FEATURE

Building Compliance Resilience Amid a Patchwork of Data Protection and Privacy Laws

CORLANE BARCLAY | PH.D., PMP

Is an attorney at law, legislative drafter, and technology consultant with a keen interest in the interconnection of technology, law, and policy. Barclay has more than 20 years in the private and public sectors and has led national and regional initiatives relating to cybersecurity, data protection, and privacy.

She recently established DPO Caribbean, a regional provider of data protection and privacy solutions that include regulatory compliance support and policy and legislation drafting services. She can be contacted at **clbarclay@gmail.com**.

In today's evolving digital society there has been exponential growth in digital dependence and interdependence, which has led both good and bad actors to recognize and exploit the significant value of data. This situation has generated substantial risk to individual privacy and security, highlighted by the estimated 5.9 billion records compromised worldwide as a result of data breaches in 2023.[1] In light of this pervasive dilemma, many countries have adopted regulatory mechanisms to help ensure that the rights of individuals are protected, personally identifiable information (PII) is safeguarded, and organizations are held accountable, especially regarding any operational failures or breaches involving personal data.

Despite the relative maturity of privacy laws and regulations in jurisdictions such as Australia, Canada and the European Union, it arguably was the extraterritorial nature of the EU General Data Protection Regulation (GDPR), the modernization of individual privacy rights, the establishment of breach reporting requirements, and other developments that radically transformed the modern global data protection legislative landscape. Many countries have either reformed their laws or drafted new laws, and a significant portion of them have been modeled after or influenced by the EU GDPR. The result has been accelerated growth in privacy legislation globally. According to the United Nations Conference on Trade and Development, more than 70% of countries around the world have enacted privacy laws.[2]

Organizations operating across multiple states or countries must contend with multiple privacy laws and regulations consisting of nuanced, divergent, or even conflicting obligations and requirements.

The current landscape is perhaps best described as a patchwork of laws and regulations relating to data protection and privacy. Comprising so many different elements, requirements and obligations, the data protection and privacy legislative regimes appear variegated. The patchwork of data protection and privacy legislation may be viewed within the context of:

- **The diversity of laws within countries**—For example, in the United States a variety of privacy legislative measures have been enacted in multiple states such as California, Colorado and Virginia.
- **The diversity of requirements and obligations within and across regions**—For example, privacy laws have been adopted at the national level in a growing number of countries in Africa, the Caribbean, and Latin America.

These trends have implications for trade, international data transfers or flows, and the general competitiveness of organizations. Organizations operating across multiple states or countries must contend with multiple privacy laws and regulations consisting of nuanced, divergent, or even conflicting obligations and requirements. With this set of circumstances, the compliance load undoubtedly becomes more significant. Given the expanding sphere of regulatory laws and obligations, compliance requirements may be viewed as excessive. The increased compliance load also has notable implications for organizations across major business functions (**figure 1**), mainly:

- **Capacity impact**—This is viewed as the number of individuals, the types of talent or the extent of expertise required to effectively support the organization's expanding compliance function. Thus, the demands on privacy

officers and employees managing privacy programs in their organizations are likely increased.[3]

- **Process impact**—This may be contextualized as the compliance process itself and its impact on the organization's business and systems routines that affect the processing of personal data.
- **Economic impact**—This is viewed as the costs associated with maintaining compliance and the effects of noncompliance. For instance, the economic impact of noncompliance is evident in the fines, sanctions, and penalties levied for violations of privacy laws and regulations and the likely reduction in profitability due to reduced customer trust.
- **Technology impact**—This includes the adoption and use of supporting technologies, including artificial intelligence (AI), to help the organization demonstrate compliance and support compliance activities.

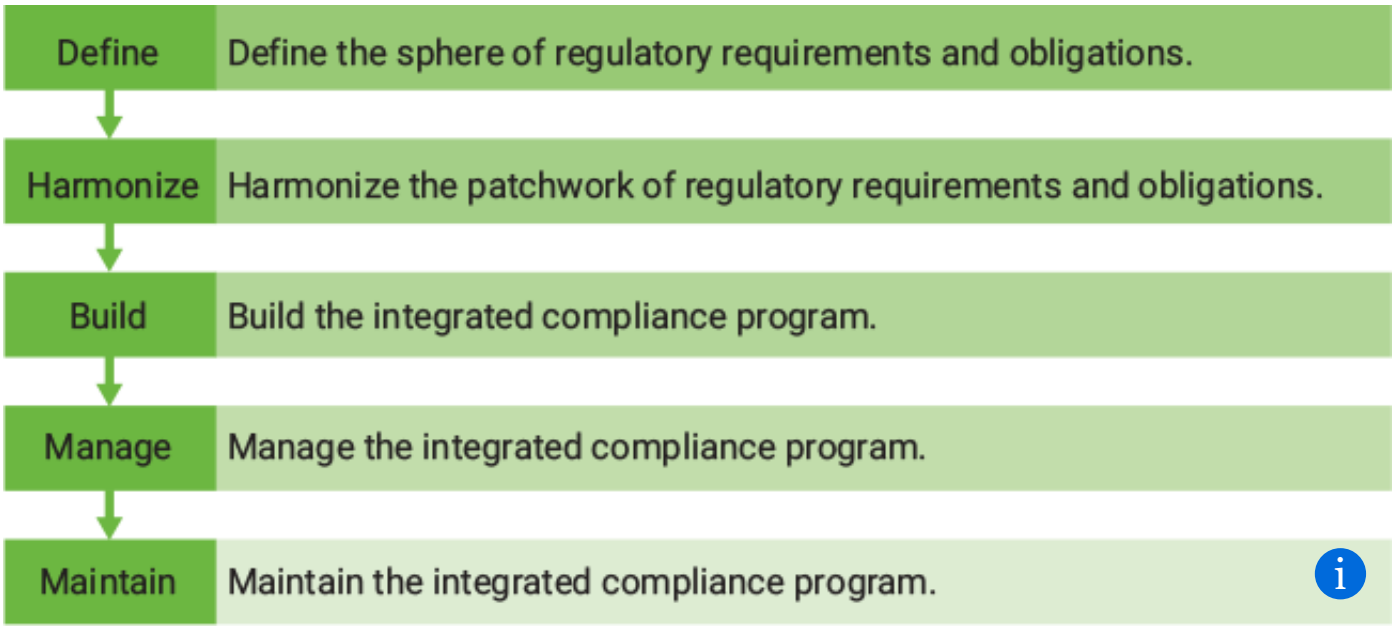
Therefore, the far-reaching impact of increased diversity in privacy laws and regulations at the global, regional, and national levels is clear, and it is reasonable to appreciate that organizations may be inclined to shy away from compliance programs because of their intricate mix of activities, varying requirements, and diverse expectations, despite the business and regulatory necessity.[4]

However, despite the apparent burden associated with compliance, it should be seen as a necessary investment or even a competitive necessity, especially in today's hypercompetitive digital environment. Against this background, it is important that organizations employ appropriate techniques and strategies to develop and maintain robust compliance programs that are responsive to the dynamic legislative environment and can exhibit compliance resilience. Compliance resilience is viewed as the ability to proactively and efficiently safeguard privacy, protect data, and maintain a robust compliance posture in the face of the growing collection of privacy laws and regulations.

Compliance by Design

A compliance by design framework is introduced to address privacy compliance management in relation to one or more data protection and privacy laws and regulations. Compliance by design utilizes the principles of privacy by design,[5] security by design,[6] the five-lens strategic perspective[7] and general good practices in optimizing an organization's data protection and privacy compliance posture. Therefore, privacy compliance considers the full product life cycle process from design to end of product life, the categories of consumers and their nature of processing, and the applicable regulatory requirements in one or more jurisdictions.

The compliance by design framework (**figure 2**) consists of five iterative processes aimed at streamlining the regulatory compliance program, reducing compliance risk, and optimizing individual privacy and the protection of personal data:



1. Define the sphere of regulatory requirements and obligations.

2. Harmonize the patchwork of requirements and obligations.
3. Build the integrated compliance program.
4. Manage the integrated compliance program.
5. Maintain the integrated compliance program.

Define

With an acknowledgement that the sphere of regulatory requirements will likely continue to expand, given the reach of an organization's products and services and the growing slate of data protection and privacy laws and regulations requiring compliance, developing a deep understanding of the collection of applicable regulatory requirements is essential. The define stage of the process entails determining which regulatory mandates are applicable to the organization, taking into account its existing and envisaged processing activities, and identifying the data subjects and their locations. Defining the baseline standards and technical and organizational controls to be adopted to ensure that requirements are met—including privacy by design principles—is carried out at this stage.

For instance, a United States-based app developer must understand the current and emerging state and federal laws and regulations applicable to its targeted user base. Assessing which consumers are minors and determining their rights, ascertaining the scope of their sensitive personal data, and logging the different requirements across states and other jurisdictions along with the impact they will have on system design and compliance processes are all critical preliminary steps. The developer must also determine the systems implications for embedding privacy into the app design and set privacy and security defaults at the product or compliance design stage. Similarly, a banking institution operating in several countries in the Caribbean must define the applicable privacy laws. Few countries in the region are without a modern privacy regime and those with current laws, such as Belize and Jamaica, have varying requirements.

Given the potential impact on product and service life cycles, business routines,

policies and procedures, a defined roadmap and an approach to tackling compliance requirements while optimizing user privacy are also considered at this stage.

Harmonize

To account for the diversity in legislative languages and requirements, organizations must carefully reconcile their obligations among the collection of privacy laws and regulations to help ensure an accurate and complete picture of their privacy compliance and risk profiles. The harmonization of applicable regulatory requirements and obligations is necessary to support the streamlining of the compliance program and the adoption of appropriate measures across the product life cycle and the organization's business processes and routines. The harmonize stage process involves the identification, analysis, consolidation, and mapping of relevant and applicable provisions under the laws and regulations to which the organization must adhere, which are identified in the define stage.

Notably, jurisdictions may differ in terms of the attributes of a data subject (whether living or deceased, for example), bases and requirements for breach notifications, forms of sensitive personal data, bases for undertaking privacy or data protection impact assessments (DPIAs), conditions for designating or appointing data protection officers, and other legal requirements. To amplify the implications for compliance, there are several general obligations of privacy laws and regulations in several jurisdictions to understand:

- **Breach notifications**—In Jamaica, the data controller has an obligation to notify the information commissioner not only of security breaches but also of any contravention of data protection principles.[8] Under the Barbados Data Protection Act, a data controller has a duty to report on personal data breaches only.[9] Both jurisdictions have the same period for notifications (i.e., 72 hours); however, Barbados provides an exception to the timing of notifications in circumstances where breaches are "unlikely to result in a risk to the rights and freedoms of an individual."[10] This provision is similar to article 33 of the EU GDPR, which further states that if the notification is not

made within 72 hours, it must be accompanied by reasons for the delay.[11] Thus, as part of the notification process an organization would consolidate the conditions for breach reporting and confirm which actions are required by different regulators and when.

- **Registration requirements**—The registration of organizations is required in certain jurisdictions. For example, the Jamaica Data Protection Act requires the registration of data controllers,[12] and the Kenya Data Protection Act requires the registration of both data controllers and data processors.[13] On the other hand, the EU GDPR does not require this form of registration. An organization operating in jurisdictions where these laws apply must appreciate the administrative requirements, including any recurring registration timelines and the application of any exemptions to registrations and registration fees.
- **Conducting DPIAs**—Although it is generally considered good practice for organizations to conduct DPIAs, among US state privacy laws, there are variations in the requirements. Organizations covered by privacy laws in Utah and California, for example, must manage different obligations. Utah does not specify a requirement for conducting DPIAs,[14] but the US State of California Privacy Rights Act (CPRA) requires regular submission of a risk assessment concerning the processing of personal information to the US State of California Privacy Protection Agency.[15] Organizations covered by these laws must meticulously identify and map their requirements to reduce compliance and privacy risk.

Based on the foregoing, an organization may consider several options, such as mapping the provisions and applying each individually, harmonizing the provisions and implementing the most stringent across the compliance program, or adopting a hybrid approach. Keeping track of the enforcement provisions across jurisdictions is also necessary in managing business and compliance risk.

The abilities to adapt, learn, and evolve are essential requirements in building resilience and are key components in bolstering regulatory compliance amid the growing privacy laws and regulations worldwide.

Build

The build stage process involves actively embedding good privacy practices into organizational processes to help manage the growth in the sphere of regulatory obligations. This takes into account the data, people, processes, technologies, and rules[16] necessary to support an integrated compliance program and to manage and safeguard privacy and business risk. Therefore, establishing the organization's integrated compliance program involves the identification, development, and management of the tools and resources necessary to demonstrate compliance, such as new and revised codes, scripts, and privacy- and security-related policies mapped to the jurisdictions. Likewise, the identification, development, and management of the tools and resources necessary to support the organization in demonstrating compliance or in building a robust privacy culture are also crucial, such as the staffing of the privacy function and the adoption of useful privacy-enhancing technologies. Thus, the core and supporting resources to enable optimized compliance and reduced privacy and business risk are effectively governed.

Manage

Managing privacy and compliance risk is a key part of the manage stage process. This process involves active monitoring and evaluation of the effectiveness of the integrated compliance program and implementing corrective actions when required. The ability to adapt to the dynamic regulatory environment through appropriate monitoring and planning is reflected in this process.

Indicators of success include a reduction in privacy violations and compliance

gaps and risk, the development of strong privacy teams supported by a suitable structure, and the strengthening of partnerships within ecosystems, including with regulators.

LOOKING FOR MORE?

- Explore the Privacy Regulatory Lookup Tool. ***www.isaca.org/privacy-regulations-lookup-tool***
- Learn more about, discuss and collaborate on privacy and compliance in ISACA's Online Forums. ***https://engage.isaca.org/onlineforums***

Maintain

The abilities to adapt, learn, and evolve are essential requirements in building resilience and are key components in bolstering regulatory compliance amid the growing privacy laws and regulations worldwide. The maintain stage process takes into account active learning and development to ensure that the organization maintains its compliance posture in the dynamic regulatory environment. This process serves to enable the organization to adopt a proactive stance to changes in the regulatory environment and wider ecosystem to aid in the management of the collection of laws and regulations. This entails employing good governance and learning practices to enable the continued evolution and growth of the organization's integrated compliance program. Key activities include keeping abreast of regulatory developments in the relevant jurisdictions, tracking the evolution of good privacy practices and standards, and managing the organization's growth and maturity, particularly in relation to privacy and compliance management. As changes in the regulatory environment occur, their impacts are closely examined within the context of the organization's operational

environment and the regulatory requirements and obligations are consolidated, amended, and harmonized.

Conclusion

Organizations are continuously pivoting as they adjust to new regulatory regimes and requirements and the growing array of approaches to consider in managing privacy risk and protecting personal data. This leads to additional pressure on compliance teams, which can lead to increased business and regulatory risk as a result of a less-than-optimal compliance program. Building compliance resilience is an important step in overcoming some of these challenges. A five-step process for integrating good practices in the full product and data life cycles to support the growing collection of privacy laws and regulations confronting organizations is introduced. An adaptive approach to the protection of privacy and personal data, which is at the center of the integrated compliance program, can provide advantages such as improved management and coordination of privacy compliance programs and more effective risk management.

Endnotes

1 Ford, N.; "List of Data Breaches and Cyber Attacks in 2023," IT Governance, 5 December 2023, ***https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023***

2 UNCTAD, "Data Protection and Privacy Legislation Worldwide," ***https://unctad.org/page/data-protection-and-privacy-legislation-worldwide***

3 Barclay, C.; "The Road to GDPR Compliance: Overcoming the Compliance Hurdles," *ISACA® Journal*, vol. 1, 2019, ***www.isaca.org/archives***

4 Barclay, C.; "What Is Your Privacy and Data Protection Strategy?," *ISACA Journal*, vol. 2, 2021, ***www.isaca.org/archives***

5 Cavoukian, A.; "Privacy by Design: The 7 Foundational Principles—Implementation and Mapping of Fair Information Practices," Internet Architecture Board, ***https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf***

6 Cybersecurity and Infrastructure Security Agency, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default," USA, 13 April 2023,

https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

7 *Op cit* Barclay, 2021

8 Jamaica Houses of Parliament, "The Data Protection Act, 2020", Part IV, Section 21, Jamaica, 2020, ***https://japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202020.pdf***

9 The Barbados Parliament, "Data Protection Act, 2019," Section 63, Barbados, 2019, ***https://www.privacylaws.com/media/4517/data-protection-act-2019-29.pdf***

10 *Ibid*.

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Article 33, 2016, ***https://eur-lex.europa.eu/eli/reg/2016/679/oj***

12 *Op cit* Jamaica Houses of Parliament

13 The Parliament of Kenya, "The Data Protection Act, 2019," Part III, Section 18, Kenya, 2019, ***https://www.odpc.go.ke/dpa-act/***

14 Utah State Legislature, Consumer Privacy Act, 2022, USA, ***https://le.utah.gov/~2022/bills/static/SB0227.html***

15 California Legislative Information, California Consumer Privacy Act of 2018, USA, 2018, ***https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5***

16 *Op cit* Barclay, 2021