CEP Magazine - April 2020
Privacy: No longer a check-the-box function

By Daniel Solo and Brooke Sweeney

Daniel Solo (dsolo@secondlineadvisors.com) is the founder of New York–based Second Line Advisors, an executive search firm for risk management, compliance, financial crime, data privacy, legal, and regulatory affairs. **Brooke Sweeney** (bsweeney@secondlineadvisors.com) is an associate at Second Line Advisors.

- linkedin.com/in/danielsolo
- linkedin.com/in/brookeosweeney

While the United States is typically known for having the toughest regulatory standards in financial services globally, it has fallen short in the privacy regulatory landscape.

The European Union has led the way in the fight to protect consumers' personal data with the implementation of the General Data Protection Regulation (GDPR),[1] which went into effect on May 25, 2018. Brazil has also passed a substantial privacy regulation, the General Data Protection Law (LGPD),[2] which will go into effect in August of 2020. The United States' first state-level data security regulation—the California Consumer Privacy Act[3] (CCPA)—went into effect on January 1, 2020. Many other states are beginning to introduce their own privacy bills too.

These regulations, however, are difficult to fully interpret and require clarification. Before the CCPA went into effect, over a dozen amendments were made to address and clarify ambiguous clauses of the regulation. Furthermore, CCPA and these new state-level legislative proposals are far from being a federally encompassing law in the way that the GDPR is for the EU. Nevertheless, the acceleration of global regulation is triggering an increased awareness of privacy from not only institutions that are collecting massive amounts of data, but also from consumers themselves, who are becoming more informed about their personal information and how it is being used.

Parallels between compliance and privacy

As a result, the privacy function as a whole has evolved. This evolution is similar to the way in which the compliance function evolved in the early 2000s. Roughly 20 years ago, post the crises of Enron and WorldCom, and with the advancement of regulations (Sarbanes-Oxley, Patriot Act, etc.), the role of the compliance officer took an evolutionary step. For the most regulated industries, the function has transitioned out from under the legal department to either stand as an organizational peer or to be viewed as a part of the risk management function. With its new prominence at institutions, the chief compliance officer (CCO) role came with significant responsibility and liability, which are still topics discussed today. The challenge of being an institution's CCO began to call for a broader skill set of great partnership, influence, and leadership, and we believe the same evolutionary steps are occurring with the privacy function today.

There are parallels to how the compliance function matured post-Patriot Act, where it doubled in size due to the efforts needed solely toward anti-money laundering obligations—which soon also included the management of sanctions concerns, anti-bribery and corruption, and the Foreign Corrupt Practices Act. Together, this became

known as financial crime compliance. We view the combination of corporate challenges as being similar to the consumer and digital spaces, which tie in privacy, cybersecurity, ethics, data, and fraud. As these functions mature alongside each other, the concept of digital governance is starting to establish itself as a combined function.

The evolution of privacy

Privacy has transitioned from a part-time, one-person job to a robust, actionable program that requires all verticals of an organization to be involved and dedicated in order to be compliant. With this, the chief privacy officer (CPO) has come front and center, as their set of responsibilities has evolved, and new challenges have emerged. In order to comply with regulatory pressures, CPOs are charged with building a flexible program that can adjust for conflicting compliance regulations. This is made more difficult given that the laws are years behind technology. In addition, the increasing nature of threats to privacy—for example, attempts to steal information and data breaches—has created a significant reputational risk for companies and heightened the need for strong privacy programs. For today's CPOs, it is essential to have a thorough understanding of company data and a strong handle on the scope of that information.

The day-to-day relationships and reporting lines of the CPO have also shifted in order to keep up with the rapidly and continuously evolving regulatory landscape. Historically, CPOs primarily worked with the chief information security officer. While this partnership is still vital, CPOs have begun to regularly and closely interact with the chief data officer, as well. As a result of this shift, privacy initiatives have largely transitioned from reactive to proactive. In terms of reporting line, the CPO had typically been positioned within legal. Recently, a significant number of organizations have moved privacy into compliance or enterprise risk management. It is now common for CPOs to report up to the CCO. This shift serves as a signal that privacy has become a priority for organizations when it comes to compliance and risk.

Fostering a privacy culture

In order to build and support a successful privacy program, companies face the feat of hiring a strong team in a market with an increasingly high demand for privacy talent. Privacy cannot be viewed as a one-time project. Rather, it must be incorporated into the everyday agenda of everyone in the organization. Thus, the best way to approach privacy is fostering it as a culture. The success of any privacy program is dependent on continuous attention, cross-functional teamwork, and a sustainable overall approach.

For many organizations, ethics is incorporated as part of the company culture and strictly upheld by a code of conduct. Privacy should be treated in the same way. There are many parallels between the roles that ethics and privacy play in an organization. Notably, both have significant internal and external fronts. While crucial for consumers, ethics and privacy also hold high stakes for employees and internal operations. In the same way that ethics must be understood and upheld by everyone in a company, privacy is also cross-functional. It takes education and collaboration from every team and department in order to create a successful culture of privacy.

Conclusion

Once considered a best practice and check-the-box item, privacy has come forth as a mandatory and prominent function for any company that collects personal information from consumers. In today's data-driven and technology-centric world, it is clear that the laser focus on privacy is here to stay. GDPR, CCPA, and LGPD are only the beginning of regulations and initiatives that will force regulators to turn their attention to privacy. Organizations will have to find a way to comply with the substantial requirements that these regulations demand, or they are bound to quickly fall behind. It seems likely that privacy will become a deciding factor in whether consumers choose to engage with a company. At all institutions, public or private, the obligations and

requirements for an effective privacy program will, without question, require attention of the CCO.

Takeaways

- New privacy and data protection regulations are forcing companies that collect personal information to become compliant.
- The privacy function is evolving in a similar way that the compliance function did in the early 2000s.
- As a result, the role of the chief privacy officer has become a priority, especially as new responsibilities emerge and challenges arise.
- The demand for privacy talent is increasing as companies attempt to foster a culture of privacy and build successful programs.
- The rise of the privacy function will require attention from the chief compliance officer.

1 Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. L119.
2 Lei Geral de Proteção de Dados Pessoais, nº 13.709/2018 (Braz. 2018).
3 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 to 1798.198 (West 2018).