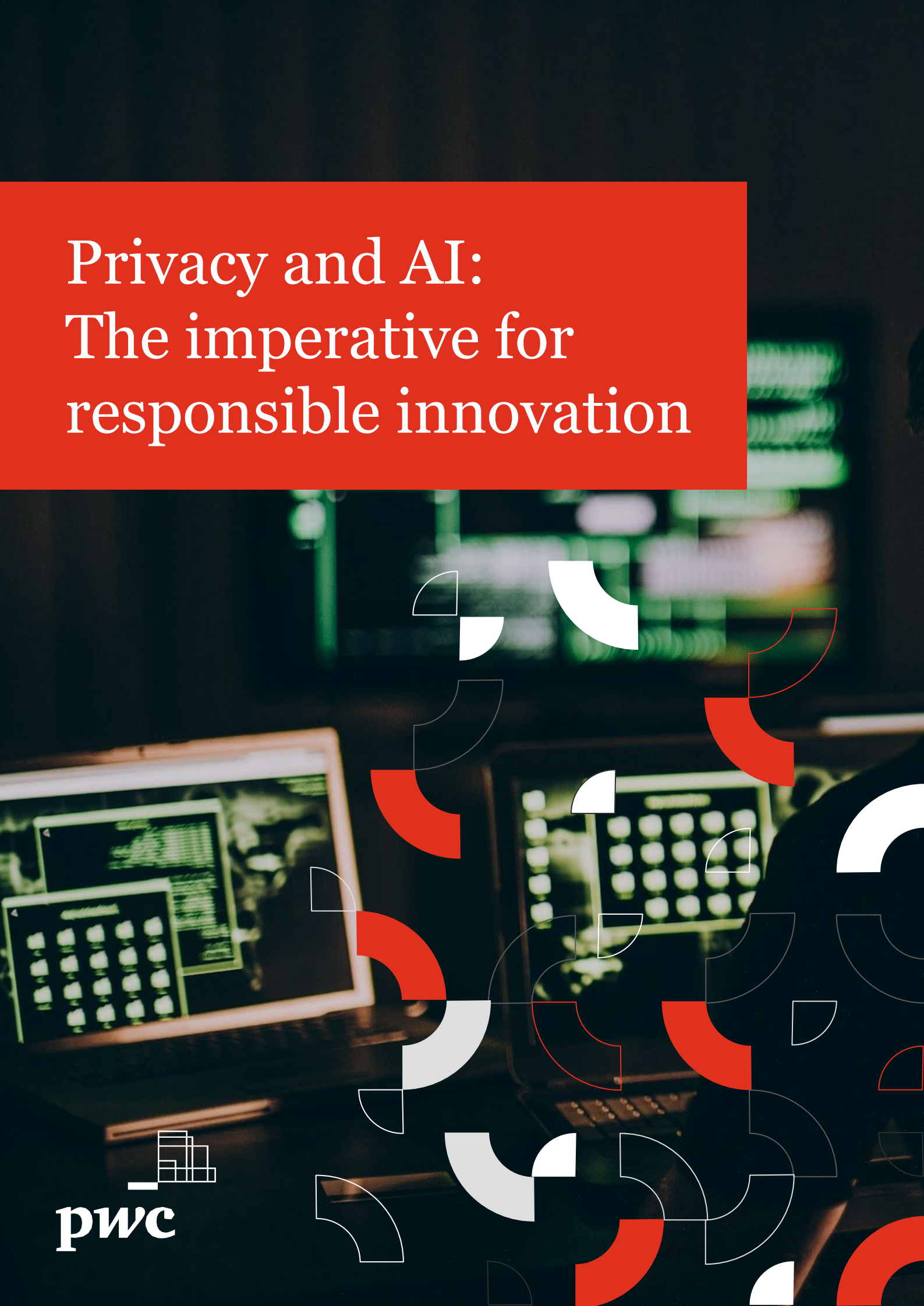
Privacy and AI: The imperative for responsible innovation



pwc

Artificial Intelligence is a source of immense excitement and apprehension globally and in the Middle East. Forward-thinking regional governments are looking to leverage the potential of Artificial Intelligence (AI) as a catalyst for digital transformation across various sectors and are subsequently investing heavily in the development and implementation of AI and its subsets, such as Generative AI (GenAI) and Large Language Models (LLMs). These advanced technologies can support regional governments' ambitious national objectives to positively impact their citizens and societies.

However, as the AI landscape evolves, privacy concerns have arisen. Our **2024 Global Digital Trust Survey** shows that mega breaches are increasing in number, scale and cost. The percentage of those reporting costs of $1 million or more for their worst breach in the past three years rose to 36% globally and 29 % for Middle East respondents.

AI has swiftly penetrated numerous aspects of our lives, including healthcare, finance, and transportation. By harnessing vast amounts of data, AI algorithms can uncover insights, drive decision-making processes, and optimise system performance. However, this data collection, processing, and analysis, present inherent risks to personal privacy. Business leaders should, therefore, champion responsible practices by harnessing the immense potential of AI to minimise the risk of privacy breaches.

While AI doesn't guarantee immunity from data breaches and needs to be included in a multi-layered approach as part of the wider technical and organisational controls, AI and machine learning-based fraud prevention capabilities can be used to ensure secure transactions, detect unusual patterns of activity that indicate a possible data breach, identify vulnerabilities in computer systems, keep systems up-to-date with the latest security patches, and limit access to sensitive data, among others. In this paper we have summarised such risks into broader remediation categories, which organisations can use as a starting point for risk mitigation.

Privacy by design

At the foundation of responsible AI lies the concept of ‘Privacy by design’. Organisations must prioritise privacy considerations throughout the development life cycle for any AI system. This includes incorporating privacy-enhancing technologies, anonymising data, and adopting robust security measures. By adhering to privacy-centric principles, business leaders can foster an industry culture that values privacy, ensuring AI systems maintain individuals' trust.

Immediate next step:

Evaluate the emerging technologies, systems, applications, and products you use to ensure that privacy-by-design considerations are incorporated, assessed, and documented throughout the entire technology deployment process.Additionally, ensure privacy by designing policies and procedures considering AI implications and the corresponding risk mitigation strategies.

Transparency

Clear communication and consent mechanisms should empower individuals to make informed decisions about their data. Organisations should advocate for standardised privacy policies and provide individuals with understandable and accessible information regarding how their data is collected, processed, and used. By making privacy measures explicit and understandable, trust in AI systems can be cultivated, promoting a society that embraces these technologies.

Immediate next step:

Revise your privacy-related policies using clear language, to ensure transparency regarding the use of AI and its implications. Implement understandable communication and consent methods that empower individuals to make well- informed decisions about their data. Advocating for standardised privacy policies promotes trust and nurtures a society that is receptive to AI technologies while also respecting privacy concerns.

Fairness

AI systems can have an underlying bias when an algorithm produces systemically prejudiced results due to erroneous assumptions in the machine learning process. This can lead to discrimination and can cause harm to the data subjects. Moreover, AI systems have the potential for automated decision-making based on the underlying data aggregation and related patterns, which can have privacy implications for data subjects.

Immediate next step:

Organisations can eradicate bias by ensuring that human scepticism is used across the AI systems deployment by conducting regular testing and audits of the underlying systems, monitoring the performance, and testing feedback to ensure no bias results in the data subject harm. Additionally, ensure that your data protection office reviews automated decision-making and the underlying personal data used to make the AI system more transparent and interpretable to the data subjects. The outcomes of such automated decisions should be explainable and easy to interpret to demonstrate how AI has arrived at a particular conclusion.

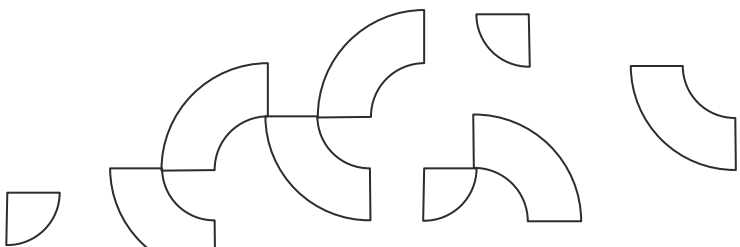
Data management

All AI systems rely on its underlying data and corresponding algorithms; as such, the quality of data is paramount to ensure the reliability of the outcome.

The underlying data that feeds into the AI model can breach the data minimisation and retention principle, which can directly impact data subjects and violate their rights. As such, companies must ensure that machine learning models are sanitised using technologies like pseudonymisation or data aggregation.

Immediate next step:

Ensure your Records of Processing Activities (RoPA) is up-to-date along with an overall data governance plan to ensure data is managed effectively throughout its life cycle. Companies can count on more robust due diligence on such underlying data by performing regular testing by a qualified human.



Information security

The Confidentiality, Integrity, and Availability (CIA) of underlying data in AI systems can be jeopardised in the event of a breach or malicious attack. Such incidents can lead to a complete system failure, resulting in the loss of personal data and impacting data subjects. Careful consideration should be given to organisational and technical controls such as data masking, encryption, password management, access controls, and robust network security to avoid potential breaches.

Immediate next step:

Review your organisational and technical controls that cover the CIA triad and ensure the highest level of security consideration is given to applications that use AI and the underlying data is protected accordingly.

Risk management and compliance

All companies should follow a risk-based approach to AI systems and conduct data privacy impact assessments to assess the level of risk involved in deploying such technologies. This should involve clear documentation of risk tolerance and mitigation strategies and appropriate sign-offs from the relevant stakeholders within the organisation.

Additionally, business leaders must actively promote the adoption of ethical frameworks and regulatory standards to govern the use of AI. Establishing enforceable regulations will help safeguard individuals' privacy rights, curbing potential abuses of AI technologies. Business leaders can play a pivotal role in facilitating the development of these regulations, ensuring they strike a delicate balance between fostering innovation and protecting privacy.

Immediate next step:

Update your enterprise risk management strategy and framework to clearly factor in privacy and AI-related risks and document ongoing risks and their remediation in a formal risk register.

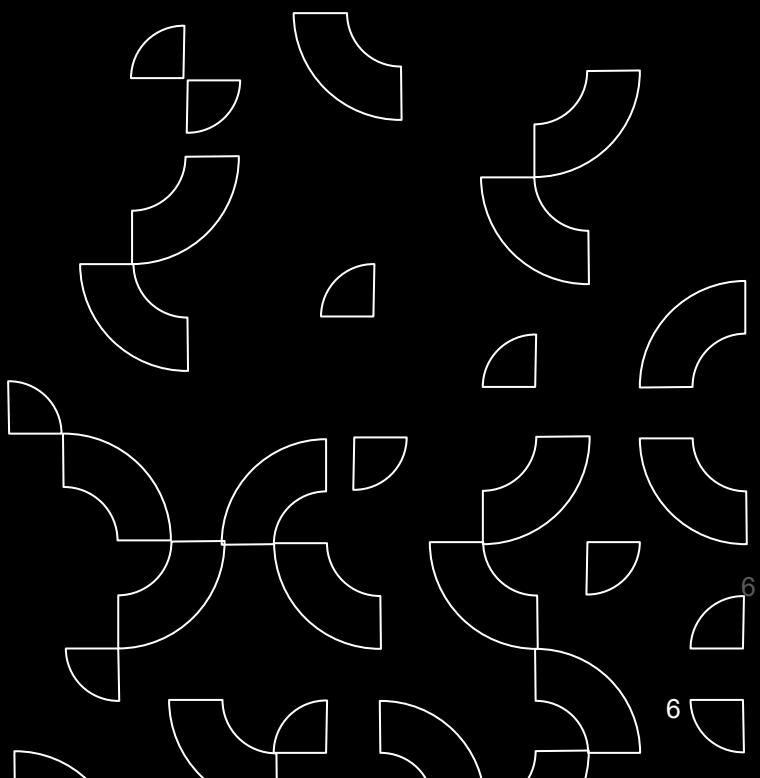
Ongoing assurance

AI systems and their underlying technology are constantly evolving. With most companies using such emerging technologies, it's prudent to ensure periodic reviews to future-proof the technology and that any ongoing concerns are regularly addressed and mitigated. With the evolving landscape of AI and other emerging technologies, there is uncertainty about the perceived risk and the future. As such, most countries are working on creating a framework that regulates AI and its corresponding risks. Companies must be on top of such regulations and how they impact their business landscape.

When procuring AI tools and systems, organisations should conduct due diligence on the vendor's credibility, including the company values towards trust and privacy and assess the underlying technology behind such AI systems to ensure the reliability and trustworthiness of the vendor. This should be further backed up with a robust data protection contract that includes relevant clauses per the data protection regulation(s) applicable to the organisation

Immediate next step:

Update your audit and training plans to factor evolving privacy and AI considerations to educate your employees and other relevant stakeholders.



Conclusion

Privacy and AI are closely intertwined, drawing the attention of business leaders to navigate the complex challenges presented by this emerging technology. Privacy must remain at the forefront of AI development, with business leaders promoting responsible practices to preserve individuals' rights. By adopting a privacy-centric mindset, prioritising transparency, establishing regulatory frameworks, and engaging in collaborative discussions, business leaders can pave the way for a future where privacy and AI coexist harmoniously. Only through such efforts can AI's full potential be unlocked, while safeguarding the fundamental rights of an individual's privacy.

At PwC, we have crafted a data privacy handbook to help simplify the requirements and make it easier for organisations to kick-start their data privacy compliance journey. This toolkit contains useful information and resources to help organisations assess their business processes against data privacy best practices and take the necessary steps to improve them.

Contact us

Phil Mennie
Data Privacy Leader | Technology Consulting Partner
phil.mennie@pwc.com

Richard Chudzynski
Data Protection and Privacy Legal Leader | Technology Consulting Director
richard.chudzynski@pwc.com

Aben Pagar
Data Protection and Governance | Technology Consulting Senior Manager
aben.pagar@pwc.com