What Is Your Privacy and Data Protection Strategy?

Author: Corlane Barclay, Ph.D., PMP
Date Published: 26 February 2021
Related: COBIT 2019 Design Guide | Digital | Spanish
中文
Download PDF
SHARE

The global data privacy and protection landscape has been radically transformed within the last five years, notably with the enactment of the EU General Data Protection Regulation (GDPR) in 2018. The environment has seen an increased focus on the:

- Levels of cross-border processing demands
- Personal data requirements of new and emerging technologies
- Varying use or adoption of technologies
- Escalating reports of security breaches
- Legislative and regulatory responses from various jurisdictions across the globe

> "IT IS IMPERATIVE THAT EACH ORGANIZATION UNDERSTANDS THE NATURE OF THE PROCESS TO DEVELOP A PRIVACY STRATEGY AND ADOPT RIGOROUS STANDARDS AND PRACTICES TO STRENGTHEN THEIR PRIVACY INITIATIVES."

This dynamic state of privacy protection has caused increased demands on privacy officers or persons managing privacy programs in their organizations. The increased privacy demands have created a critical need for clarity and structure in managing organizational privacy programs to meet

the complex array of compliance requirements, which, for some organizations, span multiple jurisdictions and laws.

It can be argued that a robust privacy strategy is key to determining the privacy compliance programs and initiatives in a coordinated manner and helps deliver success. The privacy strategy is not a one-size-fits-all approach. Each organization is likely at different stages of the compliance journey or is facing different requirements. For example, where an organization's core business process involves processing sensitive or special data categories, different or more detailed technical and legal standards or safeguards may be required to be implemented in its daily operations. Similarly, a multinational organization requires a complete understanding of the legal and regulatory requirements for each country of operation and how the laws and standards in those countries of operation affect the organization at the global and domestic levels.

Regardless of the industry type or size of the organization, developing a privacy strategy is a complex and intricate process.[1] It is imperative that each organization understands the nature of the process to develop a privacy strategy and adopt rigorous standards and practices to strengthen their privacy initiatives. According to a recent article, not too long ago, there were few compelling reasons for organizations to embed privacy considerations deeply into their larger business strategies.[2] Now organizations face greater risk to privacy and security, and, as such, devising a focused privacy strategy aligned with the organization's business strategy can yield better results. Therefore, data privacy should be a critical component of the organization's strategic management process, which can be clearly articulated through the organization's vision, values and policies.

A strategy is generally defined as a plan of action designed to achieve a long-term or organizational goal. Therefore, the privacy strategy must be a clear plan of action designed to ensure compliance with established privacy standards, rules and laws. The privacy strategy should outline how the privacy principles defined by the respective laws are applied or adopted in the organization. For example, according to Article 5(2) of the GDPR, the controller has an obligation to demonstrate compliance with the principles relating to processing personal data.[3] As outlined in Article 5(1) of the GDPR[4] and according to the US State of California Consumer Privacy Act (CCPA), for example, an organization under that respective jurisdiction must implement appropriate measures to demonstrate compliance.[5] In Jamaica, section 21 of its Data Protection Act outlines the data controller's duty to comply with certain privacy standards at the end of the transition period.[6]

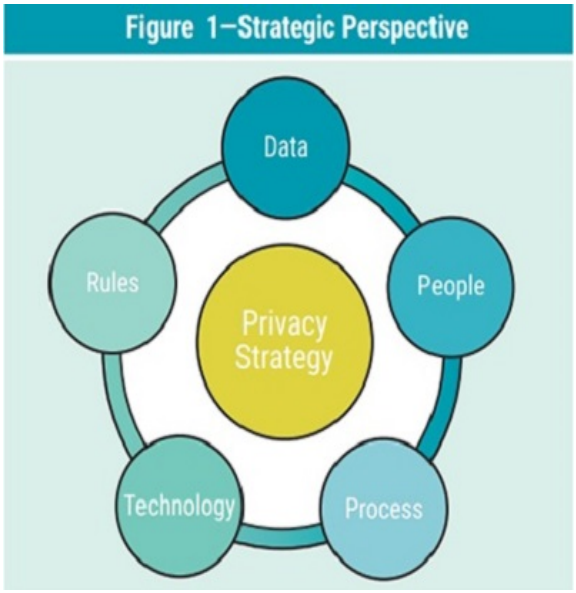
These respective privacy obligations will, no doubt, affect all areas of an organization's operations. To ensure compliance, organizations must consider:[7]

- The systems and services involved in processing personal data
- The users of these systems and services
- The policies, processes and procedures adopted to enable proper execution of the legal obligations

These factors underscore the importance of strategic oversight and the need to have a holistic understanding of the organization's privacy parameters. Therefore, developing a privacy strategy requires an integrated and thorough understanding of the organization's:

- Applicable privacy laws and standards
- Personal data being processed
- People who may interact with or process the personal data
- Various forms of processing undertaken by the organization
- Business processes needed to facilitate the processing of the data
- Tools and technologies used to process the personal data

Figure 1—Strategic Perspective



Defining a Privacy Strategy

This understanding directs the strategic perspective illustrated in **figures 1** and **2**, which seek to outline an organization's key considerations on defining their privacy management activities.

Figure 2—Components of the Privacy Strategy

Data	Categories of Personal Data
People	Privacy stakeholders within an organization's ecosystem
Process	Business activities relating to processing personal data
Technology	Applications, tools and technologies used to process personal data or support privacy management
Rules	Applicable privacy laws and standards

Data
The data component refers to diverse forms of personal data being processed by the organization or on its behalf by third parties. An organization needs to understand the different categories of personal data being processed, including which users, processes and applications interact or process the personal data. It is also critical that organizations understand the forms of processing that take place. In essence, organizations must know what, who, where and when in relation to their processing of personal data.

People
This component refers to the stakeholders in the organization's privacy process. This includes:

- The users of the personal data
- The data subjects
- The privacy personnel of the organization

Understanding the roles and functions of each stakeholder, how these stakeholders interact or process the different forms of data, and the forms of processing undertaken by the organization will

help to better understand the personal data under the organization's care and the associated processing activities.

Process
This component refers to the organizational processes that affect the various forms of processing the personal data, including those that are technology-enabled and those that are not. In addition, the forms of processing and where in the business process those personal data are processed are also contemplated here alongside the data component.

Technology
The technology component refers to the applications, tools and technologies used to process the personal data or support the processing of the data. This understanding helps to guide the implementation of the necessary technical safeguards required to effectively manage security and privacy risk.

Rules
The rules component refers to the comprehensive set of applicable privacy and related laws and standards to which an organization must adhere. In addition, understanding the circumstances where the organization is exempted will assist in promoting compliance understanding. The personnel responsible for the strategy must understand that the rules will evolve, not only in terms of the growing list of jurisdictions where the organization does business, but also in terms of amendments and changes to the collection of the rules that govern the privacy operations of the organization.

The organization's privacy strategy must build safeguards that create and support the organization's privacy vision and applicable privacy laws and standards. The components feature a tightly coupled system of interactions and intersections. However, to properly define the privacy strategy and ensure that the organization's privacy vision and applicable privacy laws and standards are executed correctly, the organization must understand how these components work individually and collectively.

The expected benefits of this approach to the privacy strategy are:

- Increased clarity and structure to the privacy initiatives and programs
- Reduced gaps in organizational privacy planning and execution
- Improved levels of executive support and buy-in
- Refined engagement and coordination at all levels of the organization including the data subjects
- Improved strategic alignment between the business and privacy strategies

Toward a Privacy Strategy

There is no single correct way to devise a privacy strategy. However, how to apply a strategic perspective approach to create a suitable privacy strategy is introduced here. A key component or input in the privacy strategy process is to understand and confirm the organization's privacy compliance requirements. A privacy compliance article proposes an initial step that involves assessing the privacy laws that are applicable to the organization.[8] In addition, it is also important to

determine the specific privacy needs for the organization. This assessment helps to determine the goals, scope and priorities of the privacy strategy. **Figure 3** defines the parameters needed to create a strategy. Six steps are identified as crucial in setting the stage for an effective privacy policy.

Figure 3—Overview of Privacy Strategy

Privacy Strategy	Key Questions
Establish the framework.	What are the guiding principles necessary for managing privacy in the organization?
Create the vision.	What is the organization's goal for privacy management?
Agree on the scope.	What are the limits or parameters of this privacy strategy?
Develop the strategic objectives.	What are the organization's desired outcomes related to privacy?
Agree on the actions.	What activities are necessary to achieve the strategic objectives?
Provide good governance.	What must the organization do to ensure success when creating the strategy?

Establish the Privacy Framework

First, the key stakeholders and executives must agree on the terms of reference and guiding principles that will inform the strategy development process. The organization's terms of reference and guiding principles determine the specific standards, best practices and framework. The organization's experience and insights define what works best for that organization.

Create the Vision

Creating a privacy vision for the organization determines the organization's goals for privacy and data protection. The planned goals are specific to an organization. The defining goals depend on the organization's size, industry, privacy maturity level, organizational priorities, compliance requirements and competitive environment. For example, the vision might focus on the organization's global competitiveness, regulatory compliance or meeting the needs of data subjects.

Agree on the Scope

Using the defined vision, the organization then agrees on the scope or breadth of activities. The scope of activities will likely involve multiple steps and activities over several financial years to complete. For example, the strategy's scope may be based on the identification of specific technical and organizational measures and activities required to achieve compliance with a specific privacy law at the end of the transition period.

Develop the Strategic Objectives

The next step is to identify the elements needed to achieve the agreed-on vision within the agreed-on scope. It is a good practice to use specific, measurable, attainable, relevant and time-bound (SMART) objectives based on the components of the strategic perspective outlined in figure 1. The organization can then identify all the objectives for achieving its vision stated previously. That may include implementing specific privacy standards or privacy by design principles in its operations. This process can also further help clarify the actions required to achieve these strategic objectives.

Agree on the Actions

In this phase, the organization identifies the set of actions and programs needed to achieve the stated strategic objectives already identified. The action plan includes identifying who, what and when. An action plan helps determine who is responsible (people), what is the activity to be executed (program) and when is the activity due (deadline). Developing an action plan requires an organization to set

priorities and determine the resources available. Also, agreeing on performance indicators that define success for each outcome is crucial to the success of this process and the strategy in general.

Provide Good Governance
A governance mechanism is a critical component in managing and monitoring the outcomes of the strategy. This step builds on the previous steps where the operational accountabilities were identified. Establishing a governance mechanism creates important levels of accountabilities that can be used for oversight and coordination. The governance mechanism includes important review stages, which confirm that planned privacy activities are proceeding well. Where the agreed privacy activities are not proceeding as planned, the organization can take corrective actions. Another integral activity is the stakeholder awareness and engagement process that is used to heighten knowledge about privacy in the organization and in the privacy strategy and minimize the risk of failure, lack of buy-in or low adoption of privacy initiatives.

Conclusion

Privacy management is a contemporary business challenge. Many organizations across the globe are grappling with their respective local privacy laws and applicable international privacy laws. For organizations to overcome this challenge, they must navigate a complex array of tasks that touches on a diverse set of concerns from disparate stakeholders. Developing a clear and robust privacy strategy is one of the first critical steps necessary for an organization to establish a solid framework for its privacy programs. Adopting the five-lens strategic perspective: data, people, process, technology and rules, combined with general privacy strategy considerations, are useful tools for implementation. This insight enables an organization to identify the key considerations required to create an effective privacy strategy and to ensure successful execution of privacy programs for greater compliance. Ensuring that these important elements are incorporated into the strategy process can help an organization achieve its privacy vision and compliance with its applicable privacy and data protection laws and standards. Stated differently, each organization, having confirmed the relevant privacy laws and standards to which they must adhere, must ensure alignment of their privacy strategy to the applicable privacy laws and regulations through consistent adoption of the elements discussed. A simple framework for developing a robust privacy strategy that is further aligned to the organization's business strategy is essential to success.

> "DEVELOPING A CLEAR AND ROBUST PRIVACY STRATEGY IS ONE OF THE FIRST CRITICAL STEPS NECESSARY FOR AN ORGANIZATION TO ESTABLISH A SOLID FRAMEWORK FOR ITS PRIVACY PROGRAM."

Endnotes

[1] Densmore, R. R. (ed.); *Privacy Program Management, Tools for Managing Privacy in Your Organization*, International Association of Privacy Professionals, (IAPP), USA, 2019, https://iapp.org/resources/article/privacy-program-management/
[2] Redman, T. C.; R. M. Waitman; "Do You Care About Privacy as Much as Your Customers Do?" *Harvard Business Review*, 28 January 2020, https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do
[3] European Parliament and the Council of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council, *Official Journal of the European Union*, 27 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[4] *Ibid.*

[5] California Consumer Privacy Act (1798.100 - 1798.199.100), USA, 2018, http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
[6] Data Protection Act, Jamaica, 2020, https://japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202020.pdf
[7] Barclay, C.; "The Road to GDPR Compliance: Overcoming the Compliance Hurdles," *ISACA® Journal*, vol. 1, 2019, www.isaca.org/archives
[8] *Ibid.*

CORLANE BARCLAY, PH.D., PMP

Is an attorney-at-law, technology consultant and the principal of Smart Projects 360, a consultancy, advisory and research services business that specializes in project management, cybersecurity and privacy management. She can be reached at clbarclay@gmail.com.

Previous Article

Next Article

QUICK LINKS

ISACA Journal

FAQs

Members: Opt-In To Print

Become A Member

Current Issue >

Journal CPE Quiz

Download Journal App

Archives >

Submit an Article
The ISACA Podcast
Past Journal Archives

Advertise ›

Editorial Calendar
Non-members Subscribe