

Privacy and AI Governance Report

Privacy, Quo Vadis — will you lead the way?

EXECUTIVE SUMMARY

Table of Contents

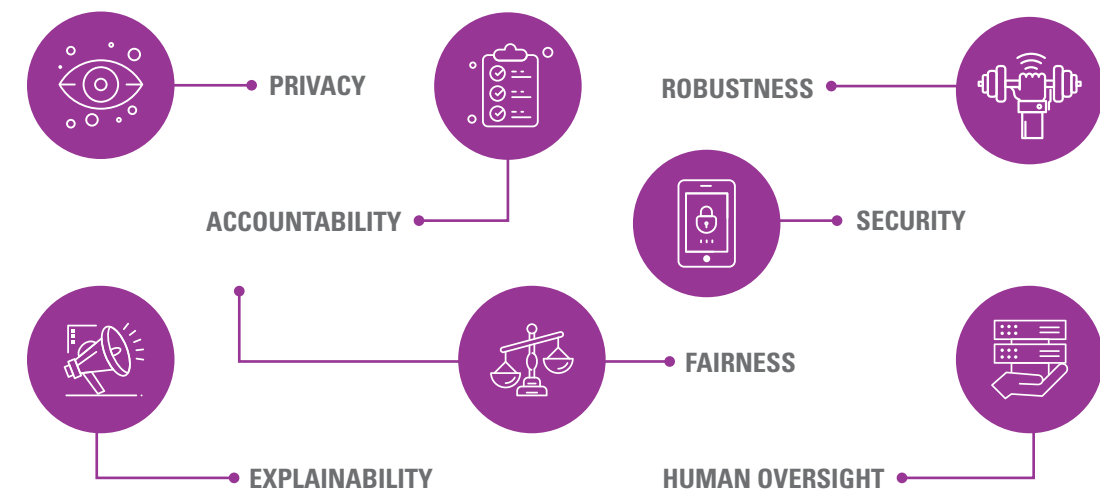
Foreword: Privacy as a key pillar of ethical and responsible AI	iii
Executive Summary	1
A new risk landscape for individuals, organizations and society	4
Challenges to responsible AI governance	14
Privacy's evolving role in right-sizing AI	20
Do I need a ruler, a tape measure or a multitool?	26
Does it take a village or a unicorn?	32
Conclusion	36
Appendix 1 — Approach	37
Contacts	39

Foreword: Privacy as a key pillar of ethical and responsible AI

The use of artificial intelligence is [predicted](#) to grow by more than 25% each year for the next five years and could contribute over \$15 trillion to the global economy by 2030.

Leveraging AI provides great benefits and opportunities for the world, but it's clear frameworks enabling consistency, standardization and responsible use are key elements to AI's success. To achieve this goal, public institutions and organizations have published numerous governance guidelines about the responsible and ethical use of AI over the last few years. While the formulation of principles in these guidelines varies, there is consensus around key principles, including privacy, accountability, robustness, security, explainability, fairness and human oversight.

Key principles in responsible AI governance guidelines



However, privacy is more than just one principle among the others; to a large extent, living up to responsible AI principles when processing personal data is already required by various privacy regulations around the globe. Prominent examples include the right to explanation and the fairness principle in the EU General Data Protection Regulation and the U.S. Federal Trade Commission [holding](#) AI developers and companies accountable for AI being transparent, fair and empirically sound.

Against the backdrop of yet uncharted risks associated with AI and machine learning, following responsible AI principles and putting them into practice through comprehensive responsible AI programs is growing fast.



Katharina Koerner
Principal Researcher - Technology, IAPP

Given the amount of organizations with mature privacy programs already in place and the broad overlap of privacy regulations with responsible governance principles for AI, several questions arise. How can AI and data privacy coexist in an organization’s AI and privacy governance? How can this complicated technical and policy landscape be navigated?


Can the nascent field of responsible AI benefit from the experiences and established processes in privacy? In other words — Privacy, quo vadis? Will you lead the way?



Jake Frazier
Senior Managing Director, IG, Privacy & Security, FTI



Executive Summary



This report explores the state of AI governance in organizations and its overlap with privacy management. We focused on companies' change processes when striving to use AI according to responsible AI principles such as privacy, accountability, robustness, security, explainability, fairness and human oversight. This study aims to report on different approaches to governing AI in general and to explore how these nascent governance efforts intersect with existing privacy governance approaches.

Scope

The scope of the study is limited to interviews with stakeholders in organizations from across six industries in North America, Europe and Asia: technology, life sciences, telecommunication, banking, staffing and retail.

In each interview, we focused on five areas: governance, risk, processes, tools and skills. We identified where the organization stood with implementing responsible AI governance, processes, and tools and how they aligned or planned to coordinate those emerging functions and policies with existing privacy processes.

In addition, we gathered data from facilitated workshops and interactive survey sessions at the annual IAPP Leadership Retreat with 120 privacy thought leaders in July 2022. These individuals included chief privacy officers, technologists (data scientists and AI engineers), lawyers and product managers.

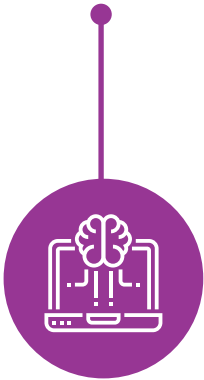


Summary of results

- **It’s a marathon, not a sprint!** The fast-growing importance of clear governance guidelines for the responsible use of AI leads to a turning point with organizations going through various maturity levels on their responsible AI journey. Of organizations included in the survey, 10% have not yet formulated responsible AI guidelines. At 20%, the most mature organizations have already rolled out responsible AI practices. The remaining organizations are either about to start or already in the process of including responsible AI in their governance.
- **A growing and complex risk landscape:** Our analysis shows organizations are aware that, with the deployment of AI systems, new risk vectors require adapting internal governance approaches to new expectations, standards and norms. The report found the AI and privacy risks top of mind for organizations are privacy, harmful bias, bad governance and lack of legal clarity.
- At the same time, there is potential for misalignment stemming from different risk terminology in AI and business operations.
- **AI and privacy have a key overlap:** While required in several areas of law and grounded in Responsible AI principles, explainability, fairness, security and accountability are also requirements in privacy regulations. While growing efforts to manage the responsible use of AI by organizations have been documented, the impact and utilization of existing privacy programs have not been explored in detail. It is important for privacy professionals to understand how responsible AI as a governance approach is applied in practice, how it intersects with privacy governance and how it can learn from privacy.
- **Higher AI maturity shows close alignment with privacy:** Organizations that clearly explain their governance models for responsible AI describe a close collaboration with privacy governance, often building upon privacy programs. We found several drivers for this decision and describe in detail what motivates organizations to utilize their privacy experience for responsible AI governance.

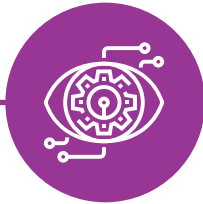
→ **Leverage what you have — join forces with privacy:** Our data indicates more than 50% of organizations building new AI governance approaches are building responsible AI governance on top of existing, mature privacy programs.

→ On an operational level, there are several ways privacy processes are used for responsible AI. AI impact assessments are typically merged or coordinated with privacy impact assessments. Of respondents, 40% are building algorithmic impact assessments on top of existing processes for privacy or data protection impact assessments. In general, security and privacy by design are considered a model for ethics by design.



40%

of respondents are building algorithmic impact assessments on top of existing processes for privacy or data protection impact assessments.



> 50%

of organizations building new AI governance approaches are building responsible AI governance on top of existing, mature privacy programs.

→ **Organizations seeking tools and skills for responsible AI:** Organizations are struggling to procure appropriate technical tools to address responsible AI, such as consistent bias detection in AI applications. While workforce capacity building and cultural change are in their infancy, momentum for responsible AI as an expected and necessary governance aspect is growing as organizations build products or services on AI and machine learning processing personal data.



Contacts

Joe Jones

Director of Research
& Insights, IAPP
jjones@iapp.org

Jake Frazier

Senior Managing Director, IG,
Privacy & Security, FTI
jake.frazier@fticonsulting.com

Katharina Koerner

Principal Researcher –
Technology, IAPP
kkoerner@iapp.org

Follow the IAPP on social media

Published January 2023.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2023 International Association of Privacy Professionals. All rights reserved.