Step-by-Step Guidance for Building a Privacy Program

1 November 2023 - ID G00761935 - 8 min read

By Analyst(s): Legal and Compliance Research Team

Initiatives: Privacy Program Management

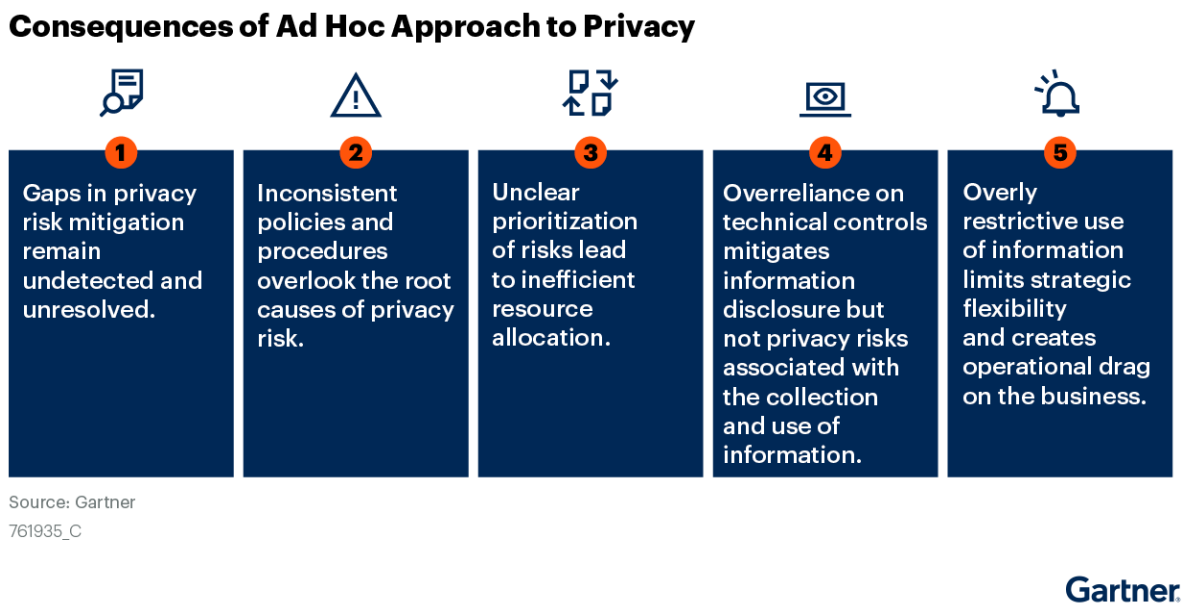
The recent influx of privacy regulations amid a widening privacy risks landscape is compelling organizations to quickly develop their privacy programs. Privacy leaders must use this research to understand the five foundational requirements of establishing a privacy program from scratch.

Strategic Planning Assumptions

- By 2024, 75% of the world's population will have its personal information covered under modern privacy regulations. [1]
- By 2024, over 80% of organizations worldwide will face modern privacy and data protection requirements. [1]
- By 2025, privacy lawsuits and claims related to biometric information processing and cyber-physical systems will result in over $8 billion in fines and settlements. [2]
- Through 2026, organizations that mishandle personal data will suffer three times more financial damage from class actions and mass claims than from enforcement sanctions. [2]

Pursuing an ad-hoc approach to privacy in this context fails to reduce risks and can result in various negative consequences (see Figure 1). Roughly $1.75 billion in GDPR fines have been levied against corporations in the first eight months of 2023 alone. [4] Together, these trends build a compelling case for establishing a privacy program in organizations that lack one.

Figure 1. Consequences of Ad Hoc Approach to Privacy



Privacy leaders should formalize their programs to ensure privacy risks are effectively identified and managed and to build customer loyalty and brand value by building greater confidence in their business's data handling practices.

Despite the associated benefits, the multiphased process of establishing a privacy program can be hard to navigate. Many new privacy leaders are often unsure where to start, which components to include, and which program elements to focus on first. The resources outlined in this research support privacy leaders in setting up an initial privacy program by providing guidance on five foundational program requirements:

1. Develop a Privacy Program Scope, Structure and Strategic Plan
2. Understand and Manage Privacy Risks
3. Develop External and Internal Privacy Policies
4. Deploy Privacy Trainings and Communications
5. Establish Metrics and Track Performance

Analysis

New demands are being placed on privacy programs. In response to new regulations and emerging privacy risks from rapid adoption of new technologies such as AI, privacy leaders must operationalize a growing array of privacy processes and activities throughout the enterprise at scale. Despite this, 36% of legal and compliance leaders report that their organizations do not have independent privacy programs, often resulting in piecemeal adoption of one-off policies, risk management activities and other program elements. [3]

Research Highlights

Some recommended content may not be available as part of your current Gartner subscription.

Develop a Privacy Program Scope, Structure and Strategic Plan

The first step of developing a privacy program is to decide the responsibilities, reporting and resources of the program. Failure to do so results in an unclear understanding of strategic privacy priorities and an uneven distribution of dedicated resources.

Structuring a privacy team has no one-size-fits-all approach. Instead, privacy leaders must consider which competencies (e.g., quick decision making, consistent messaging, visibility into functional processes, etc.) are most important to the success of their program, choose a structure that is best suited to developing them (see Top In-Demand Skills for Growing Your Privacy Program) and develop a strategic plan that fits your company's needs, and uses limited program resources to deliver the greatest impact.

Tool: Step-by-Step Guidance for Developing the Scope and Structure of a Privacy Program

This tool provides privacy leaders with step-by-step instructions for defining their privacy program's scope and mandate, organizational and governance structures, roles and responsibilities, and budget requirements. This tool helps answer the following questions:

- How should we structure our privacy team?
- Which responsibilities and activities should the privacy program own?
- Who are the key decision makers of a privacy program?
- How is a privacy program usually funded?

How to Prioritize Your Privacy Workload to Drive a High-Impact Strategy

Because there is not a one-size-fits-all approach to developing a privacy roadmap, privacy leaders must understand how to develop criteria to prioritize projects and initiatives that are best suited for their company's needs. This research identifies four new privacy program "archetypes", and shows which criteria privacy leaders should use to deliver the highest impact when deciding how to prioritize their team's workload.

Ignition Guide to Developing a Prioritized Strategic Plan for Privacy

Privacy leaders can use these tools to rigorously assess and prioritize privacy workload, and develop a strategic plan composed of initiatives and projects that will deliver the highest level of impact.

Case Study: Proactive Prioritization Criteria to Triage Privacy Activities

Privacy leaders often struggle to maintain focus on strategic activities in the face of seemingly urgent regulatory and business demands. Read this case to see how Franklin Templeton solved this problem by proactively identifying criteria to triage regulatory and business support activities as they arise.

Understand and Manage Privacy Risks

Next, privacy leaders must have a clear understanding of the privacy risks they need to manage and mitigate within their organization. Many organizations pursue ad hoc privacy risk management activities such as reviewing risks on a function-by-function or even project-by-project basis. This approach leads to gaps in risk identification as well as inconsistent assessment and management of privacy risks throughout an organization.

Leading organizations ensure they obtain a holistic view of the risk landscape and put measures in place to consistently manage risk. To achieve this, privacy leaders must follow a standard, documented and repeatable process for assessing privacy risks and create and monitor mitigation plans to address residual risks.

Tool: Step-by-Step Guidance for Establishing a Privacy Risk Management Process

Privacy leaders should use the detailed instructions provided in this tool to inform decisions on privacy risk framework selection, risk assessment, risk prioritization and action plan communication. These steps help achieve regulatory compliance and minimize organizational risk. This tool helps answer the following questions:

- Which privacy risk framework is right for my organization?
- How can we create a process to identify and assess privacy risk?
- How can we develop and communicate a risk mitigation action plan?

Privacy Risk Assessment Tool

Privacy leaders can use this survey tool to identify and assess the organization's most significant privacy risks. This tool helps answer the following questions:

- How can I build a complete view of privacy risks in the organization?
- Where does privacy risk reside in the organization?
- Where are there differences in risk perception among different segments in the organization?

Develop External and Internal Privacy Policies

After establishing a risk management process, privacy leaders must create and maintain external and internal privacy policies that ensure the organization is complying with regulatory data protection requirements. An external privacy policy discloses the ways an organization gathers, uses and manages personal data. An internal privacy policy, on the other hand, provides standards and guidance on the use, collection, management and sharing of personal data within the organization. Most organizations may already address privacy or privacy-related issues in some form across various policies. However, inconsistent privacy policies may result in customer mistrust due to poor transparency, employee noncompliance with privacy standards, and high-risk activities like unapproved internal or third-party data sharing.

Tool: External Privacy Policy Generator

This interactive tool helps privacy leaders create a customizable external privacy policy for their organization. The external policy can be generated based on the clauses selected in three privacy program variables: policy objective, level of detail and tone.

10 Privacy Policy Updates to Boost Transparency and Achieve Compliance

Privacy leaders can implement the updates on this list to achieve compliance with the most recent consent notice and opt-out requirements, and to discover ways to improve the user experience of their policies for customers and employees.

Deploy Privacy Trainings and Communications

Employees' noncompliance with privacy standards and misuse of information is the most reported privacy risk (57%), given employees have more opportunities for misuse than external actors. [5] Such internal misuse of information can lead to heavy penalties, fines and reputational damage. Leading organizations know effective training and communications are an important tool in driving employee compliance with privacy standards. However, creating effective training and messaging that breaks through the noise is an increasingly difficult challenge in a hybrid work environment.

Tool: Prepackaged Presentation for 2023 Data Privacy Training

Privacy leaders can use this customizable presentation to train employees on the basics of data privacy, including its definition, importance, key regulatory trends, and company policies and guidelines on data privacy.

Best Practices for Developing Privacy Training and Communication in a Hybrid Work Environment

With 75% of hybrid or remote knowledge workers saying their expectations for working flexibly have increased, privacy leaders must adapt their existing privacy training and communications accordingly. [6] This report, highlighting best practices from leading organizations, helps privacy leaders develop effective training and communication relevant for a hybrid work environment. This report helps answer the following questions:

- What types of training and communication should we deploy?
- How should we tailor training to specific roles or functions?
- How do we create engaging privacy training and communications?
- What is the ideal format, content and channel for privacy training and communications?
- How do we ensure employees retain privacy training?

Establish Metrics and Track Performance

As privacy programs evolve to keep pace with a constantly changing regulatory environment, a diverse set of stakeholder demands and ongoing digital transformation, privacy program owners must demonstrate program effectiveness. To do so, they must develop a balanced set of metrics that track the progress of privacy's regulatory-focused goals and business-centric initiatives. Metrics also help privacy program owners determine how to correct potential problems ranging from the productivity of the privacy team to the management of privacy risks.

Tool: Tactical Guidance for Creating a Data Privacy Metrics Program

This comprehensive, step-by-step tool helps privacy leaders select, measure, and report on metrics that are directly correlated with key privacy strategic objectives and corporate goals. This tool helps answer the following questions:

- Who is responsible for selecting the metrics?
- What are the common metrics for assessing privacy program effectiveness?
- How can we measure and monitor the selected metrics?
- How can we analyze, report and act on the metrics results?

Evidence

[1] Hype Cycle for Privacy, 2021

[2] Predicts 2022: Privacy Risk Expands

[3] Independent program in this context is defined as one that is not led by a chief privacy officer. 2023 Gartner Legal, Corporate Compliance and Privacy Budget and Efficiency Survey.

[4] GDPR Enforcement Tracker

[5] Emerging Privacy Issues (1Q21)

[6] Redesigning Work for the Hybrid World: Opportunities for Knowledge Workers

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Designing a Privacy Impact Assessment Process

Ignition Guide to Developing a Privacy Liaison Program

2021 Privacy Program Structure, Roles, Responsibilities and Effectiveness Benchmarking

Tool: Customizable Privacy Impact Assessment Training for Business Partners