Taking the Pulse of the Privacy Office

There has been no rest for privacy professionals coming out of last year’s GDPR compliance activities. California (CCPA) and other jurisdictions are bringing in new and/or amended privacy legislation creating increased demands on the privacy office.

It isn’t surprising that privacy professionals are feeling anxious and a majority still consider building a privacy program as a key responsibility and their top priority for 2019 and 2020.

What other challenges are privacy professionals facing in managing their privacy compliance efforts?

What are the realities of where they are spending their time?

How integrated is the rest of the business in privacy compliance activities?

To get to the heart of these questions, we launched our first Privacy Pulse survey in May 2019, hearing from over 100 North American privacy professionals.

KEY FINDINGS AT A GLANCE:

• Building a privacy program is the top priority
• Want to spend more time educating the business
• Documentation and data mapping dominating the time of business units
• Board reporting at regular intervals now standard
• Turnaround time for regulatory reporting a challenge

© 2019 Nymity Inc. All rights reserved.
The privacy office encompasses multiple responsibilities and often competing priorities.

Building a privacy program and safeguarding data emerged as the clear priorities for our respondents. In fact, almost half of respondents (47%) ranked building a privacy program as their top priority.

This may seem surprising as one would expect that privacy programs would have been built in the run-up to the GDPR. This could indicate that companies have been treating compliance as a tactical “check list” item and are now struggling with how to handle privacy laws that just keep coming – particularly in the US with the CCPA, Nevada, Texas, and numerous other states tabling legislation.

Of course, as mentioned, the privacy office is often faced with competing priorities with CCPA compliance activities (35%) and continued GDPR compliance activities (26%) still figuring strongly. This makes sense considering CCPA is looming around the corner and Cisco System’s report¹ found that almost a third of companies they surveyed were still working towards meeting GDPR requirements; many expect to do so within a year and almost 10% of companies believe it will take more than one year to achieve.

A DAY IN THE LIFE OF THE PRIVACY OFFICE

How are the responsibilities and priorities of privacy professionals aligning with where they are spending their time versus where they want to be spending their time?

Despite privacy policies, procedures and overall governance being a primary responsibility, our respondents want to spend 20% less of their time on documentation. Where do they want to be spending more time? Educating the business. With almost two-thirds (57%) of privacy professionals rating the level of privacy knowledge of the business as moderate to very low, their desire to divert approximately 20% of their time to education, stands to reason.

Companies have been treating compliance as a tactical “check list” item and are now struggling with how to handle privacy laws that just keep coming.
ENGAGING THE BUSINESS IN PRIVACY COMPLIANCE

Responsibility for compliance in a business unit is often assigned to a team member in addition to their day-to-day responsibilities. This may be where some of the challenges are arising with privacy knowledge in the business.

Over two-thirds (68%) of respondents indicated that business units are spending most of their privacy compliance time completing documentation and data mapping. This could be due to a number of factors: a lack of understanding on how to document their policies and procedures, a lack of understanding of privacy related terminology and how it relates to their business, a lack of appropriate tools or systems, or limited time and/or resources focusing on compliance in the business units.

In last years’ IAPP/EY Governance report, an average of only one to two part time privacy resources were available in a revenue-based business unit or internal service unit.

Business units are spending most of their privacy compliance time completing documentation and data mapping.

---

ENGAGING THE BUSINESS IN PRIVACY COMPLIANCE

The challenges with documentation being faced by both the business and the privacy office may also be leading to difficulty with regulatory reporting. **Over 75% of respondents indicated it would take them two or more days to report to regulators if required.** This is surprising as industry leading tools should be enabling privacy professionals to produce these types of reports in minutes, not days.

Streamlining compliance operations and accelerating time to compliance both in the privacy office and in the business is becoming increasingly important as the visibility of privacy compliance has been elevated to the board level. **Over 80% of respondents indicated they were reporting on privacy matters and compliance status at regular intervals to their boards with over 40% reporting on a quarterly basis.**
THE FUTURE OF PRIVACY

The role of the privacy office has gone through a renaissance over the last few years. As the regulatory environment has become more complex and the business impact of non-compliance has become more significant, over 70% of privacy professionals feel privacy has evolved into an integral part of the overall strategy and planning for their businesses.

This has also resulted in growth in the privacy function.

One respondent stated, “We have gone from privacy being 25% of one headcount to a full-fledged department in the last four years.”

Although we noted earlier that business knowledge of privacy needs improvement, our respondents also indicated an increase in involvement in business operations; actively engaging in areas such as product, and as one respondent stated, having “increased influence and earlier interaction with data centric departments involving new projects.”

“We have gone from privacy being 25% of one headcount to a full-fledged department in the last four years.”
What is in store for privacy over the next two to five years?

While there is no crystal ball, our respondents overwhelming believe (71%) that privacy will become increasingly integrated, or even embedded, into business operations.

There is also a consensus that privacy will become more complex, and data governance will be increasingly important as data types such as geolocation, biometric and industrial internet of things potentially come under the purview of data protection legislation.

Organizational awareness, business engagement, and training will become even more critical and complex in this evolving environment.
Nymity's privacy solutions enable organizations to demonstrate ongoing compliance with the GDPR, CCPA, and global privacy regulations. Nymity's solutions are built on an expert platform maintained by a dedicated in-house research team, directly embedding expert knowledge into the platform.

### HOW NYMITY HELPS

#### Reduce Complexity
Our solutions for privacy impact assessments, DPIAs, annual assessments, and vendor assessments minimize impact in your business. Nymity's expert platform learns from past assessments, using smart questions to effectively engage business representatives with their own terminology and procedures for fast and accurate assessments. Our platform identifies and sends proactive notifications on privacy risk with links to underlying regulatory supporting authority documents. On-demand reporting enables a fast and efficient response to any regulatory reporting requirements.

#### Accelerate Time to Compliance with CCPA and other Consumer Data Protection Laws
With CCPA, Nevada, Texas, and an influx of consumer data protection laws coming from the US and around the world, Nymity understands the challenges of implementing automated solutions to efficiently fulfill data subject rights requests, and manage data inventories, and records of processing activities. Nymity's solutions deliver dynamic workflows that dramatically reduce the time to complete data subject requests. DSR legal annotations are presented at every workflow step and automatically identify potentially high-risk processing according to laws in relevant jurisdictions.

#### Create a Culture of Privacy
Nymity offers the only compliance solution that enables organizations to create privacy champions through engaging training, allowing them to maintain a level of knowledge that is relevant to their role and jurisdiction. Our knowledge solutions automatically push notifications and content based on decisions, jurisdictions, and actions that are important to you and your business.

TO LEARN MORE ABOUT OUR PRODUCTS OR REQUEST A DEMO, VISIT US AT [WWW.NYMITY.COM](http://WWW.NYMITY.COM)