

Navigating responsible AI: a privacy professional's guide

APRIL 2023



The integral role of privacy teams in responsible AI adoption

Artificial Intelligence (AI) continues to transform the business landscape. But what makes this technology different from its predecessors? Unlike other technological advances seen with mobile and data warehouses, AI brings unique differences that make it harder to predict and more challenging to manage the risks. Which is why privacy professionals, alongside peers in security, ethics, and ESG, all play a critical role in ensuring responsible AI adoption within organizations.

Cross-collaboration is critical for organizations that aspire to build holistic trust programs, and with AI taking up an increasing amount of column space, privacy professionals can help board members, CEOs, and organizational peers have a clear view of how the existing work of Privacy by Design best practices and frameworks can be a launchpad for Responsible AI governance and a central driver for trust.

Let's explore how you can effectively support your organization in understanding the responsible considerations, risks, and potential benefits of incorporating AI into your business strategy while maintaining a strong focus on data privacy.

Guiding your board and CEO through responsible AI

1. Educate on responsible AI and data privacy

Privacy professionals must help board members and CEOs understand AI literacy. Board members and CEOs won't need an in-depth technical understanding of AI. However, it's beneficial that they understand the ethical implications and data privacy risks associated with its development.

To do this:

- Provide plain and clear explanations of AI concepts, technologies, and their potential impact on privacy.
- Share examples of AI successes and failures, highlighting the impact and possible sources of bias.
- Understand the unique risks AI introduces and the upcoming regulatory and compliance requirements.
- Demonstrate the value of collaboration between privacy and data ethics teams.

2. Develop and advocate for a comprehensive AI strategy and responsible AI framework

Privacy professionals should collaborate with board members and CEOs in developing an AI strategy that supports the creation of a strong responsible AI framework, integrating privacy considerations into the organization. To ensure responsible and ethical AI development and deployment, consider the following steps:

- Implement strong data privacy regulations by creating and enforcing robust data privacy policies that protect personal data and uphold individuals' rights to control how their data is used.
- Ensure the organization's AI initiatives are agile and adhere to relevant laws and standards, including the proposed European Union Artificial Intelligence Act (The AI Act) and the NIST AI Risk Management Framework.
- Develop transparent and accountable AI systems by working with Machine Learning Operations (MLOps) teams to ensure model training and decision-making is transparent and auditable.
- Address AI privacy and ethical risks by proactively identifying and mitigating potential concerns, such as misuse of personal data, biased algorithms, and

discrimination based on ethical principles.

- Collaborate with internal and external stakeholders to develop guidelines that address reducing bias, mitigating risks, and ensuring transparency, fairness, privacy, and accountability in AI systems.
- Determine criteria for classifying different levels of risk posed by AI activities, such as higher risk for facial recognition compared to spam filters.



Lifecycle and Key Dimensions of an AI System. Modified from OECD (2022) [OECD Framework for the Classification of AI systems — OECD Digital Economy Papers](#).

3. Foster a privacy-focused culture around AI decision-making

As a privacy professional, you can help create a culture of privacy awareness around AI decision-making within the organization. To do this:

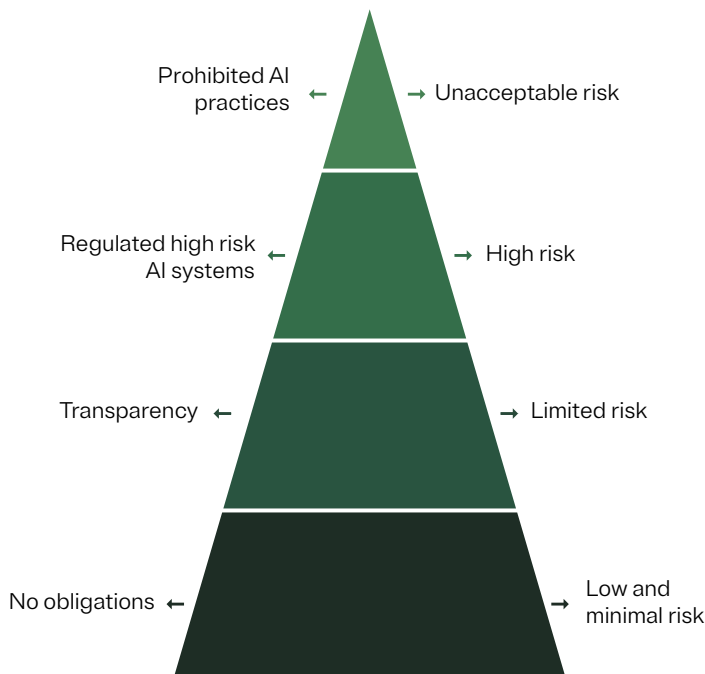
- Encourage open communication and dialogue between privacy, data / MLOps, product, security, and ethics teams.
- Provide regular updates on AI initiatives, highlighting changes to ethical and privacy concerns, changes in AI technologies and areas for improvement.
- Offer guidance and support to other departments in implementing privacy-focused AI solutions and addressing potential privacy risks associated with AI projects.

4. Navigate the risks of AI

While AI offers immense potential for businesses, it also presents risks that vary in magnitude, allowing organizations to tailor their response according to the level of risk associated with each AI project. Proactively address the risks associated with AI by:

- Assessing the level of risk associated with each AI project, factoring in data sensitivity and potential impact on individuals including bias and discrimination.
- Collaborating with IT and security teams to implement stringent data protection policies and procedures based on risk assessments.
- Monitoring and ensuring compliance with relevant data protection laws and regulations and advising on best practices for data anonymization and pseudonymization in AI applications.
- Establishing clear and transparent consent mechanisms for data collection and usage in AI systems and providing opt-out mechanisms.

- Informing the organization about evolving AI regulations and standards, incorporating AI risk management into the organization's risk management frameworks, and focusing on unique aspects of AI-related risks, such as the potential for autonomous decision-making and its implications on liability and regulatory compliance.



Data source: [European Commission](#)

Empowering privacy teams to support responsible AI

As privacy professionals, you play a pivotal role in guiding your boards and CEOs toward responsible AI adoption. By educating them on AI ethics, data privacy, developing a comprehensive AI strategy with privacy in mind, advocating for a robust AI ethics framework, and fostering a privacy-focused culture around AI decision-making, you can ensure that your organization effectively harnesses the power of AI while safeguarding user privacy and maintaining trust. Embrace your role as a privacy champion and help steer your organization toward a future of ethical, responsible, and privacy-conscious AI innovation.

As society redefines risk and opportunity, OneTrust empowers tomorrow's leaders to succeed through trust and impact with the Trust Intelligence Platform. To learn more about how the market-defining Trust Intelligence Platform from OneTrust can help you build trust into the center of your operations and culture, visit onetrust.com.



onetrust

As society redefines risk and opportunity, OneTrust empowers tomorrow's leaders to succeed through trust and impact with the Trust Intelligence Platform. The market-defining Trust Intelligence Platform from OneTrust connects privacy, GRC, ethics, and ESG teams, data, and processes, so all companies can collaborate seamlessly and put trust at the center of their operations and culture by unlocking their value and potential to thrive by doing what's good for people and the planet.

Copyright © 2023 OneTrust LLC. Proprietary & Confidential.