ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Privacy Now: Data Protection Counsel Are Change Agents by Design

Technology, Privacy, and eCommerce

The Mission

Privacy laws are proliferating and adapting rapidly. The organizational shifts and change management needed in most organizations to accommodate requirements and obligations under existing and developing data protection laws are significant, and the advocacy skills of privacy counsel are likely to be put to good use on a daily basis.

If this is your role, you have already begun to demonstrate to your organization that privacy law touches every aspect of business operations. Like it or not, the chances are good that you have found yourself in the role of change agent. *(Congratulations, you're doing it right.)*

As a change agent enlisted in the name of privacy you may find that — in addition to what you bring to bear in your own right — you have been issued some critical tools and supplemental scope by an unseen quartermaster.

The Privacy Lens

Some people ran toward privacy law, some gradually learned to be mindful of its requirements, and others had organizational responsibility for privacy law thrust upon them. Regardless of through which path you came to it, if privacy is within your purview now, you have already been issued a lens

and vantage point that will impact and influence your work and thinking henceforth.

The Security Alliance

Whether through policy development, Data Protection Impact Assessments, data mapping, or contracting, an organization's privacy counsel was among the first to note that privacy and security are inextricably entwined. While data protection requirements (and the potential for fines) may lead the charge and help raise the profile of security needs in some instances, ever-changing security requirements and standards will work on behalf of privacy's interest without fail.

In most cases, security teams were early adopters of privacy requirements within their organizations and quick to incorporate the specific protocols around personal data into their policies, processes, and checklists. Most privacy counsel have learned the benefits of being proactive with regard to a reciprocal familiarity with security terminology and requirements. You don't have to become a security expert to provide robust guidance to the business on privacy law, but the points of overlap in contracting and data protection evaluation are sufficient that you would do well (or have already done well) to cultivate a sincere interest.

The Information Governance Backstop

A comprehensive information governance program is arguably the true linchpin for privacy and security and the most effective means by which to implement and evaluate data protection protocols and change. Employees need to understand what kinds of information they are handling and where and how to access, store, and dispose of the types of information in their care. Much like security, information governance is a specialization and defined profession unto itself and has its own set of rules and requirements. Those who are charged with IG oversight have long had the watch and are glad for the comity.

An organization's information governance protocols and requirements are essential to privacy counsel's understanding and assessment of how personal information is handled. The information governance program is a key mechanism by which to ensure that data minimization and classification and handling of personal data are built into every layer of process and protocols. Well-developed classification and handling policies that properly incorporate data protection principles and requirements will fold into the information governance audit program and serve to provide a periodic compliance gap analysis.

The Change Management Alarm

Where a real shift needs to occur for privacy compliance and data hygiene, privacy counsel, security, and information governance teams will need to work with leadership to ensure that every aspect of the business is aware of the scope of both the changes and the proportional change management undertaking required. Change within an organization of any size is something that should be planned and navigated with care to ensure that the culture only shifts in ways intended as a result of what is being set in place.

The Human Resources Alignment

Human resources professionals are adept at helping organizations navigate change and are already attuned to the process of adding in new protocols in support of the protection of individuals. Privacy

(both as both a human right and as a compliance requirement) is something that HR is well-poised to support, and most privacy counsel can attest that the HR function within an organization has a natural allegiance and alignment with an organization's privacy office. Where privacy counsel can work to understand and anticipate the needs of HR and its engagement with the lifecycle of employee information (beyond simply data mapping), they will be able to provide detailed guidance and assistance around specific process shifts and privacy considerations for new and changing circumstances with privacy implications.

The Inclusion and Diversity Cornerstone

Organizations that are positioned to build out or refine their diversity, equity, and inclusion (DEI) programs will find that data protection and privacy counsel play important roles in DEI. Privacy counsel can assist beyond evaluating legal requirements and organizational appetite around the collection and processing of sensitive data. The role of privacy in an inclusion program and any people analytics is key, and from an organizational culture standpoint, privacy can be a real differentiator for organizations asking their staff for additional identity characteristic information and inclusion feedback.

While a truly inclusive organization is often cited as one to which an individual can bring their full self to work, it is important to remember that many people count their privacy, and the protection of same, to be a critical aspect of their identity. Privacy can be the key to inclusion feedback and program refinement, which is, in turn, the key to meeting and maintaining organizational diversity.

Wherever anonymity is asserted or sensitive personal data is involved, privacy counsel will need to be pulled in and can provide options to help the DEI team build a privacy by design road map forward for the data they seek to collect and make use of.

The M&A Due Diligence and Integration Asset

The potential value of the use of a Data Protection Impact Assessment as a tool in both M&A due diligence and the planning for the integration of new organizations is significant and too rarely discussed.

Privacy counsel can assist in due diligence by understanding and articulating the risks around data types held, the policies and protocols in place, and the culture and awareness levels around privacy and data protection in a target company, and a DPIA can be used to run alongside and inform the acquisition and integration process.

Regardless of what is uncovered by due diligence, any shift in culture around privacy, security, and information during a merger of organizations is an opportunity to better insulate and protect the data of both entities. When integration is underway, privacy counsel and a dedicated DPIA are helpful resources in evaluating and strategizing to mitigate risk for any new information around processors, data collection, or compliance issues that come to light.

The Marching Orders

With the landscape of privacy and data protection law evolving at a rapid pace over the last many years (and months, really), privacy counsel has a substantial remit, an enviable arsenal of tools and allies, and a regular allocation of new orders that will not often self-destruct upon reading.

Privacy counsel has a distinct vantage point on an organization and will be privy from several angles to how that organization engages and interacts with shifts in policies and protocols. If you are in the role of privacy counsel you will have (and have likely already taken) many chances to highlight the ways in which data protection can be a point of insulation and integrity around of everything your organization does. If you are not in the role of privacy counsel, don't fail to learn more about your regional and international data protection laws out of deference to your privacy office. Privacy is here to stay, and there is virtually no aspect of business that it doesn't impact.

Shoshana Rosenberg

Deputy General Counsel - Privacy | Cybersecurity | Data Strategy, Chief Privacy Officer and a Vice President

Shoshana Rosenberg is the Deputy General Counsel - Privacy | Cybersecurity | Data Strategy, Chief Privacy Officer and a Vice President at WSP USA with experience across all aspects of corporate law. She is a Navy veteran, an Inclusion by Design advocate, and an international privacy law devotee who served as the global privacy lead and CPO for professional services firms for more than a decade.