Benchmarking Businesses' Privacy Framework: Highlights from the 2019 IAPP-EY Annual Privacy Governance Report

October 03, 2019

IAPP and EY published their fifth annual Privacy Governance Report (Report) last week.

The authors of the Report surveyed companies across the globe to determine privacy governance trends. The Report aims to understand the structure of businesses' privacy programs (*e.g.,* budget, staffing, career development), measure privacy compliance efforts (this year, with a focus on compliance with the EU General Data Protection Regulation, or GDPR) and identify recent trends in the daily routines of privacy and data protection professionals.

While the survey respondents are from all around the world, many of the responses and trends may be relevant for Canadian businesses that are in the process of benchmarking or updating their privacy governance framework. We have highlighted in this bulletin the following topics of the Report: the role of the board of directors in privacy governance, the types of issues reported to the board, the privacy role and responsibilities within businesses, the management of third-party vendors, and the types of data subject requests that organizations receive.

Respondents

The survey respondents are privacy professionals in various roles (*e.g.*, data protection officers mandated by the GDPR, privacy officers, chief privacy officers, privacy analysts, *etc.*), from various jurisdictions, industries and business sizes.

- **Jurisdiction:** 6 per cent of the respondents are from Canada, with the remaining from the U.S. (39 per cent), the EU (33 per cent), the U.K. (13 per cent), and other countries (7 per cent).
- **Industries:** These respondents are from various industries including tech (22 per cent), financial services (22 per cent), health care and pharmaceuticals (9 per cent), government (5 per cent), consulting services (3 per cent) and other (39 per cent).

- **Size:** Most respondents come from medium or large companies with 1-4.9K employees (21 per cent), 5-24.9K employees (24 per cent), 25k-74.9K employees (11 per cent), and over 75K employees (12 per cent).

Interestingly, the Privacy Governance Report mentions that more often than in past years, survey respondents are lawyers, general counsel in particular, which may be signaling either promotion of privacy professionals to the GC role or (more likely) adoption of privacy responsibilities by GCs who previously did not pay as much attention to this issue.

Role of the Board

In the last few years, boards of directors have started to recognize privacy issues as significant legal and reputational risks. The Privacy Governance Report raises that while the role of the board of directors has always been important to privacy governance, the FTC further elevated the board's privacy role in its recent settlement order with Facebook over the Cambridge Analytica matter. In that case, the FTC not only levied a $5 billion fine on Facebook, but also required the company's board to create a special independent privacy committee to oversee and take responsibility for the company's privacy program. The SEC also reprimanded Facebook for not disclosing the risk that its customers might suffer privacy harms to its investors and ordered payment of $100 million as a fine. The Report states:

"Although such numbers are not as significant to a company with annual revenue exceeding $50 billion as they might otherwise be, they are eye-catching nonetheless and should result in greater attention to privacy issues at the highest corporate levels."

Reporting to the Board

It is interesting for Canadian businesses to consider to whom privacy leaders report within organizations. According to the Report, privacy leaders are most likely to report to the board if they are data protection officers (67 per cent), if the company has less than $100 million revenue (39 per cent), if the headquarters is located in the EU (35 per cent), or if the company has less than 5,000 employees (29 per cent).

The Privacy Governance Report states that in the U.S., the privacy leader reports to the board of directors in 10 per cent of the situations, while this number is at 35 per cent for the EU. When not reporting to the board of directors, they report to the general counsel (35 per cent of the time for the U.S. or 18 per cent for the EU), or they report to the CEO (16 per cent of the time for the U.S. or 25 per cent for the EU).

We learn that when privacy topics are reported to the board, it is usually related to data breaches (68 per cent of the time) or GDPR compliance (64 per cent of the time). The other specific privacy topics reported to the board relate to privacy program key performance indicators (58 per cent), progress on privacy initiatives (47 per cent), privacy litigation (38 per cent), number of privacy complaints (36 per cent), specific incidents (36 per cent), privacy compliance developments (26 per cent), plans and strategies to prepare for the *California Consumer Privacy Act* (CCPA) (23 per cent), privacy budget details (22 per cent), information regarding certifications and attestations

(21 per cent), material impact of CCPA (17 per cent), or questions of data ethics (15 per cent).

Privacy Role and Responsibilities

The location of the privacy role varies depending on the organizations. The Privacy Governance Report states that half of the privacy teams are located in the legal department while 22 per cent are located in regulatory compliance, 17 per cent in privacy and data protection, 14 per cent in information security, 10 per cent in corporate ethics, 8 per cent in information technology and 22 per cent in another department.

On the issue of the type of responsibilities of the respondents by jurisdiction (comparing the U.S. vs. the EU), the Report lists: GDPR compliance (72 per cent U.S. vs. 97 per cent EU), following privacy legislative developments (92 per cent U.S. vs. 80 per cent EU), service provider/vendor management (83 per cent U.S. vs. 64 per cent EU), ethical decision-making around data use (72 per cent U.S. vs. 56 per cent EU), privacy-related subscriptions and publications (60 per cent U.S. vs. 33 per cent EU), preparation for the CCPA (80 per cent U.S. vs.17 per cent EU), redress and consumer outreach (47 per cent U.S. vs. 33 per cent EU), and privacy-related web certification and seals (38 per cent U.S. vs. 21 per cent EU).

The Report shows 33 per cent of the respondents are very satisfied and 49 per cent are satisfied with their jobs. Many also expect a promotion. Their main duties include dealing with privacy policies, procedures and governance, company awareness and training, addressing issues with products and services, following legislative developments, performing privacy impact assessments (PIAs), incident response, privacy-related communications, compliance with the GDPR, design and implementation of privacy controls, addressing privacy in product development, privacy-related investigations, and data inventory and mapping.

Managing Third Party Vendors

Canadian organizations generally remain accountable for personal information transferred to a third party vendor or service provider for processing, and must therefore use measures to ensure that this personal information remains adequately protected while in the hands of the third party. It is often difficult for organizations to determine what types of measures they should take in this respect.

On this issue of third-party service providers/vendor management, the Privacy Governance Report says that:

- 94 per cent of respondents are “relying on assurances in the contract” as their method to ensure processors live up to their GDPR and other privacy and security obligations – with 88 per cent confirming that the top consideration for processor selection is the existence of data protection and information security warranties.
- 57 per cent of respondents require completion of questionnaires addressing data handling practices.
- 48 per cent of respondents require third party attestations or certifications. ISO 27001 remains the favourite (44 per cent). The other reported certifications are

EU-U.S. Privacy Shield (23 per cent), PCI (25 per cent), SOC 2 Privacy (27 per cent), ISO 27002 (16 per cent), SOC 2 HIPAA (10 per cent), ISO 27018 (9 per cent), TrustArc (formerly TRUSTe) (3 per cent) and CSA STAR (3 per cent).
- 26 per cent of respondents report conducting on-site service providers/vendor audits to vet their data-processing programs.

Other reported important considerations are carrying out due diligence of the service provider/vendor and limiting how much personal information such service provider/vendors receive.

Types of Data Subject Requests Received

Organizations often notice that when a highly publicized privacy incident or scandal occurs, there is an increase in data subject requests.

According to the Privacy Governance Report, most of the requests received from individuals in the previous year were access requests (68 per cent), followed by right to erasure requests (60 per cent), rectification requests (32 per cent), processing restrictions and objections (31 per cent) and data portability requests (14 per cent).

The most difficult type of data subject requests received involve: locating unstructured personal information (56 per cent), monitoring data protection/privacy practices of third parties (36 per cent), ensuring data minimization (28 per cent), developing an easy-to-use centralized opt-out tool (25 per cent), anonymization (20 per cent), making necessary changes to privacy notifications (9 per cent), interconnected devices (9 per cent), making changes to cookie policies (4 per cent) and requests involving artificial intelligence (4 per cent).

Conclusion

Organizations wishing to determine best practices for their privacy governance program can use the Privacy Governance Report as a benchmarking tool when establishing their program. Canadian organizations may also use the Report as a preview of what to expect in terms of privacy governance if Canada adopts a more stringent privacy statute inspired by the EU GDPR.

Other topics addressed in the report include the salaries of privacy professionals within organizations and the budgets dedicated to privacy. On this topic, the Privacy Governance Report notes that businesses are increasing their privacy-related spending and that 55 per cent of the respondents expect their privacy budget to rise in the next twelve months. This reflects the growing complexity of the global privacy landscape, with jurisdictions adopting privacy legislation at an increasing rate.

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.