THE IMPACT OF CANADA'S PROPOSED PRIVACY LEGISLATION ON COMPLIANCE AND INSURABILITY

As the means to collect, share and use personal data have changed dramatically over the past 20 years, the imperative for robust data privacy laws has come to the forefront of international discourse. One of the latest significant advancements in the Canadian market is a proposed update to federal privacy legislation. The proposed Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts marks a pivotal expansion of laws and regulations that apply to data handling and cybersecurity measures, including the enforcement of those laws and regulations. This, by extension, is anticipated to have an impact on the Canadian cyber insurance marketplace.

As both public and private corporations await these proposed changes, understanding the forthcoming legislation's potential implications is crucial for continued resilience and growth in both the Canadian and global cyber insurance marketplace. This Arch Perspective aims to dissect the potential ramifications of these legislative changes, offering insights into compliance, operational agility, and risk mitigation best practices for safeguarding Canadian organizations.

Arch | Insurance

The Impact of Canada's Proposed Privacy Legislation on Compliance and Insurability

By Chris Pitcher & Katherine Solomon

Canada's position in the global market hinges on maintaining its General Data Protection Regulation (GDPR) adequacy status with the European Union. This status, crucial for seamless data exchange between Canadian organizations and those of EU member states, is predicated on Canada providing data protections on par with the EU's stringent standards. Without achieving this equivalency status, Canadian organizations would be encumbered with additional compliance requirements, potentially hampering transatlantic trade and necessitating complex data protection safeguards.

This backdrop has generated a pressing need for legislative modernization, which is where the proposed Bill C-27 comes in. This proposed legislation aims to bring Canada's privacy laws into the current age, expanding the mandate beyond the over-twenty-year-old framework presently in place. The proposed bill is designed to address the nuances of modern data collection and usage, and better protect data from breaches, mishandling and misuse. Overall, the framework is designed to improve the trust of individuals and corporations by providing safeguards, along with greater transparency and controls available to those whose data is being collected.

The proposed legislative enhancement also aims to offer protections against targeting vulnerable demographics such as minors against invasive practices like targeted advertising or having their identifying information stored or shared for any purpose beyond what is immediately necessary for the particular transaction or purpose. By updating these laws, Canada strengthens its commitment to safeguarding personal information for all citizens, aligning with international data protection trends and maintaining its global economic competitiveness.

Embracing these changes will allow businesses to not only enhance their cybersecurity posture but also leverage their compliance to gain a competitive edge. The partnership with insurance providers will become more crucial than ever, as it will play a pivotal role in risk management strategies tailored to this new legislative context.

Q1

What are the new requirements under Canada's updated privacy legislation, and how do they impact data handling practices?

A

The proposed privacy laws introduce multiple mandates aimed at strengthening data handling practices.

The legislation calls for robust privacy management programs. This is typically characterized by a shift from reactive data protection to a proactive privacy governance framework, as well as an increased onus on businesses to craft comprehensive policies that span the lifecycle of data—from collection to deletion. These policies should be clear and communicable, not only within the organization but also to the public and regulators. Any changes to an organization's privacy policy should be communicated immediately and clearly. The privacy policy should be reviewed and updated on a regular basis, with all employees within an organization being familiar with its provisions.

The legislation would also mandate transparent data collection, usage and consent processes, which extends to informing data subjects of the practical implications of their consent, such as sharing of data with third parties and potentially recommendation algorithms. Organizations will need to delineate and explain the scope of data usage clearly and provide options for data subjects to actively manage their consent preferences where necessary. The standard applied to the adequacy of a privacy policy is one of reasonableness: whether a reasonable person would find the scope, use and retention of data collected to be appropriate for its necessary and stated purpose, and not beyond. The onus will rest with organizations to understand and implement these parameters to avoid penalties.

Finally, the proposed legislation introduces new and expanded powers of enforcement for the Office of the Privacy Commissioner ("OPC") to make orders and levy fines similar to the powers of the Data Protection Authorities in the EU member states, as well as some existing Canadian Provincial Privacy Commissioners.

Organizations will need to delineate and explain the scope of data usage clearly and provide options for data subjects to actively manage their consent preferences where necessary.

The proposed legislation also establishes an administrative tribunal to hear appeals of certain OPC decisions and to impose penalties for contraventions. The penalties are designed to scale with the severity of the breach and the size of the business, to ensure that they are impactful and will affect compliance with the law.

The impact of these proposed requirements on data handling practices could be profound for organizations that handle personal data, especially those that have not adhered to, or fallen short of, any strict provincial requirements they may already be subject to. To comply with the intent of the proposed change, organizations will need to not only align their policies with the letter of the law but also adopt a culture of privacy that permeates their operations. This cultural shift is fundamental to ensuring that data handling practices meet the new legislative benchmarks.

Q2

How will the changes in privacy legislation affect the existing cybersecurity measures and insurance policies of businesses?

A

With heightened privacy regulations demanding robust protection against breaches and a documented, strategic approach to handling personal data, existing cybersecurity measures must be re-evaluated and, where necessary, fortified not only to comply with new legislation initially but at regular intervals thereafter. For many organizations, this may necessitate investment in advanced cybersecurity technologies, skilled personnel, and continuous training and monitoring to ensure each data touchpoint is secure and compliant.

The changes also underscore the need for incident response plans that are quick to action, with a focus on minimizing damage and restoring operations. These plans should be thorough, tested regularly and updated to align with any new legislative requirements.

We anticipate these new legislative changes will create a surge in demand for cyber liability insurance from businesses that did not previously have a cyber policy, and demand for increased limits and scope of coverage for those that already have cyber policies in place, as businesses seek to mitigate the financial risks associated with their collection, use and storage of data, among other cyber risks.

Insurance providers could look to revise coverages, limits and exclusions in response to the new legislation. Industry-standard policies may become more stringent, with precise definitions of what constitutes compliant data handling practices. The onus could shift more and more to businesses to demonstrate that they have adequate data privacy and cybersecurity controls and procedures in place, as a precondition for adequate insurance coverage.

The onus could shift more and more to businesses to demonstrate that they have adequate data privacy and cybersecurity controls and procedures in place, as a precondition for adequate insurance coverage.

The prospect of additional exposure to regulatory penalties and legal costs also needs to be taken into account. With expanded powers, the Privacy Commissioner's Office will have the ability to levy substantial fines. The bill as drafted would allow up to the higher of $10,000,000 or 3% of the organization's gross global revenue—and organizations may face increased litigation risks. This has the potential to put more focus on insurance policies as a tool to shoulder additional exposure from a liability perspective in Canada.

Q3 How will the regulation of AI under the new legislation impact businesses, and what insurance considerations arise?

A A notable advancement in the proposed Bill C-27 is its adaptation to the rapid integration of artificial intelligence (AI) in business practices. Regulation of AI under the bill applies to "persons", which is defined to include trusts, joint ventures, partnerships, unincorporated associations, and any other legal entities (such as corporations), and emphasizes their legal responsibilities within the lifecycle of AI systems.

This evolution presents a dual challenge: ensuring AI systems comply with enhanced privacy standards and managing emergent risks through tailored insurance solutions.

Transparency will be a key element, with companies now obligated to maintain records regarding their AI systems and, where a system is a "high impact system" (a concept yet to be defined by regulations), to publicly disclose the rationale behind the decision-making processes of their AI systems. This will likely be especially imperative when these systems influence consumer behaviors or outcomes, ensuring that consumers are not left in the dark about the digital determinations that affect them. Effectively, transparency could potentially extend to algorithms used by organizations such that an organization should be able to explain the mechanics and outcomes of their algorithms at any given time.

In tandem with these new compliance requirements, the insurance landscape is transforming. Traditional liability coverage is expanding to accommodate the unique risks presented by AI. This includes potential errors in AI decision-making, data misuse and even the inadvertent creation of biased algorithms, particularly those that might impact vulnerable demographics. Insurers have crafted policies that cover not only the direct liabilities but also the peripheral risks, such as the costs of regulatory audits, legal defenses and the financial repercussions of non-compliance penalties.

Transparency will be a key element, with companies now obligated to maintain records regarding their AI systems and, where a system is a "high impact system" (a concept yet to be defined by regulations), to publicly disclose the rationale behind the decision-making processes of their AI systems.

Businesses must therefore not only conform their AI systems to meet regulatory expectations but also engage in ongoing dialogues with insurance providers to ensure their coverage is both adequate and relevant. As AI technology continues to evolve and permeate more aspects of business operations, insurance products that protect against AI-related risks will also need to evolve as well. Companies that anticipate these changes and prepare accordingly will be best positioned to leverage AI's benefits while mitigating its risks.

Q4 What are the potential legal exposures for businesses under the new legislation, and how can they mitigate these risks?

A Beyond regulatory exposure, the proposed legislation's reach extends to enabling individuals affected by contraventions to initiate legal action. This emboldens not just individual claims but also sets the stage for potential class-action suits, thereby amplifying the risk of potential significant financial repercussions for businesses and insurers.

One of the keys to mitigating these risks will be meeting the standard of informed consent. The proposed legislation highlights the importance of obtaining explicit and informed consent for the collection and use of personal data, and that companies must not exceed the purpose and scope of the initial consent. This consent goes hand in hand with the individual's right to data deletion, which must be honored upon request. Together, these measures will help serve as a shield against legal challenges, provided they are meticulously adhered to and documented.

To effectively manage and mitigate these emerging legal exposures, businesses can adopt a multi-faceted strategy: Developing comprehensive privacy policies, conducting regular data protection impact assessments, ensuring transparency in data collection and processing activities, and leveraging a defense in depth cybersecurity strategy. Maintaining these standards will likely involve continuous investment in cybersecurity personnel, tooling and planning as well as regular staff training to ensure a high level of organizational awareness and adherence to privacy standards. It will be important for employees, at all impacted levels from the executive level to the operational staff, to understand the implications of the new legislation and their role in upholding it.

It will be important for employees, at all impacted levels from the executive level to the operational staff, to understand the implications of the new legislation and their role in upholding it.

In response to the anticipated new legislative environment, businesses should also thoroughly review their insurance policies to pinpoint any potential gaps or exclusions and ensure that limits are adequate in the context of their business should they be exposed to a covered cyber event. Engaging in open dialogue with insurance providers is critical to understanding the impact of legislative changes on coverage and determining the need for any additional protections. There is an opportunity to explore customized insurance solutions that are specifically designed to address the unique risks that may emerge from these proposed legislative changes, providing targeted protection where it is most needed.

Q5 What should a compliant framework include?

A

Under the proposed legislation changes, many businesses will need to pivot towards a more sophisticated compliance framework. This will involve an understanding of the legal mandates as well as a proactive approach to implementing them effectively within their organizational structure. Tenets of a strong, compliant framework could include, but are not limited to:

Developing Codes of Practice and Certification Programs

The newly proposed Bill C-27 introduces the innovative concept of "Codes of Practice," empowering private organizations to seek the Privacy Commissioner's approval of their own internal codes of conduct and certification programs surrounding privacy protection. These programs, once approved by the Privacy Commissioner, will define the organization's legal compliance obligations. This autonomy allows businesses to tailor their privacy practices in a way that aligns with both the regulatory framework and their unique operational needs.

Conducting Thorough Operational Risk Assessments

Central to the compliance process is a thorough assessment of the types and nature of data handled by the organization. Understanding the specifics of data collection, storage, usage and sharing is vital to tailoring the privacy framework to the organization's operational model. This assessment should inform all aspects of the privacy strategy, ensuring that it addresses the unique risks and data handling requirements of the business.

Tailoring Privacy Frameworks for Consumer and Vendor Data

The nature of the data subjects—be they consumers, vendors or business partners—should guide the development of the privacy framework. Organizations need to consider how the data they collect from different entities impacts their compliance strategy, especially in terms of consent acquisition and data processing transparency.

Reinforcing Data Deletion Processes

In response to the new legislation, organizations must establish efficient processes for the deletion of personal data. This involves collaboration with IT departments to create systems capable of handling deletion requests promptly and effectively, ensuring compliance with the right of individuals to have their data removed.

Enhancing Employee Training and Sensitivity Awareness

Continuous education and training of all impacted employees on the nuances of data collection and retention are crucial. This training, integral to both new hire onboarding and periodic refreshing, ensures that every impacted team member is aware of the evolving privacy landscape and their role in maintaining compliance. Special emphasis should be placed on understanding and handling sensitive information, particularly data related to minors or other vulnerable groups.

Utilizing External Expertise

To successfully navigate these proposed changes, businesses can seek guidance and support from external resources including specialized IT vendors to help ensure compliance, and their insurance partners to ensure they are adequately protected in the event of any actual or alleged privacy violation or other cyber breach.

With the proposed Bill C-27 on the horizon, your organization requires a new level of cyber resilience and the type of comprehensive insurance strategies we advocate for at Arch. Visit our website, or contact our dedicated team for personalized assistance with any inquiries.

Q6

What steps should businesses take to help ensure compliance with the proposed legislation and to maintain insurability?

A

To navigate the proposed updates to Canadian privacy legislation, businesses may need to take decisive steps to ensure full compliance and maintain insurability. This proactive approach is about adherence as well as demonstrating to key partners, like insurers, that the business is utilizing the best practices available to mitigate risk based on the proposed legislation; these are the actions businesses should consider prioritizing:

Implementing a privacy management program

Establishing a comprehensive privacy management program involves constructing or refining data protection policies, incident response strategies and consent procedures involving data subjects.

This strategic development should be collaborative, drawing on the expertise of internal risk management teams and input from designated personnel across all departments and potentially third-party vendors, to create a robust framework.

Additionally, attention should be given to data retention and disposal, setting clear protocols to minimize risks associated with data storage and to reduce the likelihood of exposure.

Data should not be kept beyond the timeframe required to fulfill the purpose for which it was originally collected.

Regular audits and cybersecurity updates

Continuous monitoring through regular audits is an important part of identifying and addressing vulnerabilities within cybersecurity protocols.

This vigilance extends across all facets of the organization's digital assets and data-handling practices. Equally important is the enforcement of stringent data management and cybersecurity standards upon third-party partners to control supply chain risks.

Documenting these efforts provides tangible evidence of an organization's commitment to compliance, which is important for both insurers and regulatory bodies.

Employee training and organizational awareness

To maintain compliance, businesses must invest in continuous education programs that impress upon employees the significance of data protection standards.

Keeping abreast of legislative changes and integrating these updates into the company's training regime is necessary, especially with the growing prevalence of AI and the evolution of current cyber threats like phishing.

These procedures can be further enhanced by cultivating an organizational culture of privacy and cybersecurity awareness, empowering employees to understand and fulfill their role in safeguarding data.

All employees should be aware of the organization's privacy policy and their own role in safeguarding private information.

Attention should be given to data retention and disposal, setting clear protocols to minimize risks associated with data storage and to reduce the likelihood of exposure.

Authors

Chris Pitcher
Chris Pitcher is AVP and Head of Cyber for Arch Insurance Canada based out of Toronto, ON. Previously he was an Underwriting Manager within the Professional Liability group in the US where he had a focus on Cyber, Tech, and E&O. He joined Arch Canada after eight years with Arch in New York City and Jersey City, holding positions in claim operations and finance before transitioning to underwriting. He was instrumental in the growth of Cyber for Arch US and brought his technical skillset and solution-oriented mindset to Canada. Chris has a bachelor's degree in finance from Central Connecticut State University (US).

Katherine Solomon
Katherine Solomon B.A., CIP, is the Technical Claims Manager for Arch Insurance Canada based out of Toronto, ON. She has over 15 years of claims handling experience in multi-lines. She manages Arch's cyber claims program, leads a team of examiners, and handles multi-line large or complex claims including coverage matters, Professional Liability, CGL, and Cyber.

Katherine is a graduate of the University of Toronto, obtaining a Bachelor of Arts degree, Sociology Major. She has also completed her Chartered Insurance Professional Designation and obtained a Certificate in Risk Management from the University of Toronto's School of Continuing Studies. She is currently in the process of completing a Certificate in Information Privacy at York University.

Prior to her 8-year tenure at Arch, Katherine spent one year working at a large insurance property-restoration company, 4 years as an examiner with a large Property and Casualty insurer, and 3 years as a Third-Party Administrator for Lloyd's of London syndicates.

Arch Insurance

Arch Insurance North America is part of a global insurer offering superior coverage and service. We participate in specialty lines where the talent and knowledge of our employees are a competitive differentiator. We serve North America from offices in the United States and Canada, providing superb coverage and claims handling through careful and diligent underwriting of risks and business-friendly solutions. With over 20 years of operating history and strong financial ratings, our track record remains solid. In Canada, our insurance policies are issued by Arch Insurance Canada Ltd.

Pursuing Better Together®

archinsurance.com