



Privacy culture:

The new corporate redesign

By **Sharon Bauer**

Senior Manager, Forensic
KPMG in Canada
416-777-3336
sharonbauer@kpmg.ca

*This article was originally
published on 29 October 2018 at
www.thelawyersdaily.ca*

The rise in privacy breaches has caused consumers to become increasingly concerned about the way in which organizations are handling their personal information. As consumers experience a paradigm shift towards the need for trust and transparency before handing over their personal information, organizations need to adjust the way they perceive compliance with privacy legislation and standards.

Privacy compliance is no longer a business inhibitor; instead it is a business enabler. If organizations want to build a trusting relationship with their customers, they need to look within and adjust the architecture of their organization and foster a culture that genuinely aligns with the expectation of their customers.

In-house counsel may be delegated the role of also performing the privacy function of a business because the organization is under the mistaken assumption that privacy is a legal problem. It is not a legal problem. In fact it is not an IT problem either. Privacy is a "business problem". Privacy cannot be siloed; it does not fit into just one portfolio; it affects the entire organization. In-house counsel needs to advise the organization that the privacy program should align with all the business functions including human resources, procurement, project management, and risk and compliance to name a few.

According to the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, an organization is required to appoint Chief Privacy Officer (CPO) who will be accountable for the organization's privacy compliance program.

Today, organizations are still unsure of where the CPO should be situated in the organization. The confusion may be because there is no right answer. Every organization is structured differently and what may work for one business may not work for another. What can be certain is that the CPO must be able to establish and implement privacy and security controls, assess and revise the privacy management plan, and represent the organization in the event of an investigation. Most importantly, the CPO needs

to break down all silos and be agile and flexible so as to work with all functions of the organization and ensure privacy alignment. The CPO needs to identify opportunities to facilitate collaboration and integration. The CPO needs to report to senior management and C-suite, and encourage those at the top to adopt a "privacy culture" as opposed a simple "privacy compliance" agenda.

Once C-suite executives recognize that protection of personal information is a social or even personal responsibility and a business enabler, a privacy culture is born. The privacy mission and statement of the organization will then infuse with the rest of the organization creating a privacy mindset and culture throughout the entire organization. Privacy will then be embedded in the design, management, and organization of the business; a concept known as Privacy by Design.

Privacy legislation such as the EU's *General Data Protection Regulation (GDPR)*, one of the strictest data protection regulations, has been viewed by organizations as a difficult and expensive compliance venture. While the GDPR aims to give consumers control over their data, it is also meant to strengthen consumer trust in the digital economy by forcing organizations to assess and improve their data governance in the hopes that a privacy culture will be developed. This is a win-win situation for both organizations and consumers.

Prioritizing privacy will undoubtedly improve security within the organization. Most privacy breaches are related to employee negligence. Employees who recognize the responsibility that comes with personal information will be more diligent when handling personal information and more skeptical of suspicious activities, such as phishing or social engineering.

A privacy culture is a business advantage that all organizations should value and implement. Although some may view a redesign of the organization as a costly endeavor, there is no doubt that it is a great return on investment.

kpmg.ca/rethinkrisk
#rethinkrisk