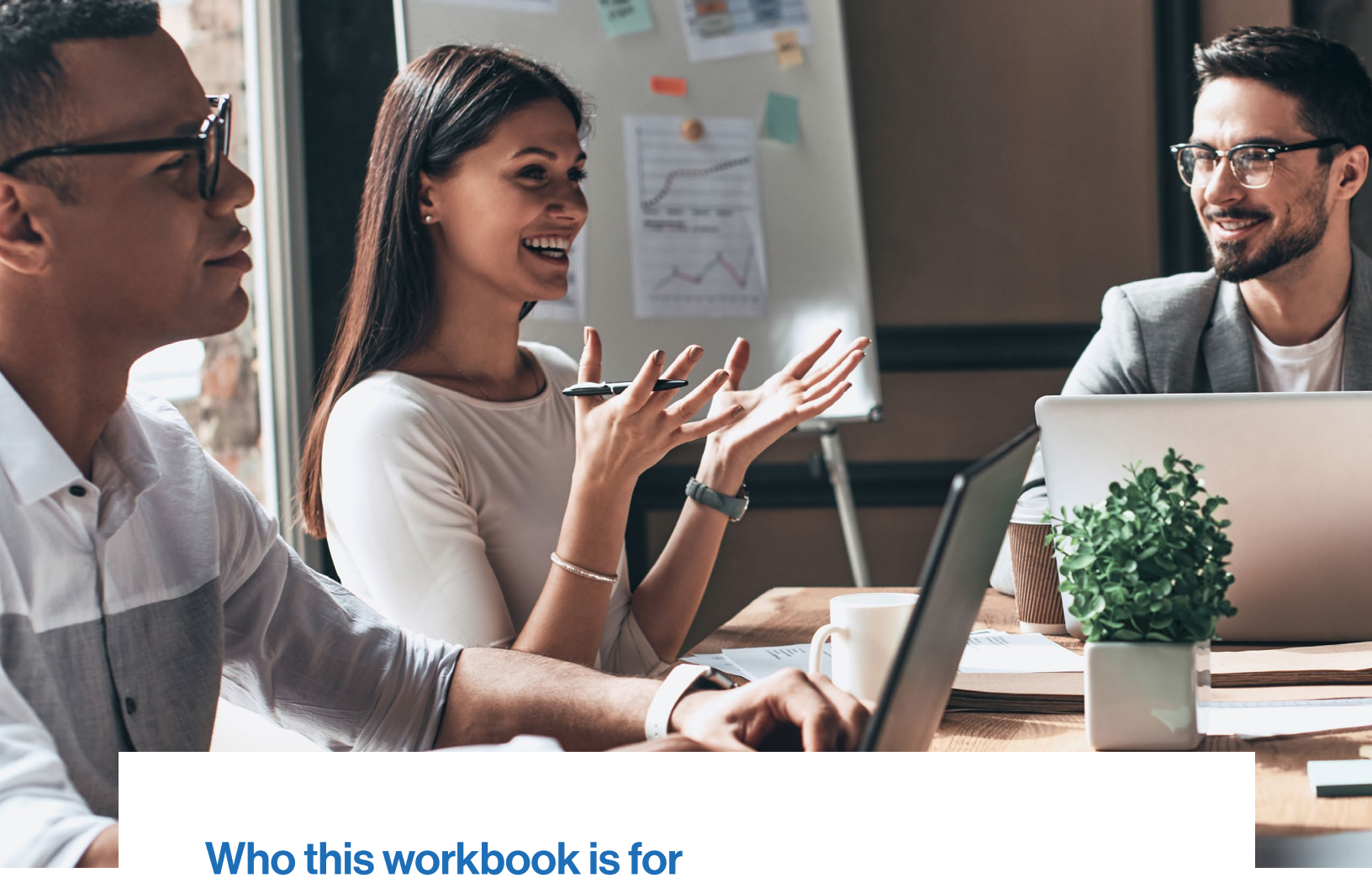
Collibra

Workbook

The blueprint for data privacy in the age of AI

The data privacy workbook

Table of contents



Who this workbook is for

This workbook is designed for organizations and teams that want to get data privacy right from the start, especially when it comes to AI. Data privacy requires effort from across the organization, including AI governance stakeholders.

Pro tip: If you're a data privacy professional and you don't have a seat with your AI governance team, get one now.

What will you learn?

AI offers great promise. But it also presents significant risks, especially when it comes to data privacy. This workbook is designed to help you:

- Introduce and guide you through establishing a data privacy program that works seamlessly with your emerging AI programs. You'll learn how to align data privacy practices with AI development and deployment, ensuring that privacy is integrated from the ground up
- Help you make an effective, successful data privacy program a reality at your organization. We'll provide you with the tools and frameworks necessary to build a robust data privacy infrastructure that supports and enhances your AI projects

By the end of this workbook, you'll not only have a comprehensive understanding of the steps involved in effective data privacy, but also practical insights into executing these steps effectively in the age of AI.

Key benefits of data privacy

In today's digital world, a robust data privacy program is fundamental to maintaining customer and stakeholder trust and data integrity.

- **Stay in compliance with data and AI laws and regulations:** Understanding the legal landscape involves navigating the complex, ever-evolving regulatory requirements, including GDPR and the EU AI Act. Compliance not only helps avoid hefty fines and legal repercussions, but also involves proactive risk management
- **Build trust with customers and stakeholders:** The effect of transparency and accountability around data collection, usage and protection assures stakeholders, including investors and partners, that data privacy and security are top concerns for your organization
- **Enhance reputation and future business opportunities:** As a direct result of strong data privacy practices, an enhanced reputation as a leader in data privacy can deliver a competitive advantage and strengthen brand loyalty
- **Significantly reduce data breach costs:** With the successful implementation of preventative measures, your organization can not only minimize the the risk of breaches, but also reduce the impact when breaches do occur
- **Drive efficiency:** Understanding the data you hold can help discover customer insights and behaviors as well as increase operational efficiency by uncovering inefficient workflows, helping you reduce costs and increase revenue

Why data privacy and AI are inextricably linked

AI systems rely on vast amounts of data to function effectively. And this data often includes sensitive information. Without robust data privacy measures, the unlawful or misguided use of personal data in AI can lead to significant privacy breaches, eroding trust in your organization and potentially causing significant harm (and expense). Laws and regulations, such as the EU AI Act, underscore the importance of data privacy when it comes to AI. These regulations require organizations to comply with strict data protection standards. The truth is that compliance isn't just a legal obligation; it's a critical component of AI development. Adhering to these regulations helps your organization not only avoid hefty fines and legal repercussions, but it also can foster a culture of trust and accountability.

Moreover, when personal information is shared, your customers expect it to be protected and used appropriately. Failure to do so can result in a loss of customer confidence, damaged reputation and decreased business opportunities. Additionally, the use of personal data in AI can lead to discriminatory outcomes if not properly managed. Robust data privacy measures can help mitigate these risks. But your organization must be vigilant in auditing AI systems for biases and implementing corrective measures. Finally, intellectual property challenges occur when data used to train AI models includes proprietary information, trade secrets and other intellectual property. To safeguard intellectual property, organizations must implement stringent data privacy practices as they push for greater innovation.

By prioritizing data privacy, your organization is positioned to harness the full potential of AI while maintaining compliance and customer trust.

Questions to get started with data privacy

Assessing data privacy is vital for successful AI projects. These questions will help your organization get started with evaluating data governance and AI-specific privacy practices, ensuring compliance and building trust.

Questions to ask yourself:

1. Do you have an understanding of where all of your data is?
2. Do you have both structured and unstructured data that will be used in AI?
3. Is data tagged to indicate PII or other sensitive data classes?
4. Are datasets properly protected to ensure only specific people or teams can access them?
5. Does your organization have designated data owners?
6. Will any customer data be accessed, stored or otherwise processed by AI?
7. Will data that is considered sensitive (like PII) be used by AI?
8. Will the AI model use or implement any type of social scoring or real-time biometric data?

Critical capabilities for success

To build a successful data privacy program in the AI era, you'll need several critical capabilities. These essential capabilities ensure robust data governance, regulatory compliance and the trust needed for effective AI implementation.

1. Automated privacy operations to support global regulations
2. Data catalog to inventory data across your organization and deliver faster insights
3. Automated data governance workflows and controls to drive trust
4. Enterprise data lineage to scale
5. Embedded privacy by design to drive compliance

Next, let's look at the questions that will guide how you implement these critical capabilities.

Critical capability 1 | Automated privacy operations to support global regulations

Automation is essential in driving effective privacy operations and complying with regulations. These questions will help your team evaluate automated tools and processes, ensuring they effectively manage data privacy, mitigate risks and maintain compliance across all your AI initiatives.

1. How do you ensure your data privacy operations comply with global regulations such as the EU AI Act, GDPR and CCPA?
2. Do you have alerts/triggers in place to know when to re-visit your compliance?
3. Can you utilize automated tools like PI discovery and classification to streamline data privacy operations?
4. How frequently do you audit your AI systems to ensure they comply with privacy laws?
5. Do you have a process for handling data subject access requests (DSARs) with your AI system?
6. How do you manage data deletion and retention?

Critical capability 2 | Data catalog to inventory data across your organization and deliver faster insights

A robust data catalog, preferably part of a scalable data intelligence platform, is essential for enterprise-wide data privacy and governance. These questions will help you evaluate the security measures, access controls and guide the overall design of your catalog and platform to ensure it supports your data privacy and AI goals effectively.

1. Is your data catalog designed to support secure, enterprise-wide usage?
2. Do you have a marketplace for employees to quickly "shop" for the data they need?
3. How do you ensure the security of data across different departments and teams?
4. Can you conduct an comprehensive data inventory and map relationships across the data ecosystem to understand data flows and dependencies?
5. What measures are in place to prevent unauthorized access to your catalog and data intelligence platform?
6. Can you implement role-based UIs and permissioning to ensure compliant and secure data access?
7. How do you manage and monitor access controls within your catalog and data intelligence platform?
8. Are there regular security assessments conducted on your data intelligence platform?
9. Do you have the triggers in place to know when a new assessment needs to be done?

Critical capability 3 | Automated data governance workflows and controls to drive trust

Data governance with automated workflows and controls is crucial for building trust and ensuring data privacy within AI initiatives. These questions will help you assess how well your organization integrates data governance practices into its processes, ensuring consistent policy adherence, risk mitigation and accountability across all data activities.

1. How does your organization implement active data governance to ensure data privacy?
2. Are most of your current procedures manual and inherently error-prone?
3. What processes are in place to identify and mitigate risks related to data privacy in AI?
4. How do you ensure that data governance policies are followed across the organization?
5. How is data governance embedded into the lifecycle of your AI projects?
6. Do you have metrics to measure the effectiveness of your data governance efforts?

Critical capability 4 | Enterprise data lineage to scale

Enterprise data lineage is essential for scaling data privacy and AI initiatives. These questions will help you evaluate how well your organization tracks and monitors data flow, ensures sensitive data is classified and protected, and detects and responds to data breaches effectively.

1. How do you maintain visibility over your enterprise data to ensure privacy?
2. What tools do you use to monitor and track the lineage of data across the organization?
3. How do you ensure that sensitive data is appropriately classified and monitored?
4. What processes are in place to detect and respond to data breaches?
5. How do you scale your data privacy practices as your data volume grows?

Critical capability 5 | Embedded privacy by design to drive compliance

Embedding privacy by design into your AI development process, as well as implementing critical capabilities like data assessments, is crucial for ensuring compliance with privacy regulations. These questions will help you assess how well privacy considerations are integrated into your AI projects from the outset, ensuring continuous adherence to privacy laws and fostering a culture of proactive privacy management.

1. How is privacy by design integrated into your AI development processes?
2. What steps do you take to ensure that AI models are designed with privacy in mind from the start?
3. How do you gather information about data and AI models?
4. How do you ensure continuous compliance with privacy regulations throughout the AI lifecycle?
5. Are there specific privacy impact assessments conducted for AI projects?
6. How do you train your AI and data teams on the principles of privacy by design?

7 steps to setting up a data privacy program

Ready to get started? Here are 7 crucial steps to establishing an effective data privacy program that will support AI governance, safeguard your organization's data and maintain the trust of your stakeholders.

1. **Understand regulatory requirements:** Identify, understand, and continuously monitor the data/AI laws and regulations that apply to your organization, such as GDPR, CCPA, HIPAA and the EU AI Act
2. **Catalog and map data:** Do a comprehensive data inventory to identify what data you collect, where it is stored, how it is processed and who has access to it
3. **Establish a data governance framework:** Define policies/procedures for data handling, including data collection, storage, processing, sharing and disposal, as well as assign specific data governance roles
4. **Implement privacy by design:** Integrate privacy considerations into the design and development of products, services and processes. Conduct Privacy Impact Assessments (PIAs) for new projects or changes to existing processes to identify and mitigate privacy risks
5. **Enact robust protection measures:** Implement measures to protect data, such as encryption, access controls and data anonymization. Regularly update and patch systems to protect against vulnerabilities
6. **Employee training and awareness:** Continuously train employees on data privacy policies, procedures and best practices
7. **Continuous monitoring and auditing:** Regularly monitor and audit data privacy practices to ensure compliance and identify areas for improvement. Use data protection impact assessments (DPIAs) and regular audits to assess the effectiveness of privacy controls

Become a data privacy leader

By prioritizing data privacy, your organization is positioned to harness the full potential of AI while maintaining compliance and enhancing customer trust. Implementing a comprehensive data privacy program not only protects your organization from legal and reputational risks but also can strengthen customer loyalty. Now is the time to take action and lead the way in data privacy, ensuring that your AI initiatives are both effective and ethical.

Embrace proactive data privacy practices—including privacy by design, regular training, continuous monitoring and robust incident response plans—to navigate AI complexities confidently. Leading in data privacy means setting a standard, demonstrating your commitment to protecting personal data, and driving long-term success as a trusted and ethical AI leader.

Take the initiative now.

Implement a comprehensive data privacy program to ensure your AI initiatives are compliant, secure and trusted. You can create a future where innovation and privacy go hand in hand.

We can help. Learn more at Collibra Data Privacy.

Collibra

Helpful resources

Looking to begin your data privacy or AI governance journey? Collibra is here to help.

- Collibra Data Privacy Factsheet
- AI governance: 4 steps to success
- IDC insights: The critical role of AI governance for AI success
- AI governance 101: The basics of governing AI
- AI governance framework
- AI readiness checklist

If you are interested in learning more, please visit collibra.com

CO20-P0824-11