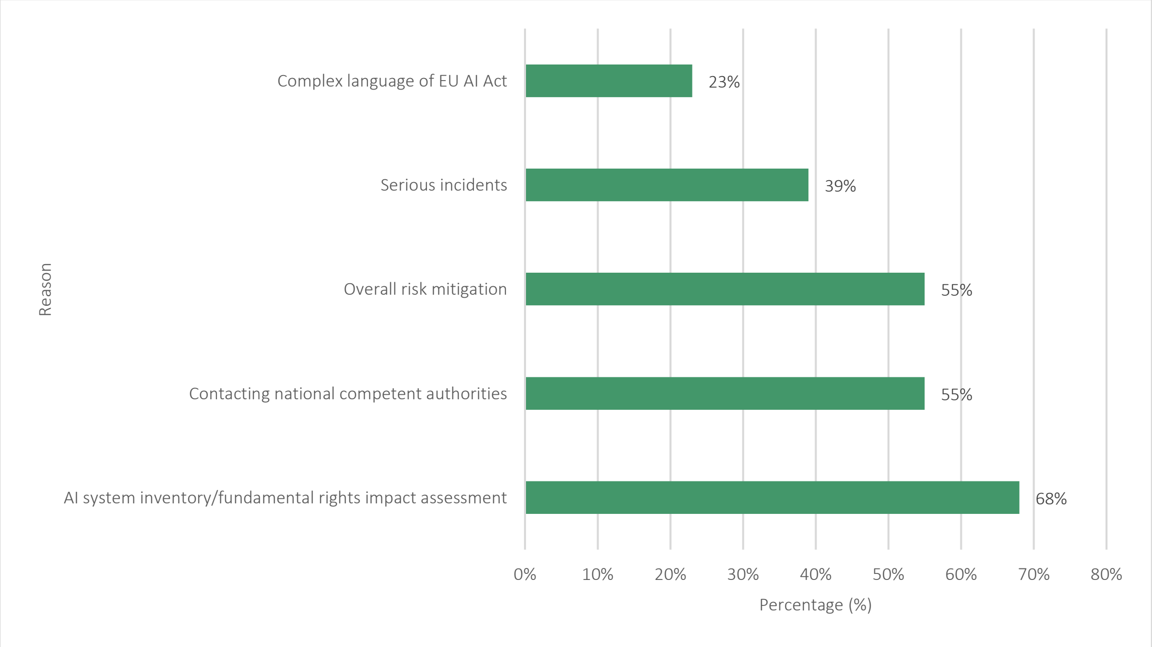
Lisa Venture MBE, *Founder,* Cyber Security Unity

Figure 18: Anticipated areas that require significant efforts after August 2024



Many companies are expected to hire outside counsel to assist with EU AI Act compliance. Forty-six% of respondents are likely to hire outside counsel to support their EU AI Act compliance activities. As shown in Figure 18, the primary reason is likely to be assisting with the increasing number of FRIAs that will be conducted (68% of respondents). 55% of respondents are expected to say outside counsel will establish relationships with national competent authorities and another 55% of respondents say it will be to assist with overall risk mitigation.

Figure 19: Expected reasons for organisations to hire outside counsel to assist with EU AI Act compliance

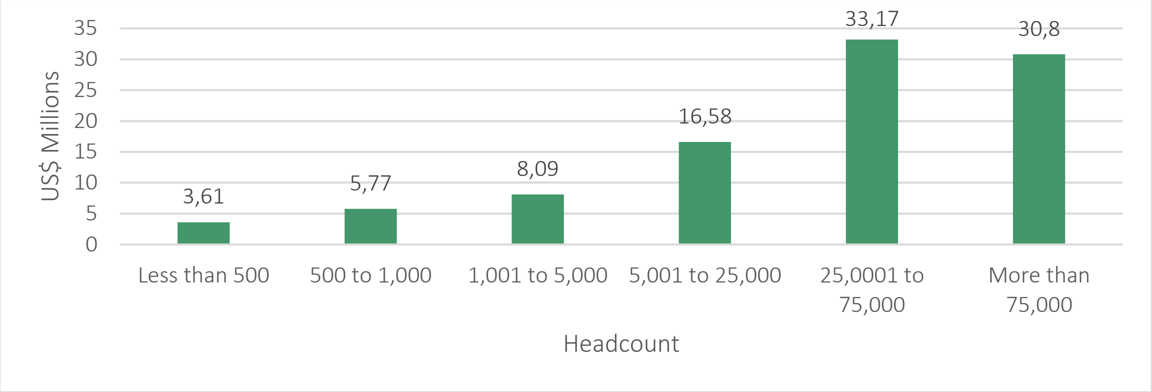


The expected EU AI Act budget

The average expected annual budget for compliance with EU AI Act is US$13 million. 33% of respondents are expected to believe the budget for EU AI Act will be renewed annually and 22% of respondents are anticipated to say the budget will continue indefinitely.

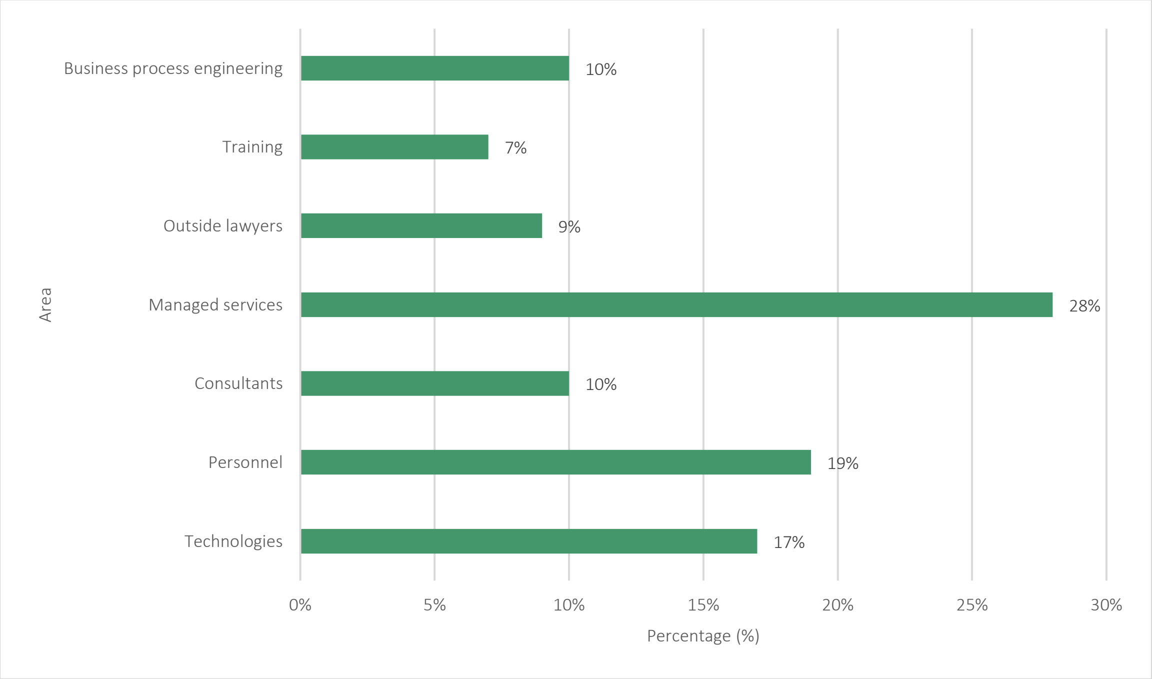
As shown in Figure 20, the annual budget for compliance is likely to vary by organizational headcount. The budget for organizations with a headcount of more than 25,000 is posited to be significantly higher than those organizations with a smaller headcount. However, because of economies of scale the average per capita budget for organizations with a headcount over 5,000 is forecasted to be $351.59.

Figure 20: Expected annual budget for compliance with EU AI Act by organisational headcount



Most of the budget is anticipated to be allocated to managed services. As shown in Figure 21, companies are expected to spend most of their budget on managed services followed by personnel and technologies.

Figure 21: Seven expected areas for EU AI Act budget



‘Looming compliance deadlines pressuring US firms action plans’, Loeb Smith Attorneys

US organizations face difficulties in aligning with the EU AI Act, primarily due to the need for stricter regulatory standards and risk management, enhanced corporate governance and ethical AI practices. With compliance deadlines looming, companies must prioritize their resources to meet the Act's requirements and avoid potential penalties.

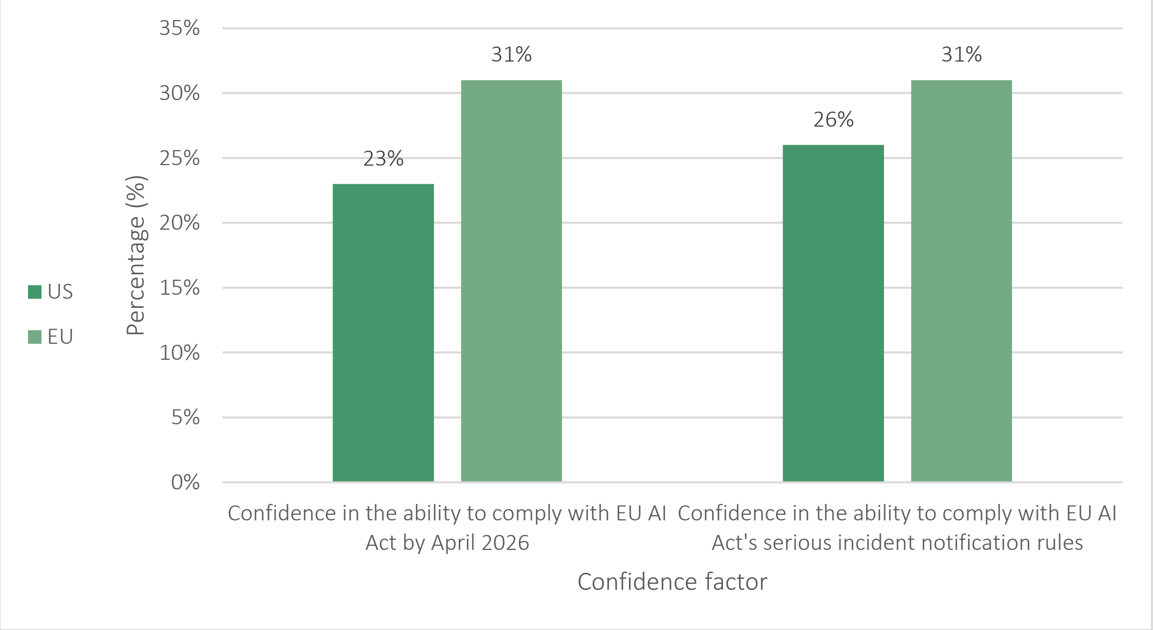
> **The time act for US companies is now**
>
> *“US organizations face significant challenges aligning with the EU AI Act, especially in adapting to regulatory standards, ensuring transparency and ethical AI practices. The time to act is now.”*
>
> **Robert Farrell,** *Partner,* Loeb Smith Attorneys

A comparison of likely US and EU respondents

In this section we present the other most likely differences between respondents in the US and EU regarding EU AI Act compliance.

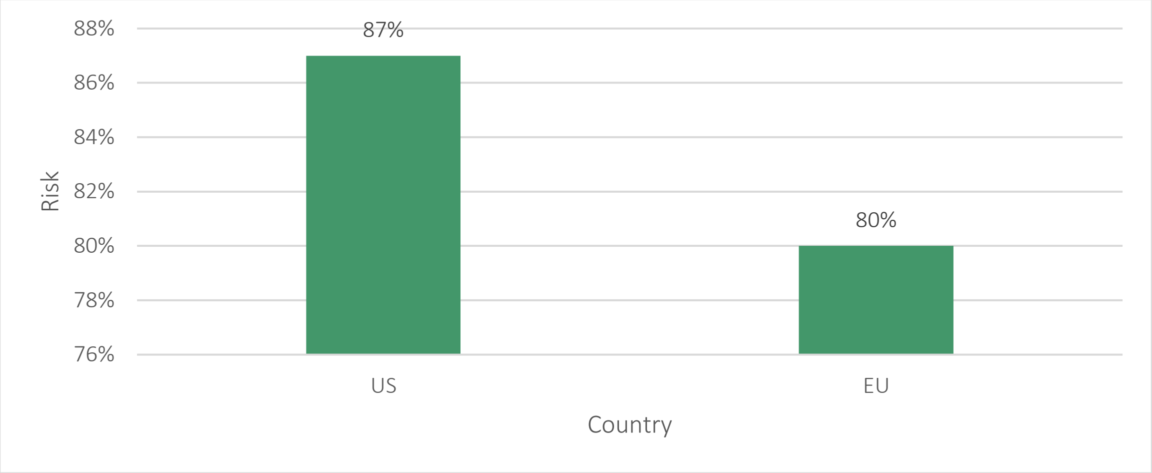
Confidence in meeting the EU AI Act deadline and serious incident notification rules is expected to be low in both the US and EU. As shown in Figure 22, only 23% of US respondents and 31% of EU respondents are expected to say they are confident they will meet the EU AI Act deadline by August 2026. Similarly, confidence is expected to be low in meeting the serious incident notification rules, according to 26% of US respondents and 31% of EU respondents, respectively.

Figure 22: Expected confidence in complying with EU AI Act



Both respondents in the US and EU are expected to worry that their profile with regulators increases the risk of fines and penalties. While higher in the US (87% of respondents), EU respondents are estimated to also worry they may be a target for regulatory action, as shown in Figure 23.

Figure 23: The likely risk of possible EU regulatory action because of the organisation's profile with regulators



US respondents are expected to be more likely to say that EU AI Act is more difficult to comply with than other regulatory requirements, such as prudential, data protection and consumer protection. According to Figure 24, 50% of US respondents versus 35% of EU respondents are expected to say EU AI Act exceeds other requirements in its level of difficulty.

California's SB 1047 signals a 'Regulatory Shift', Silvia A. Meyer

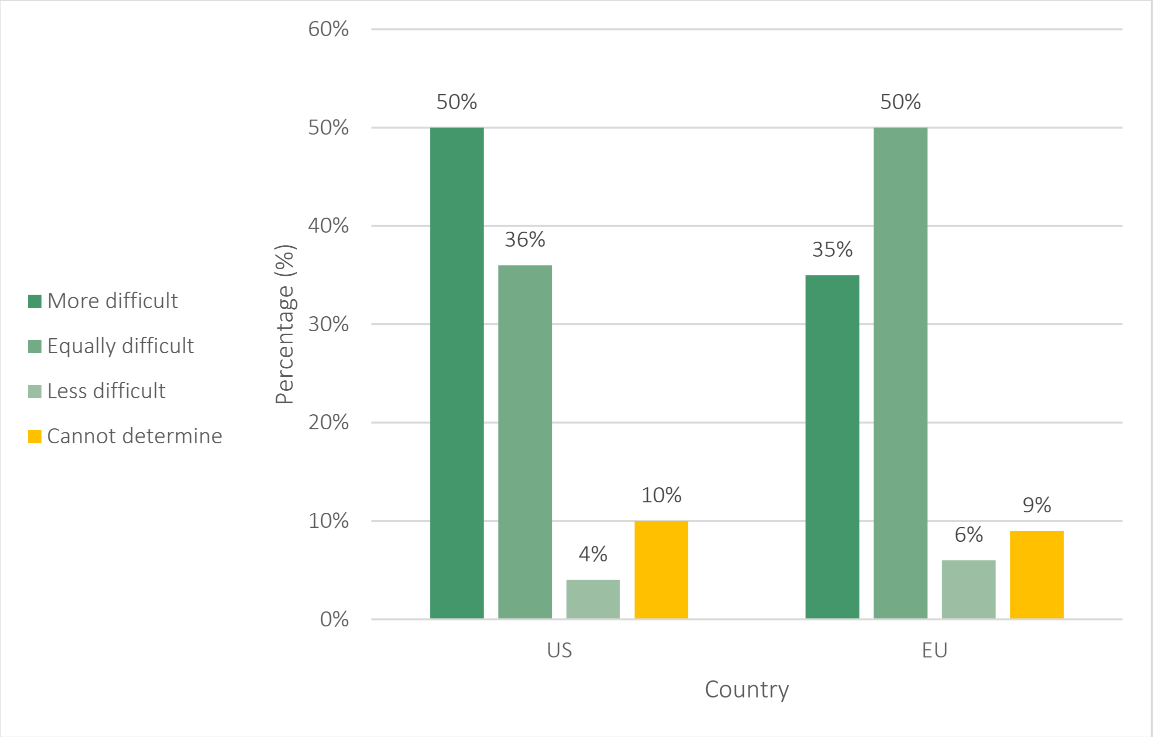
SB 1047 could mirror the EU's top-down regulatory approach, requiring tech companies to follow strict protocols and face audits. This marks a notable shift from Silicon Valley's self-regulatory model, as discussed with Stanford, Berkeley, and European startups.

US Shifting towards more regulatory oversight

"SB 1047 in California signals a shift towards more state oversight, echoing the EU's top-down regulatory approach, challenging Silicon Valley's tradition of self-regulation and company-driven compliance."

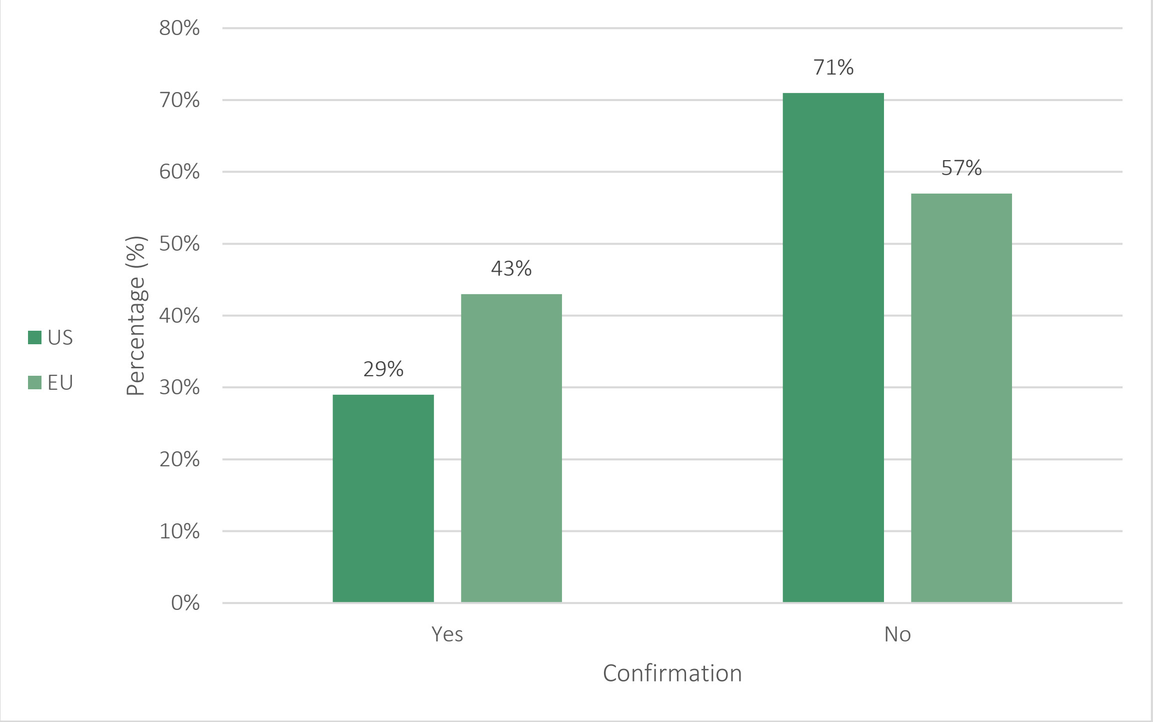
Silvia A. Meyer, *Executive Advisor for International Business,* Silvia Meyer & Company

Figure 24: Relative to other regulatory regimes, how difficult is the EU AI Act expected to be to implement?



More EU organizations are expected to conduct a AI system inventory or audit of their EU-focused AI systems. As shown in Figure 31, only 29 percent of US respondents versus 43 percent of EU respondents say they have conducted a data inventory of their EU personal information to understand how it is used and where it is located.

Figure 25: Likelihood of an organisation having conducted an AI system inventory or audit of its AI systems to understand where they are deployed and who uses them



Part.3 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
Amsterdam – London - Singapore

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, CEO/CFO, s.musch@ai-and-partners.com

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

Authors

Sean Donald John Musch, CEO/CFO

Michael Charles Borrelli, Director

Acknowledgements

Corporate Partners

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

Individual Partners

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

Binesh Balan, Binesh Balan is 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'.

Bisera Savoska, Bisera Savoska is a tech-driven CEO and creative strategist who founded Savion Ray over 10 years ago. Based in Brussels, she works with internationally renowned brands and organizations, helping them develop effective digital communications and producing high-quality video campaigns and impactful social experiments. Prior to Savion Ray, she worked as a Head of Communications for a woman empowerment organization and headed digital teams for Brussels-based consultancies.

*Doug Hohulin, Business Associate (AI & Partners), Strategy and Technology Advisor on Responsible AI (Ethics, Governance, Policy, Regulation, Compliance, Safety), AI in Healthcare, and AI Operations and Workflows.

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.

Fanni Kadocsa, Fanni Kadocsa, Managing Partner at Hybridge Consulting, specializes in guiding HR teams through AI adoption. With a focus on data governance, tech adoption (Microsoft Viva & Copilot), and strategic workforce planning, Fanni assists HR teams in aligning HR strategies with regulatory frameworks like the EU AI Act.

Ina Schöne, Ina Schöne is Founder of Data Privacy and AI and follows the a practice oriented approach to understand the requirements of AI-Act and the measures to implement this requirements and guides the companies on the path to get the corresponding certifications.

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.

Mitko Karushkov, Mitko Karushkov has been providing legal, regulatory, compliance, transactional and business solutions to international companies for more than 20 years now. Focused on enterprise companies and their strategic (or daily) operations, Mitko has solved matters related to the digital, tech or electronic assets of such businesses. Active and involved also in bridging between traditional and technology markets, including to the application of the EU DSA, DMA, AI and other regulations. Media, Telecoms, IPRs, Corporate, M&As are also part of the service portfolio of Mitko.

Robert Farrell, Robert Farrell is a Partner at international law firm, Loeb Smith Attorneys. Robert originally qualified in England and Wales where he practiced for twelve years as a Banking & Finance lawyer, representing senior business leaders and financial institutions. Since relocating to the Cayman Islands, Robert has developed a practice in advising a variety of crypto / web3.0 businesses on their regulatory obligations. This includes writing legal opinions on the project's white paper to determine its regulatory status, advising on structuring and submitting applications for regulatory registrations and licences. Robert has also spoken at conferences, including most recently at the 'Deep Dive into the Metaverse and Web3: Second Global Law Symposium', hosted by the New York State Bar Association.

Silvia A. Meyer, Silvia A. Meyer is an Executive Advisor for International Business and a consultant specializing in global strategy implementation. She creates effective go-to-market (GTM) approaches for emerging markets, develops leaders who drive transformative change, and guides companies in aligning and synchronizing dispersed teams. Silvia's expertise centers on driving growth, expanding markets, and leading innovation to achieve impactful outcomes.

*Doug has made significant contributions to AI & Partners over the course of its lifetime, particularly in regards to responsible AI practices, ethics, regulations, governance and policy primarily for the healthcare sector.

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.