Law 25 Survey Report:

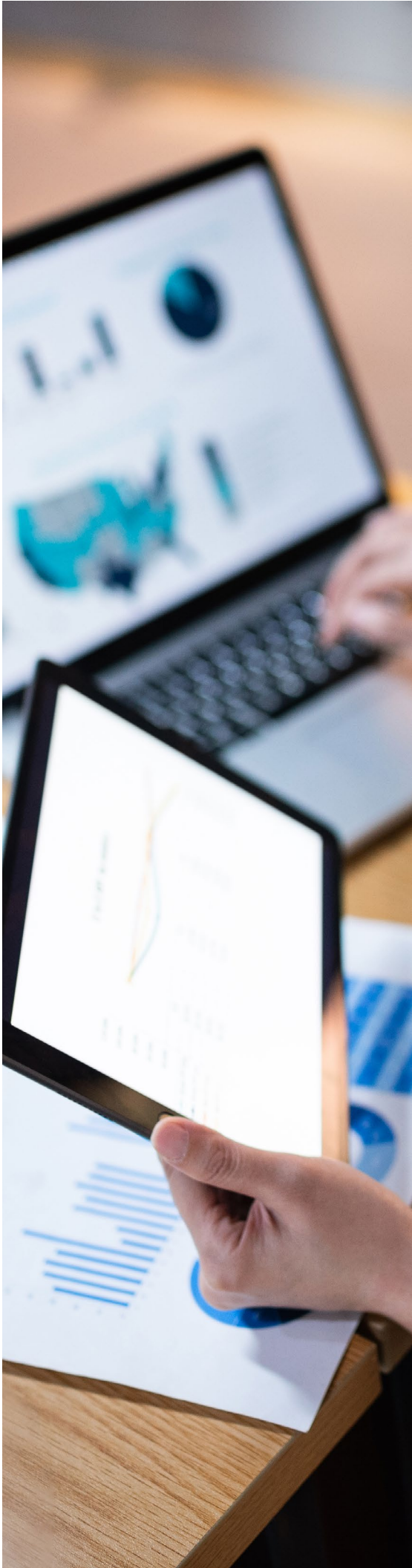
Are organizations ready for Québec's new privacy legislation?

August 2023

GOWLING WLG

iab. canada

Contents

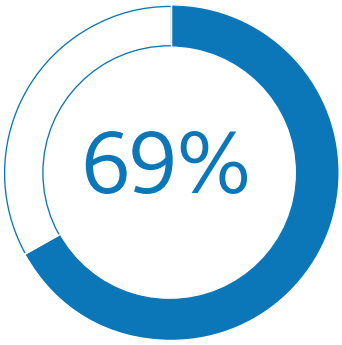


Executive Summary

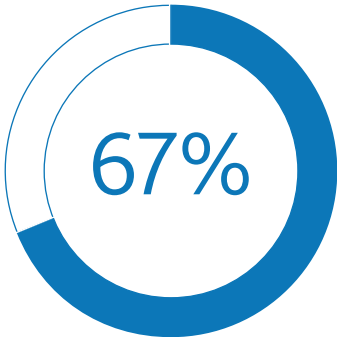
Concern, confusion and lack of clarity remain around Québec's new privacy legislation

The key provisions of Law 25, Québec's new privacy legislation, are scheduled to come into force in September 2023. Despite the fast-approaching deadline, many organizations – both inside and outside of Québec – remain concerned and unclear about many significant aspects of this new law.

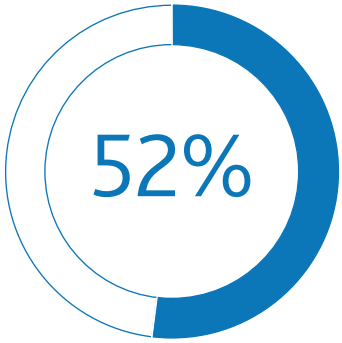
In order to understand in detail how industry is feeling in the face of Canada's toughest privacy regime to date, Gowling WLG and IAB Canada recently surveyed over 100 organizations across various business sectors. The results revealed significant reservations and concern with respect to Law 25. Of the organizations surveyed:



expressed **a need for greater clarity** around Law 25's practical requirements



reported **concern about the risk of penalties and sanctions** against their organizations for non-compliance with Law 25



indicated that they **lacked sufficient resources** within their organization to implement Law 25's requirements

Other concerns highlighted in the survey relate specifically to requirements governing data transfers and consent, as well as the implications of Law 25's sweeping "privacy by default" mandate.

"Despite Law 25 having come a long way since its introduction under Bill 64, unresolved questions of interpretation and implementation spell a challenging rollout of the legislation in September," said Antoine Guilmain, Co-Leader of Gowling WLG's national Cyber Security and Data Protection Group.

"With the survey findings top of mind – and as we await further guidance from the Commission d'accès à l'information du Québec ¬– our first priority is to help clients understand precisely how Law 25 applies to them and, from that understanding, develop practical, cost-effective strategies for compliance."

"The results of this survey indicate a clear sense of urgency to implement appropriate and proven frameworks that will enable the industry to strike a balance between innovation in the important and growing Canadian digital advertising sector, with the protection of citizen rights to privacy," said Sonia Carreno, President of IAB Canada. "We are working with our members to help those in the digital advertising ecosystem comply with the complex requirements of this new law and the TCF Canada framework serves as an effective tool to provide enhanced transparency, meaningful consent and demonstrable accountability."

Background

Québec's Law 25 (*An Act to modernize legislative provisions as regards the protection of personal information)* is the most significant privacy legislative development in Canada in decades. The vast majority of the amendments enacted by Law 25 will come into force on September 22, 2023.

For organizations operating in Québec – or that are collecting, using, or disclosing personal information of individuals located in the province – these amendments will require significant changes to privacy compliance frameworks and the way in which business is currently being conducted.

With a view to better understanding the most pressing concerns businesses have with respect to Law 25, as well as to assess their level of preparedness, Gowling WLG and IAB Canada conducted a 40-question survey. A diverse range of organizations were invited to participate, including 10 industry associations, which together represented a variety of sectors, sizes, industries and degree of privacy sophistication. Responses were received from more than 100 organizations, headquartered both inside and outside of Canada.[1]

In many cases, the survey was distributed to known individual contacts – primarily those responsible for privacy compliance within their respective organizations – although the survey responses themselves were anonymous. The survey was also distributed to members of both national and Québec-based trade associations in the advertising, retail, banking, automotive, insurance, and finance industries.

The survey was open for responses from June 6, 2023 until June 30, 2023. This period overlapped with the consultation period for the draft consent guidelines published by Québec's Commission d'Accès à l'Information (CAI) between May 16, 2023 and June 25, 2023.

[1]All questions in the survey were optional to complete. Not all organizations surveyed responded to all questions. Unless otherwise stated, the percentages reported below were calculated based on the total number of responses received for each question, rather than the total amount of survey respondents. The sample sizes for each question ranged from 87 to 46.

Key Findings

A. Demographics: Profile of Organizations Interested in Law 25

The majority of organizations that responded to the survey had significant operations in Québec, with 100 or more employees in the province. However, there were also participants that were not located in Québec, as well as a small subset not currently operating in Canada, speaking to the far-reaching application, implications and interest in this law.

All private sector respondents had an obligation to comply with legislation in jurisdictions other than Québec (such as the Personal Information Protection and Electronic Documents Act (PIPEDA)). **37 per cent** of respondents were required comply with private sector privacy laws in jurisdictions outside of Canada, primarily the EU's General Data Protection Regulation (GDPR) and various US state laws.

The organizations that responded to the survey were generally well established in terms of existing privacy compliance measures. All respondents with more than a single employee had in place at least one or more formalized policies and practices in respect of privacy law compliance

B. Privacy Officers

The survey was completed by one individual per organization, on behalf of their organization. These individuals represented a range of senior job titles, including legal counsel, managers, officers and executive (e.g., CEO, Vice President).

Notably, **54 per cent** of survey respondents served as their organization's dedicated "Privacy Officer," as per the requirements of Law 25, despite only **26 per cent** of respondents actually working in a professional privacy role. This underscores the fact that those chiefly responsible for ensuring their organization complies with Law 25 frequently have significant additional responsibilities.

Juggling these responsibilities can present a serious challenge, particularly considering the obligations Law 25 imposes on Privacy Officers – including consulting on privacy impact assessments and responding to access, rectification and deletion requests. It is not surprising, then, that many organizations' Privacy Officers do not conduct those activities personally, but rather supervise these activities.

The survey findings attest to this:

Less than

1/4

of respondents indicated that their Privacy Officer **currently conducts** all of these obligations **personally**.

30%

said it **would be feasible** for their Privacy Officer to conduct all of the required activities **personally**

71%

indicated it **would be feasible** for their Privacy Officer to **approve** all policies and practices personally, **while supervising** other activities.

These numbers highlight the need for a realistic approach to implementing and enforcing Law 25 – one that accounts for the limitations and daily realities of organizations and their Privacy Officers.

C. Concerns and Uncertainties

Survey respondents were provided with a link to the relevant provisions of Law 25, grouped into the following categories:

- Automated Decision Making (ADM) and Profiling
- Confidentiality Incidents
- Data Transfer
- Privacy by Default
- Privacy Impact Assessments
- Transparency and Consent

Respondents were asked to review the provisions and (1) rate on a scale of 1 to 10 their level of confidence in understanding the provided provisions, with 1 being not at all confident and 10 being highly confident, and (2) identify sources of interpretive uncertainty impacting their confidence rating. For sources of uncertainty, pre-selected options were provided, but respondents were also provided an opportunity to identify further sources of uncertainty in an open field "other" option.

Law 25's "Privacy by Default" provisions were the cause of greatest interpretive uncertainty, according to the survey. **43 per cent** of respondents gave their understanding of those provisions a confidence rating of 5 or below, with a mode of 4. The "Data Transfer" provisions were close behind with **40 per cent** of respondents reporting a confidence rating of 5 or below.

50%

of respondents identified the "Data Transfer" requirements as among the most significant sources of concern for their organization with respect to Law 25.

Law 25's "Transparency and Consent" requirements followed closely behind, having been selected by **48 per cent** of respondents as a source of most significant concern.

Further questions were then posed exploring the root cause of such concerns, including how they could be remedied. **54 per cent** of respondents indicated a need for further interpretive guidance

69%

expressed a need for clarification on the practical requirements of the statute. This was further emphasized in the open field comments provided by respondents.

However, rather than any of the specific requirements of the law, it was the cost of implementing Law 25's requirements that was most frequently identified by respondents as a major source of concern, having been selected by **54 per cent** of respondents.

This indicates that, while organizations are uncertain on how to interpret certain of Law 25's provisions, substantive and practical considerations are a potentially more significant source of concern

Approximately **60 per cent** of respondents ranked their agreement with the following statements at a 5 or below:

- My organization has adequate time to achieve compliance with the new requirements of Law 25 prior to their coming into force.
- My organization has adequate resources to implement required measures and comply with the requirements of Law 25.
- My organization has sufficient personnel to implement required measures and comply with the requirements of Law 25.

52%

of respondents indicated that they lacked sufficient resources within their organization to satisfy Law 25's requirements

Many also said that they could use more time.

Throughout their responses, respondents also expressed concern over the feasibility and cost of satisfying the substantive requirements of the law. Practical concerns included:

- Potential non-alignment with other applicable privacy statutes in other jurisdictions.
- Potential non-feasibility due to the onerous nature of requirements and lack of necessary resources.

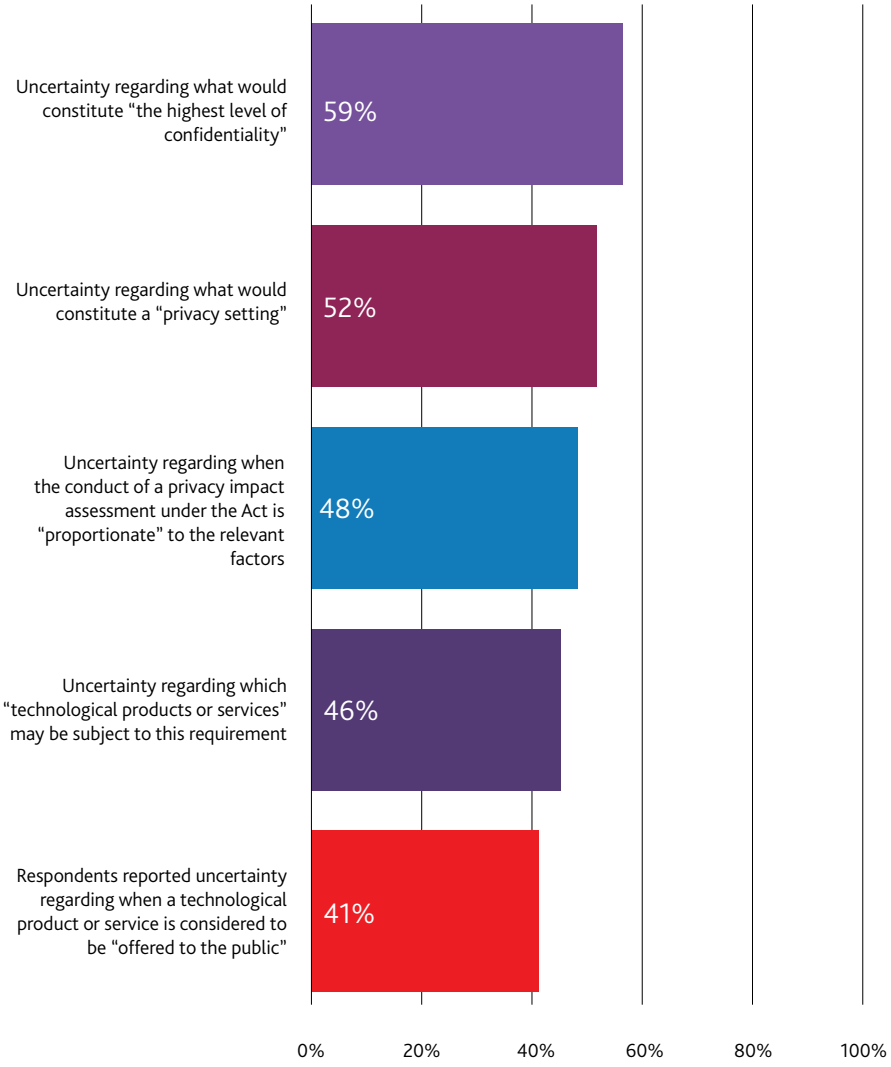
Some comments also indicated that the burden imposed by Law 25, in conjunction with Bill 96 (imposing French language requirements), has resulted in organizations taking steps to leave the Québec market altogether, which could have a significant negative impact on those residing in Québec.

The concerns identified above appear to be exacerbated by significant concerns among organizations regarding penalties and sanctions under Law 25. **67 per cent** of respondents reported concern about the risk of penalties and sanctions against themselves or their organizations for non-compliance with Law 25. Only **15 per cent** of respondents reported that they believed that the penalties and sanctions capable of being imposed under Law 25 are fair.

D. Specific Insights

Specifically, for each of the primary substantive areas of concern for organizations highlighted by the survey, the survey results revealed the following insights regarding the primary sources of interpretive uncertainty.

a. Privacy by Default



b. Data Transfers

Generally, respondents were more confident than not regarding their understanding of the requirements of Law 25 for transfers of data outside of Québec (Section 17). With 1 being not at all confident and 10 being highly confident, **60 per cent** of respondents ranked their confidence in their understanding of the data transfer requirements at 6 or above.

This suggests that the reported high level of concern among organizations regarding Law 25's data transfer requirements relates to issues other than basic understanding.

In particular, **35 per cent** of respondents expressed it would not be feasible for their organization to conduct a data transfer impact assessment (i.e., privacy impact assessment focused on data transfer) for all transfers and all jurisdictions to which data is transferred. Currently, only **19 per cent** conduct the soon-to-be required assessments, although **42 per cent** said it would be feasible to do so.

However, despite respondents' reported level of confidence in interpreting the data transfer requirements, when respondents were asked to identify remaining sources of uncertainty impacting their confidence rating, the following were the most prevalently reported sources:

c. Consent

Respondents reported concerns with Law 25's consent requirements, but the majority of respondents were fairly confident in their understanding of the legislation's consent and transparency provisions. This suggests that the high level of concern over Law 25's consent requirements has mostly to do with uncertainty regarding the practical implementation of the requirements, as opposed to interpretive ambiguity. However, interpretive uncertainties still remain with respect to the consent and transparency provisions.

With 1 being not at all confident and 10 being highly confident,

75%

of respondents rated their confidence in their understanding of the consent and transparency requirements at 6 or above, with a mode of 8.

Of the various Law 25 elements that the survey identified, this resulted in the highest interpretive confidence rating. Such confidence may be, in part, related to the release of the draft consent guidelines from the CAI. It may be related to the fact that

38%

of respondents interpret the consent requirements of Law 25 to be equivalent to those under PIPEDA

Whatever the reason, it places the focus on organizations' practical concerns. In open field comments, organizations expressed that Law 25's express consent requirements will likely case major consent fatigue for individuals. Additionally, the consent and transparency requirements of Law 25 have a high degree of interface with, and are informed by, Law 25's other provisions, including those regarding privacy by default, and those applicable to confidentiality incidents, profiling and cookies. Despite a greater reported level of interpretive confidence in understanding the consent provisions, the higher level of interpretive uncertainty remaining as to these intersecting requirements is a key source of organizational concern. Further practical guidance on how different types of consent should be collected – particularly in the context of profiling, tracking, and cookies – was requested.

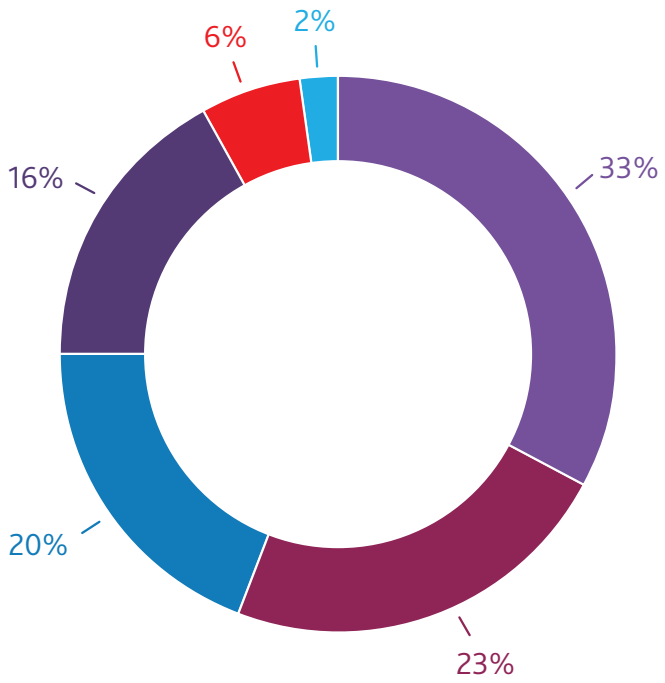
Nonetheless, uncertainties remain with respect to the interpretation of the consent and transparency provisions (Sections 8, 8.3, 12, 14). When respondents were asked to identify remaining sources of uncertainty impacting their confidence rating, the following were the most prevalently reported sources:

Description	Percent
Uncertainty regarding what would constitute "reasonable measures" to limit the risk of someone identifying an individual using de-identified information.	62%
Uncertainty regarding when personal information is "clearly used for the benefit" of a person, such that it may be used for a purpose without consent.	47%
Uncertainty regarding what may constitute a "direct and relevant connection" between purposes, such that a purpose would be considered consistent with the purposes for which it was collected, and therefore used without consent.	43%
Uncertainty regarding each of the following: • What may constitute a "category" of third parties or persons to whom it is necessary to communicate information, which would be necessary to disclose to individuals when information is collected; • When purposes may be considered consistent with the purposes for which information was collected.	42%
Uncertainty regarding each of the following: • What conduct may constitute "commercial or philanthropic prospection," and therefore be exempt from being a "consistent purpose" for which information may be used without consent; • When information may entail a "high level of reasonable expectation of privacy," such that information may be considered "sensitive"; and • When information would be considered "de-identified."	40%
Uncertainty regarding when a use may be "necessary" for a particular purpose (e.g., preventing and detecting fraud, providing or delivering a product or service, research purposes, etc.)	36%
Uncertainty regarding what may be considered "clear and simple language" with respect to requests for consent.	34%
uncertainty regarding when personal information may be considered "sensitive."	32%

Detailed Report

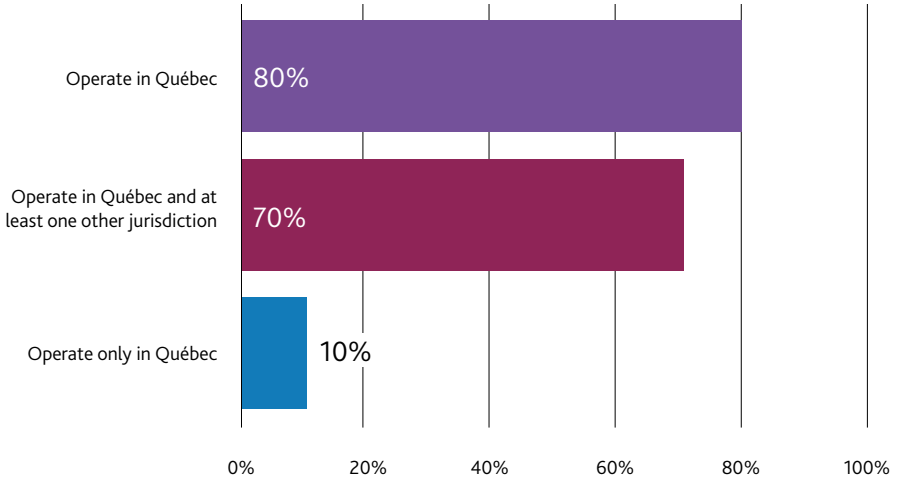
Organizational Demographics

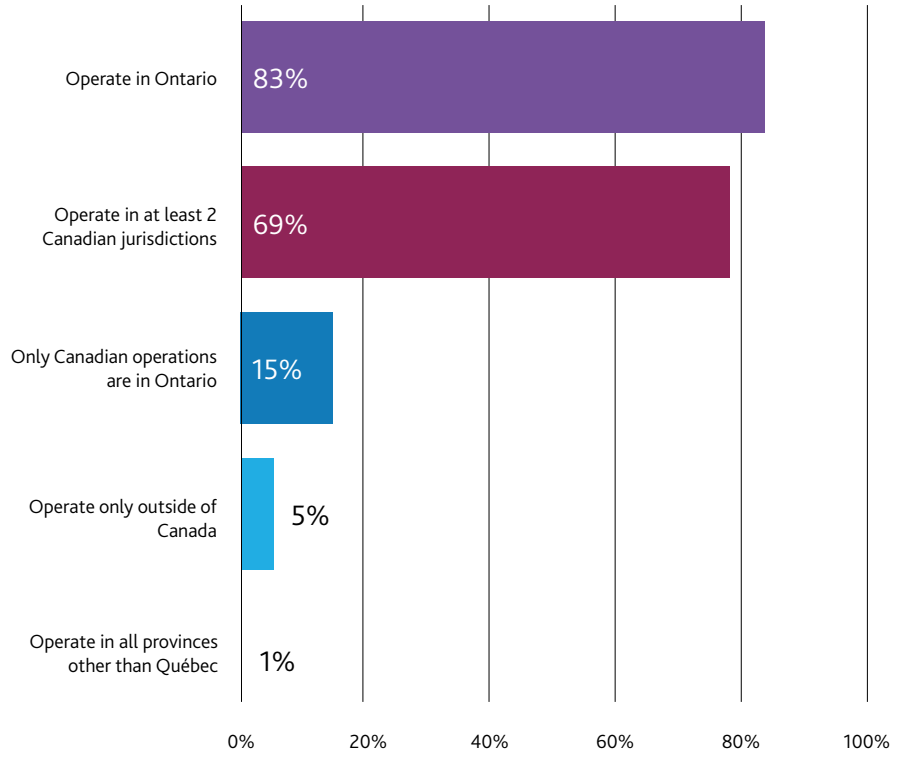
33 per cent (one third) of respondents provide services, and **36 per cent** sell products. One self-identified Crown corporation and 5 non-profit organizations also responded. Not all organizations that responded were directly subject to private sector privacy legislation.



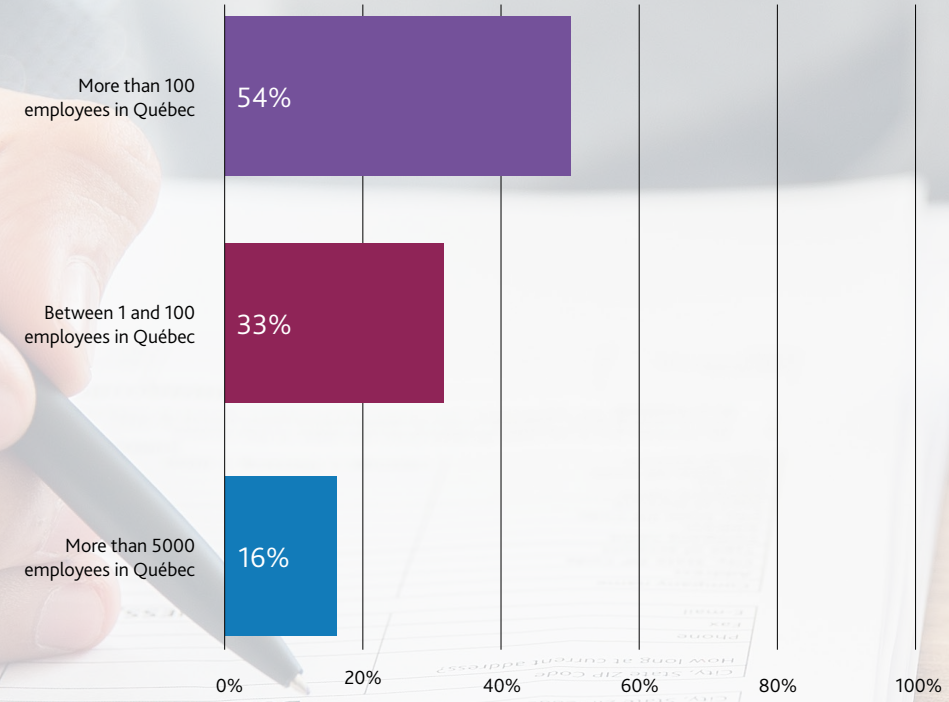
- It sells directly both to consumers and other businesses/organizations – 33%
- It sells directly both to consumers and other businesses/organizations – 23%
- It sells directly to other businesses/organizations – 20%
- It sells directly to individual consumers – 16%
- It is a non-profit organization – 6%
- Other – 2%

Most organizations surveyed currently operate in Québec. However, there were organizations that participated in the survey that were not located in Québec, and a small subset not currently operating in Canada, demonstrating national and international awareness and concern:

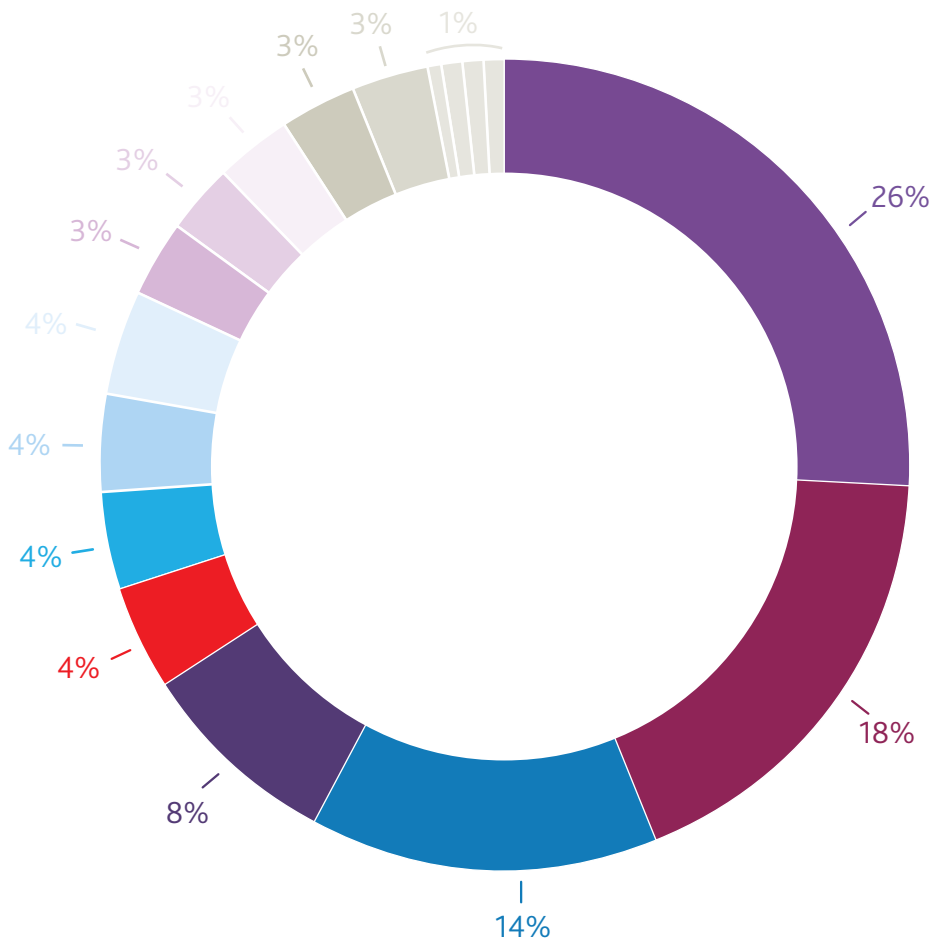




The majority of organizations surveyed had significant operations in Québec



The majority of respondents were in the Advertising or Advertising Technology sectors (**32 per cent**), closely followed by the Finance and Insurance sectors (**26 per cent**).



- Finance and Insurance - 26%
- Advertising/Media - 18%
- Ad Tech - 14%
- Retail Trade - 8%
- Arts, Entertainment and Recreation - 4%
- Health Care and Social Assistance - 4%
- Professional, Scientific and Technical Services - 4%
- Technology, Data and Information Services & Software - 4%
- Agriculture, Forestry, Fishing and Hunting - 3%
- Educational Services - 3%
- Manufacturing - 3%
- Telecommunications - 3%
- Automotive - 3%
- Accommodation and Food Services - 1%
- Construction - 1%
- Other Services (except Public Administration) - 1%
- Transportation and Warehousing- 1%

Privacy Officer

The survey was completed by one individual on behalf of their organization. The individuals that completed the survey held a range of roles in their organization:

54%

of the individuals responding to the survey were their organization's "Privacy Officer" as defined under Law 25 ("person in charge of the protection of personal information").

26%

of responding individuals hold a dedicated privacy officer role.

This indicates that individuals responsible for Law 25 compliance frequently have additional responsibilities, and often significant additional responsibilities, to their privacy compliance role

Law 25 imposes several obligations on Privacy Officers, such as conducting privacy impact assessments and responding to access, rectification, and or deletion requests.

13%

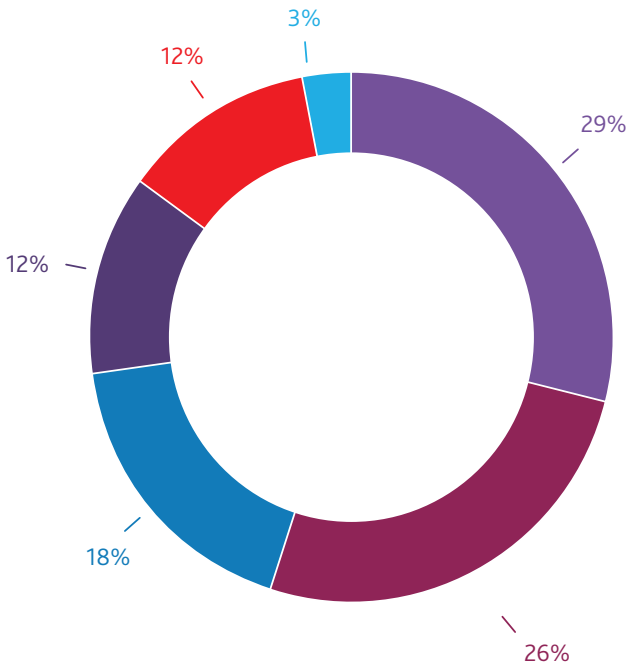
of respondents indicated that their Privacy Officer currently conducts all obligations personally, as opposed to supervising those activities.

30%

said it would be feasible for their Privacy Officer to conduct all of the required activities personally,

71%

indicated it would be feasible for their Privacy Officer to approve all policies and practices personally, while supervising other activities.



- 29% were legal counsel
- 26% held the role of privacy analyst, officer or coordinator
- 18% held the role of vice president
- 12% held the role of owner, president or CEO
- 12% held the role of general or other manager (i.e., HR, operations, product manager)
- 3% held other officer roles (compliance officer, chief information security officer)

Privacy Compliance Obligations Pre-Law 25

Responses were received from several public sector organizations who indicated that they were not required to comply with private-sector privacy laws. All private sector respondents indicated an obligation to comply with legislation in place in jurisdictions other than Québec.

86%

of respondents indicated that they are required to comply with PIPEDA.

27%

of respondents indicated an obligation to comply with health information laws that have been deemed substantially similar to PIPEDA.

37%

of respondents indicated that they are required to comply with private sector privacy laws in place in jurisdictions outside of Canada, primarily EU GDPR, and various US state laws.

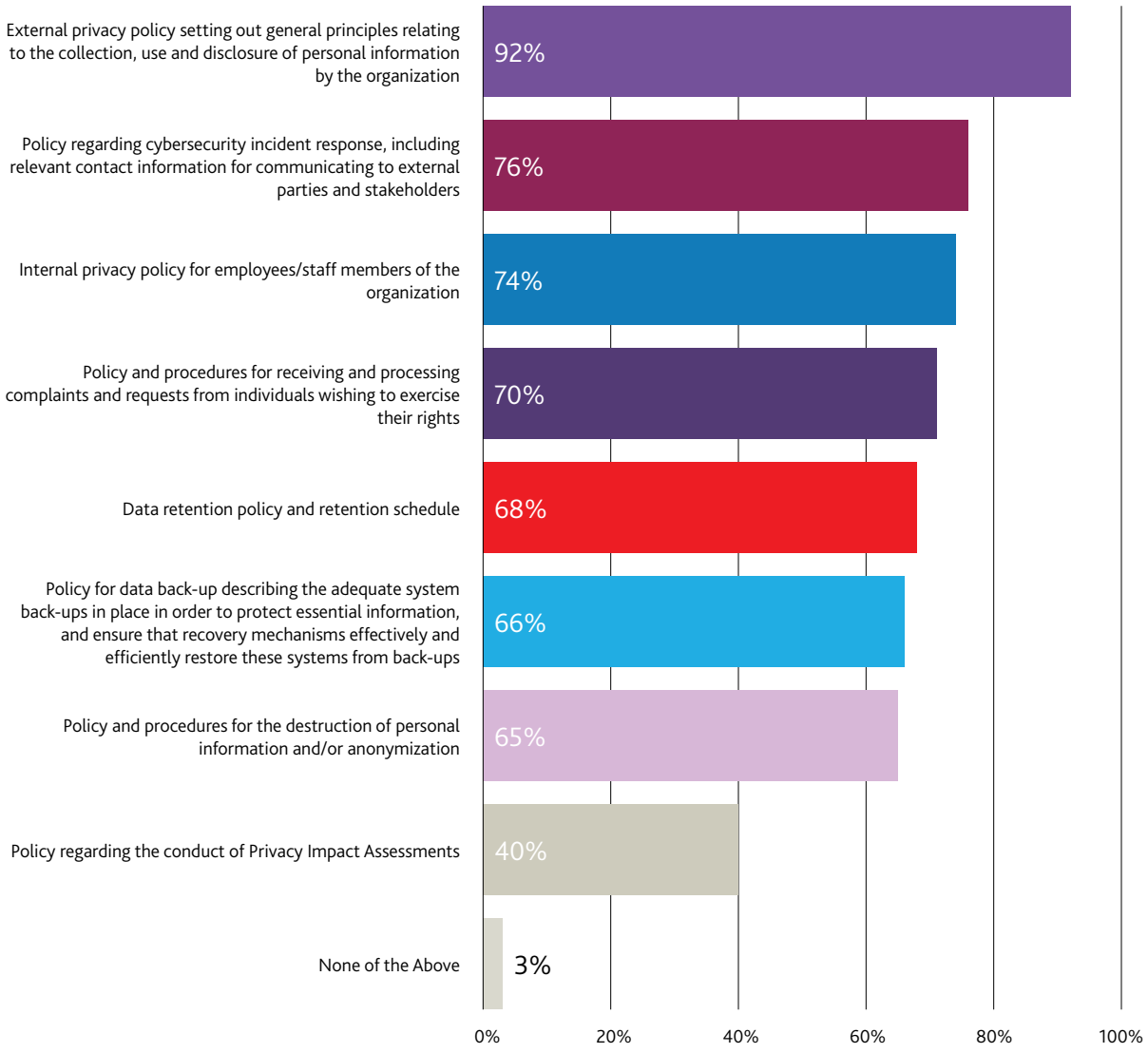
Prior to Law 25, which of the following policies did your organization have in place, either independently or as part of one or more larger policies

Surveyed organizations were generally fairly sophisticated in terms of existing privacy compliance measures. All respondents with more than a single employee had in place at least one or more existing formalized policies and practices in respect of privacy law compliance.

92%

of respondents had in place an external privacy policy.

The same percentage had in place policies regarding at least two distinct data protection elements (i.e., collection, use and disclosure, cyber security incident response, and/or individual correction or complaint response).



Awareness

There was a high level of awareness regarding Law 25 and its requirements among surveyed organizations. With 1 being strong disagreement, and 10 being strong agreement as to their level of awareness:

81%

of respondents rated their awareness of the new privacy rights that Law 25 will implement at between 6-10.

75%

of respondents rated their awareness of when each of the requirements of Law 25 come into force, and awareness of the penalties and sanctions that may be imposed under Law 25 at between 6-10.

Law 25 Readiness & Resources

Organizations are generally confident in their ability to comply with the requirements of Law 25; however, they do not agree that they have sufficient resources and personnel to do so in the time that has been provided.

With 10 being strong agreement and 1 being strong disagreement, **70 per cent** of respondents ranked their agreement with the statement "I am confident in my organization's ability to comply with the requirements of Law 25" at a 6 or above, with a mode of 8.

60 per cent of respondents ranked their agreement with the following statements at a 5 or below:

"My organization has adequate time to achieve compliance with the new requirements of Law 25 prior to their coming into force."

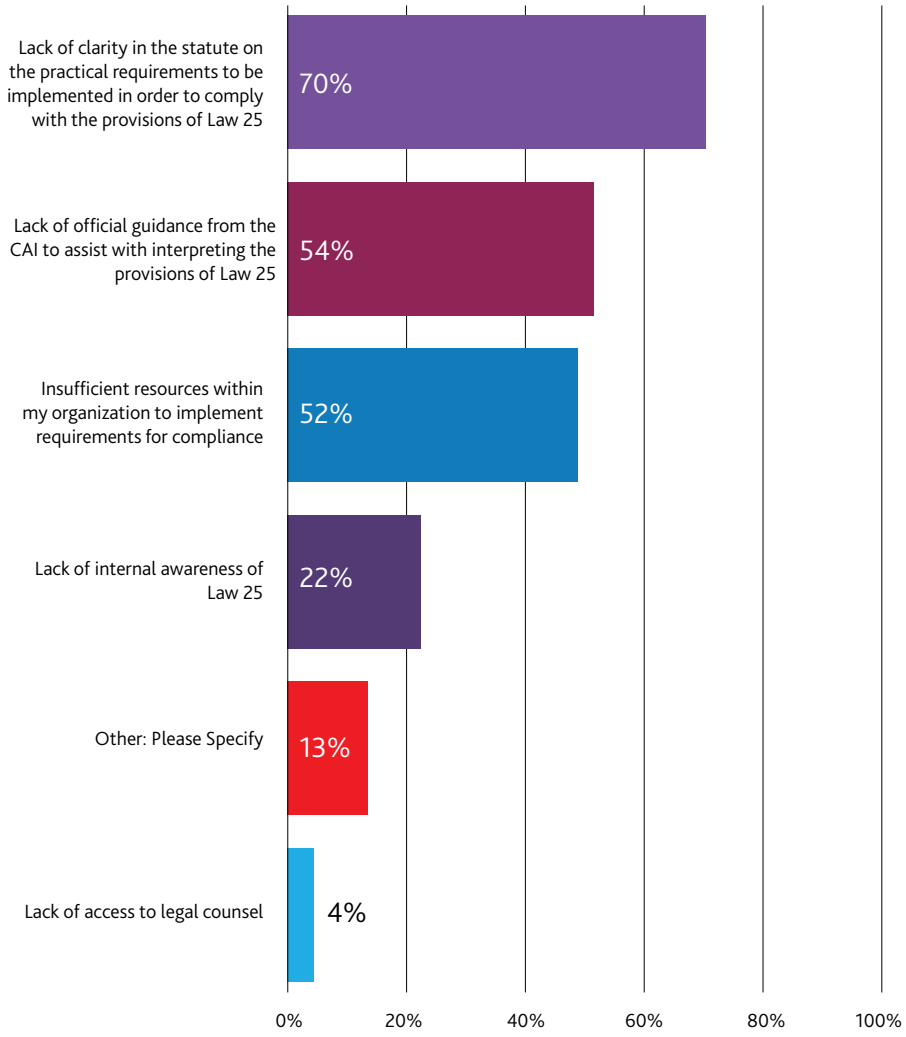
"My organization has adequate resources to implement required measures and comply with the requirements of Law 25."

"My organization has sufficient personnel to implement required measures and comply with the requirements of Law 25."

While many organizations have a plan in place to achieve compliance prior to September 22, 2023, this is not the case across the board:

61 per cent of organizations surveyed have a plan in place to achieve compliance with all requirements of Law 25 prior to their coming into force.

A majority of surveyed organizations (**70 per cent**) indicated that, to the extent that they are not yet compliant with all requirements of Law 25, this is because of a lack of clarity in the statute on the practical requirements to be implemented in order to comply with the provisions of Law 25. **More than 50 per cent** of respondents also attribute it to a lack of official guidance to assist with interpretation, and to insufficient resources.

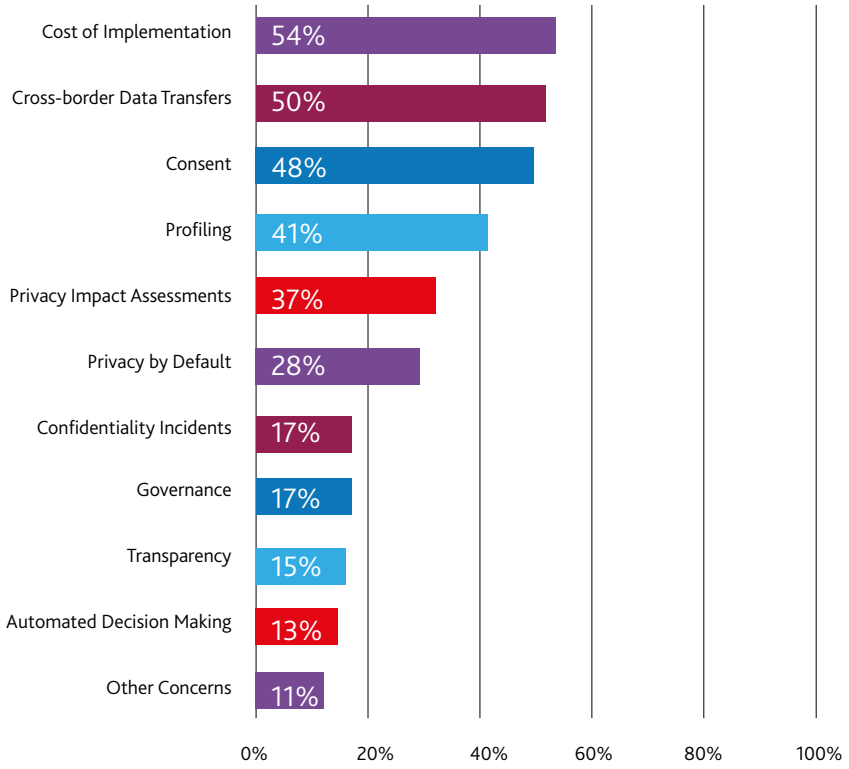


The primary concerns of organizations regarding the requirements of Law 25 were:

- **Costs of Implementation (selected by 54 per cent of respondents)**
- **Cross Border Data Transfers (selected by 50 per cent of respondents)**
- **Consent (selected by 48 per cent of respondents)**

Note that the timing for this survey aligned with the consultation period for the consent guidelines conducted by the CAI.

Costs of implementation and the requirements in the law regarding cross-border data transfers are the clear frontrunners for areas of most significant concern for organizations with respect to Law 25, having been selected by **54 per cent** and **50 per cent** of respondents respectively. Consent is close behind, having been selected by **48 per cent** of respondents as an area of most significant concern.



When asked to select which additional measures or resources would be most helpful in increasing organizational confidence regarding compliance with Law 25, an extension of the period prior to coming into force of the new provisions was the clear frontrunner. It was selected by **52 per cent** of respondents. An extension of the period prior to coming into force was preferred over an enforcement grace period following September 22, 2023 during which penalties and sanctions would not be imposed. This was selected by only **9 per cent** of respondents as most helpful for their organization.

20 per cent of respondents indicated that additional guidance from the CAI on the practical steps to be taken by organizations in order to comply with Law 25's novel requirements would be most helpful for their organization.

Finally, **17 per cent** of respondents indicated that additional guidance from the CAI on the appropriate interpretation of the language of Law 25 would be most helpful for their organization.

Respondents were also provided with an opportunity to identify further resources that would be helpful, beyond that which would be most helpful. Several respondents indicated that, in addition to their primary selection, delayed enforcement would be helpful. Other respondents specifically identified:

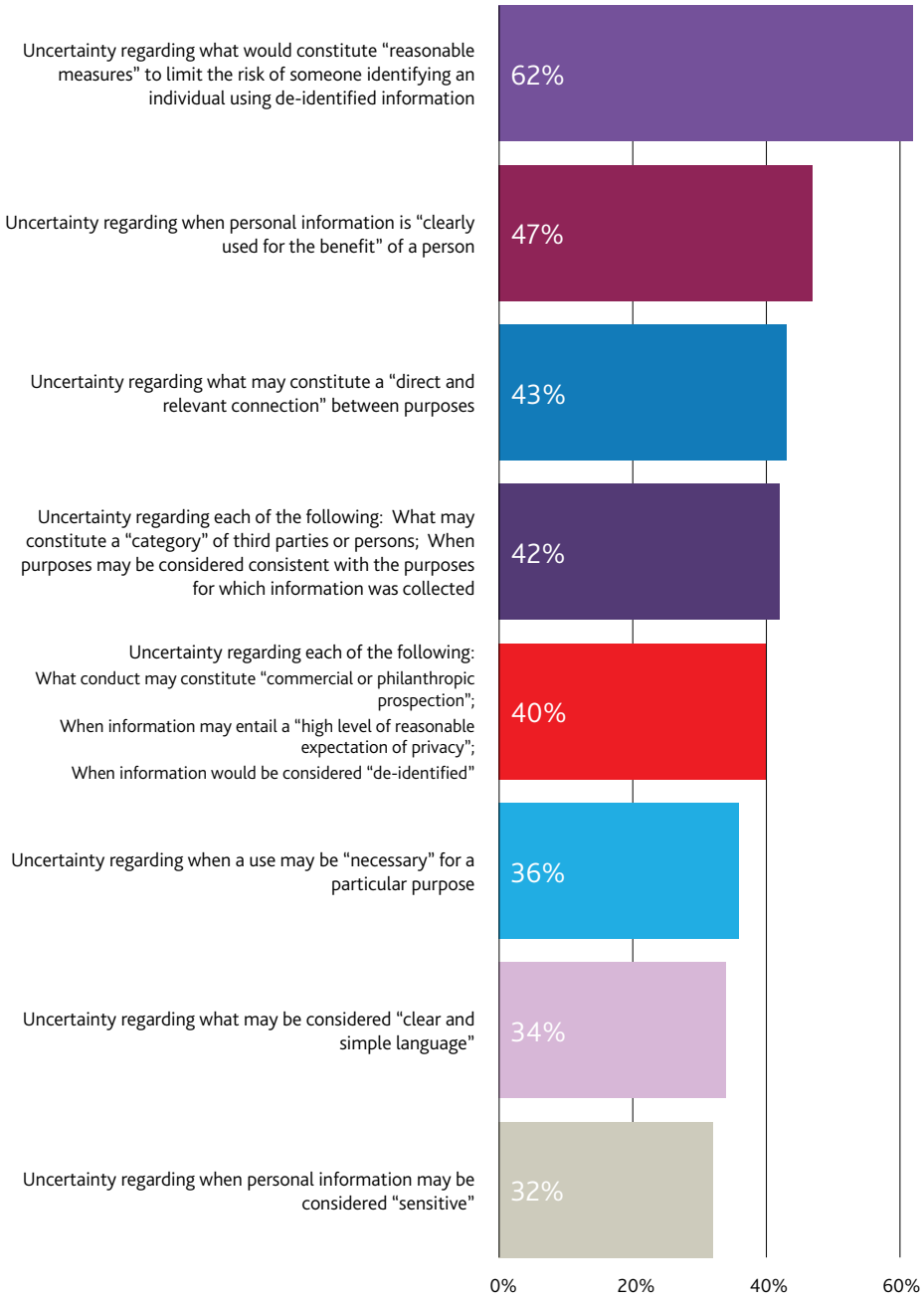
- Guidance on complying with Law 25 alongside other privacy legislation in other jurisdictions around the world,
- Guidance on application of Law 25 to organizations outside of Québec whose services may be accessed by people in Québec, despite them not being directly targeted,
- An updated privacy impact assessment template.

Consent & Transparency

Despite reporting concern regarding the consent requirements, generally, respondents were fairly confident regarding their understanding of the consent and transparency provisions of Law 25.

With 1 being not at all confident and 10 being highly confident, **75 per cent of respondents** ranked their confidence in their understanding of the consent and transparency requirements at 6 or above, with a mode of 8.

The following were the most prevalently reported sources of uncertainty:



Other reported sources of uncertainty included: how different types of consent should be collected online (e.g., on a website); what would qualify as being "presented separately from any other information provided to the person concerned"; consent requirements for profiling; application of requirements specifically to cookies; the distinction between "implied consent" and "express consent."

There was a significant amount of reported uncertainty among organizations regarding the distinction between the relative requirements for meaningful consent under Law 25 and under PIPEDA.

25 per cent of respondents indicated that they were unsure whether the requirements for meaningful consent were the same under Law 25 as under PIPEDA. The remaining respondents were split near evenly between interpreting the requirements as being the same (**38 per cent**) and being different (**37 per cent**).

Automated Decision Making & Profiling

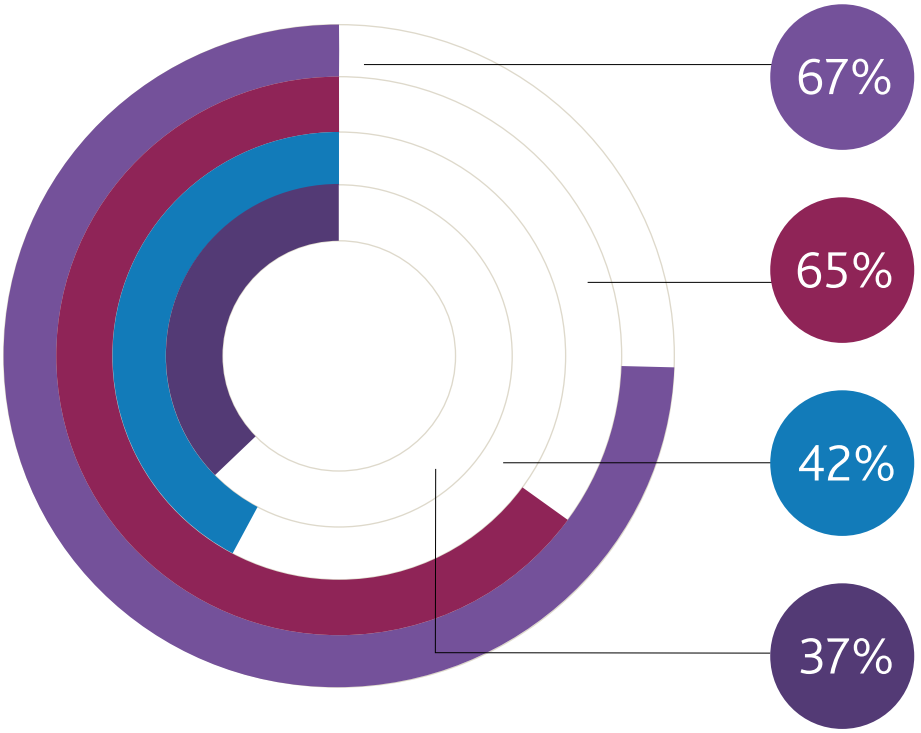
Generally, respondents were more confident than not regarding their understanding of the automated decision making and profiling requirements of Law 25.

With 1 being not at all confident and 10 being highly confident

62 per cent of respondents ranked their confidence in their understanding of the automated decision making and profiling requirements at 6 or above.

Of the respondents that indicated they used automated decision making processes, only **17 per cent** stated that it would be feasible for their organization to notify individuals of all decisions made exclusively using automated processing. By contrast, **69 per cent** indicated it would be feasible to notify individuals of those decisions based exclusively on automated processing that would have a material, direct or significant impact on an individual or their rights. **9 per cent** indicated neither would be feasible, and **6 per cent** indicated they were uncertain as a result of a lack of clarity regarding the requirements of the law.

The following were the most prevalently reported sources of uncertainty



Uncertainty regarding the following:
- What may constitute "profiling"
- What "functions" may allow a person to be identified, located or profiled

Uncertainty regarding what the relevant "factors" or "parameters" are that would be required to be disclosed to a person concerned

Uncertainty regarding what may be considered "automated processing" of personal information

Uncertainty regarding when a decision may be "exclusively" based on automated processing

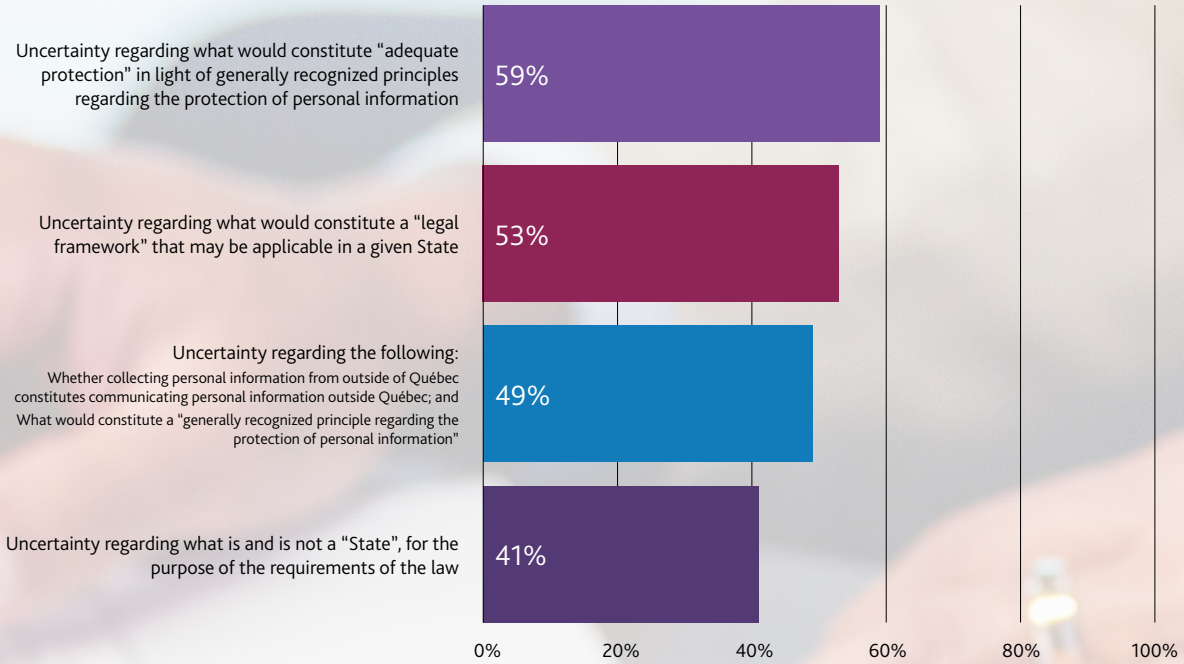
The application of the profiling requirements to the use of cookies, in light of their exclusion from the privacy by design requirements of Law 25 was also raised as a concern.

Data Transfers

Generally, respondents were more confident than not regarding their understanding of the requirements of Law 25 for transfers of data outside of Québec.

With 1 being not at all confident and 10 being highly confident, **60 per cent** of respondents ranked their confidence in their understanding of the data transfer requirements at 6 or above.

The following were the most prevalently reported sources of uncertainty:

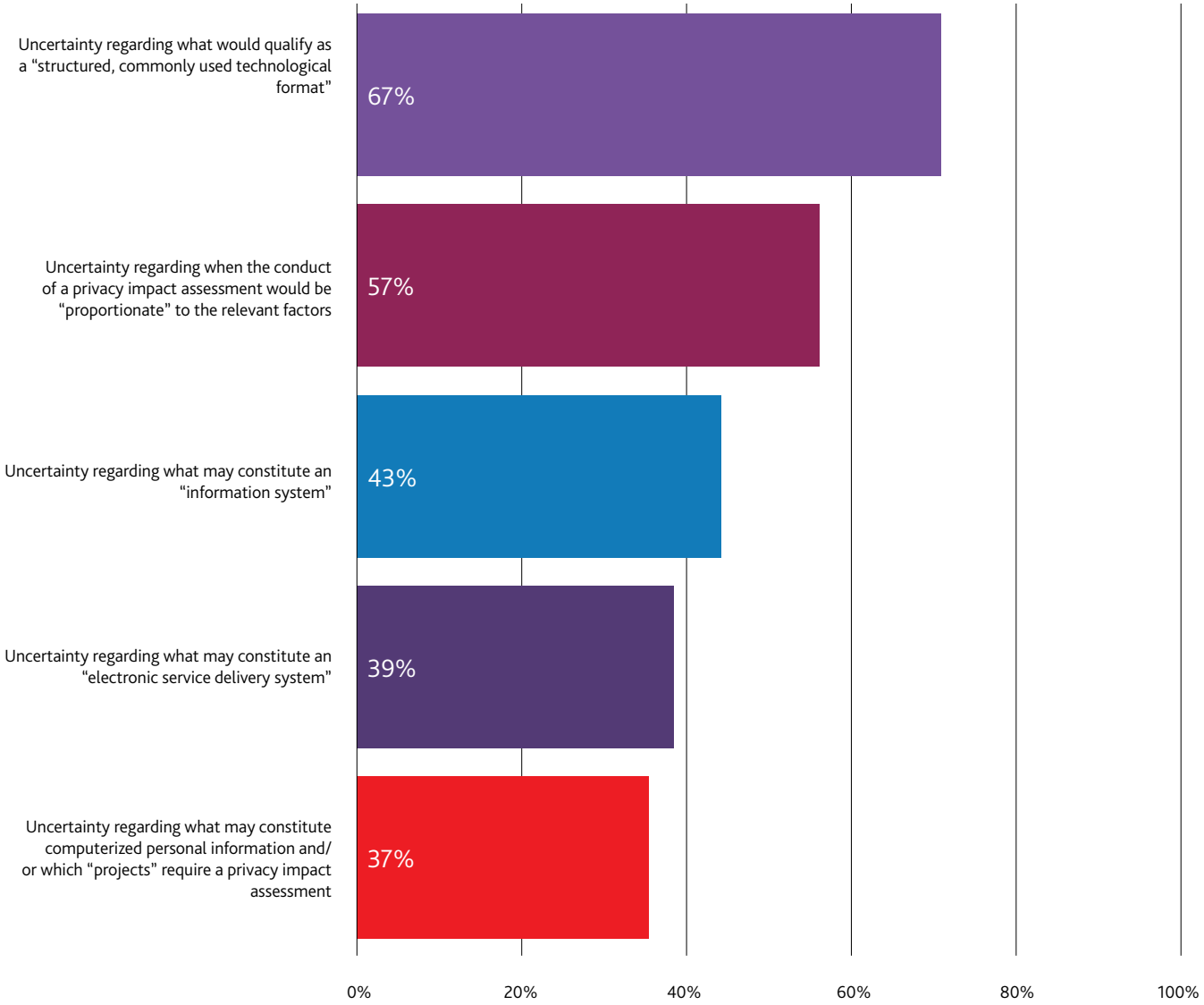


Privacy Impact Assessments

Generally, respondents were fairly confident regarding their understanding of the privacy impact assessment provisions of Law 25.

With 1 being not at all confident and 10 being highly confident, **68 per cent** of respondents ranked their confidence in their understanding of the privacy impact assessment requirements at 6 or above.

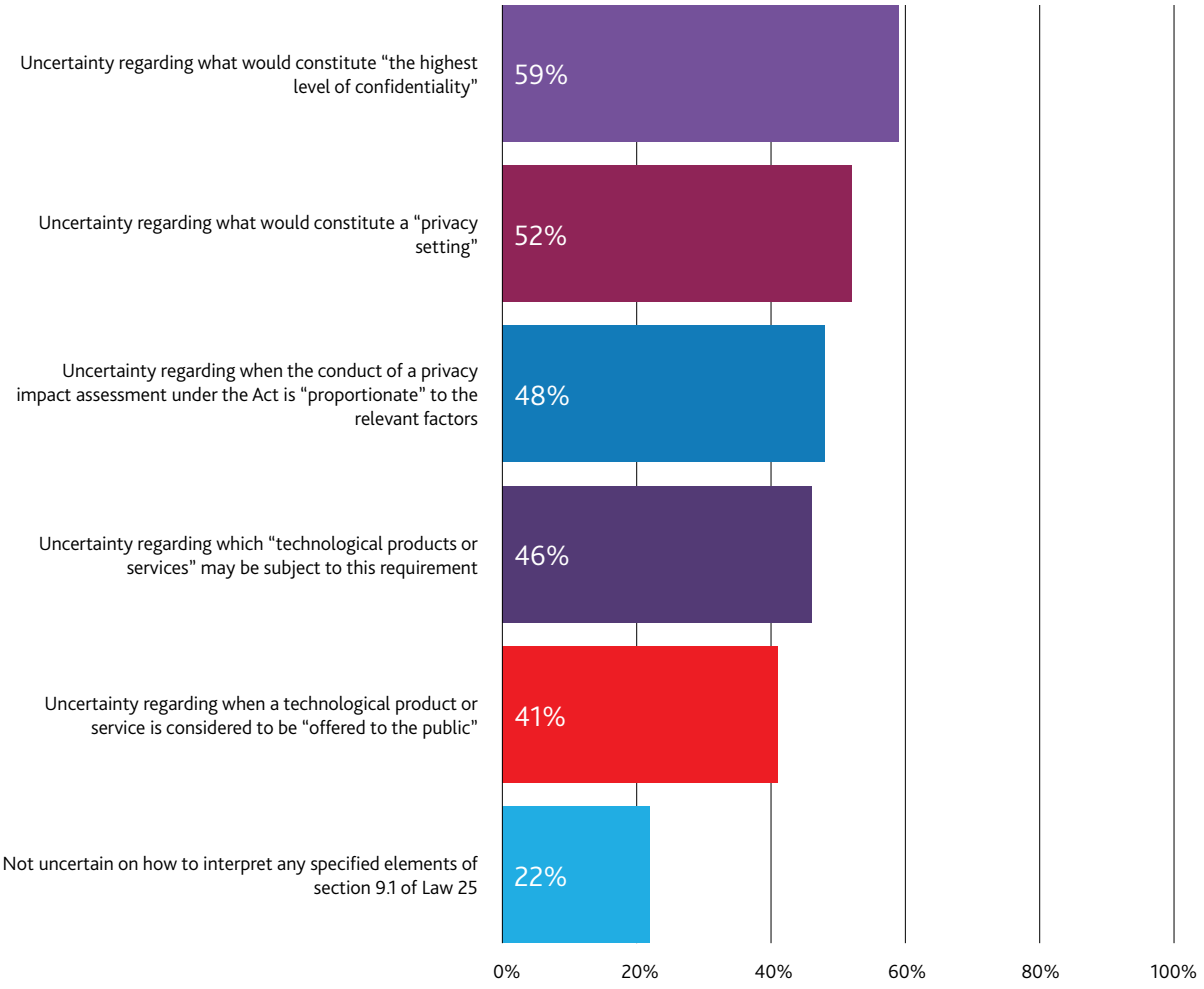
The following were the most prevalently reported sources of uncertainty



Privacy by Default

Respondents were divided regarding their confidence in their understanding of the privacy by default requirements of Law 25.

With 1 being not at all confident and 10 being highly confident, **57 per cent** of respondents ranked their confidence in their understanding of the privacy by default requirements at 6 or above.



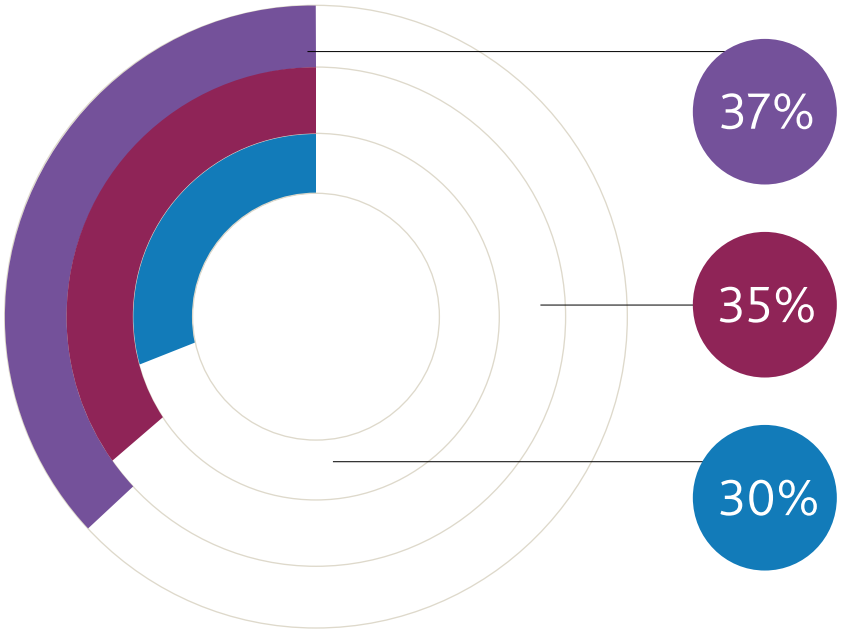
More than **50 per cent** of respondents were not confident that implementing the privacy by default requirements would be feasible for their organization.

30 per cent of respondents were unsure whether it would be feasible for their organization to make the highest level of confidentiality the default for all privacy settings. **22 per cent** reported that it would not be feasible.

Confidentiality Incidents

Generally, respondents were fairly confident regarding their understanding of the confidentiality incident reporting requirements of Law 25. These requirements came into force in September 2022, likely resulting in increased familiarity with the requirements.

With 1 being not at all confident and 10 being highly confident, **72 per cent** of respondents ranked their confidence in their understanding of the confidentiality incident reporting requirements at 6 or above.



Not uncertain on how to interpret any specified elements of section 3.5 or 3.8 of Law 25. The same percentage selected the following as areas of uncertainty:

- When an incident presents a "risk of serious injury"
- What types of persons or bodies could reduce the risk of serious injury

Uncertainty regarding what would constitute reasonable measures to reduce the risk of injury

Uncertainty regarding what would constitute reasonable measures to prevent new confidentiality incidents "of the same nature"

Several respondents also indicated uncertainty regarding when use of personal information without authorization would constitute a confidentiality incident, and referred to example 16.2 of the CAI's draft consent guidelines as adding further ambiguity.

Respondents were fairly uncertain regarding the distinction between reporting standards under Law 25, where an incident presents a risk of serious injury, and under PIPEDA, were an incident presents a real risk of serious harm. **52 per cent** of respondents rated their confidence in their understanding at a 5 or below, with a mode of 5.

70%

of respondents reported that it was a source of concern that the names of organizations that report confidentiality incidents to the CAI may be published.

Penalties and Sanctions

15%

of respondents reported that they believed that the penalties and sanctions capable of being imposed under Law 25 are fair.

67%

of respondents reported concern about the risk of penalties and sanctions against themselves or their organizations for non-compliance with Law 25.

61%

of respondents reported a lack of confidence in their understanding of the circumstances in which monetary administrative penalties may be imposed under Law 25, as opposed to circumstances where penal proceedings may be brought. With 1 being not at all confident to 10 being highly confident, only 39 per cent reported a confidence level of 6 or higher.

Additional Comments

Finally, respondents were provided with an opportunity to provide additional comments regarding Law 25 and their organization's concerns. In addition to repeating requests for guidance in each of the above identified areas, organizations expressed that:

- **The lack of guidance for Law 25 in advance of the coming into force of the provisions is a serious problem and unreasonable.**
- **That the express consent requirements of Law 25 will likely cause major consent fatigue for individuals.**
- **Law 25 presents a very heavy compliance burden.**

Organizations also expressed a desire for Québec to align its framework with the future Federal framework to be adopted (ie. Bill C-27).

About Us

About Gowling WLG

Gowling WLG provides clients with world-class legal acumen and multi-jurisdictional support in key global sectors, including technology, manufacturing, banking and finance, capital markets, infrastructure, and the life sciences. We are also home to one of the world's premier intellectual property practices, and a full suite of business law and dispute resolution services.

With more than 1,500 legal professionals around the world, we provide our clients with in-depth knowledge in key global sectors and a suite of legal services at home and abroad.

We see the world through our clients' eyes, and collaborate across countries, offices, service areas and sectors to help them succeed, no matter how challenging the circumstances. Our on-the-ground presence in Canada, the UK, Continental Europe, the Middle East and Asia means that we are able to provide our clients with the full-service legal support you need to succeed – at home and around the world. Learn more »

National Privacy and Cyber Security Group

Comprised of leading privacy and data protection professionals, our team deploys our vast experience to create effective and valuable solutions for our clients. We provide practical advice and resources to help clients assess legal and strategic business implications across a broad spectrum of privacy and data protection matters, including Law 25. Our team of dedicated Gowling WLG professionals includes those who have held positions as senior political staff, held senior government positions or have contributed to the development of policy, legislative and regulatory regimes. This experiences helps us ensure that our clients can engage fully in the policy conversation.

Let us help you stay one step ahead in this evolving privacy law landscape. Explore our resources or contact a member of our team to begin a conversation.

About IAB Canada

The Interactive Advertising Bureau of Canada (IAB Canada) is the national voice and thought leader of the Canadian interactive marketing and advertising industry. We are the only trade association exclusively dedicated to the development and promotion of the digital marketing and advertising sector in Canada. As a not-for-profit association, IAB Canada represents over 250 of Canada's most well-known and respected advertisers, ad agencies, media companies, service providers, educational institutions, and government bodies. Our members represent a diverse range of stakeholders in the rapidly growing Canadian digital marketing and advertising sector and include small and medium sized enterprises.

What We Do

As the only organization fully dedicated to the development and promotion of digital/interactive advertising in Canada, IAB Canada works with its members to:

- Conduct original, Canadian digital/interactive research;
- Establish and promote digital/interactive advertising standards & best practices;
- Build human capital, through educational courses, certification, our job board, and other initiatives that help the industry in attracting, training and motivating human resources;
- Act as an advocate for the Canadian digital/interactive advertising industry to the Canadian government; and,
- Organize networking events that enhance communication between members.

IAB Canada & IAB Worldwide

IAB Canada is an independently organized and operated organization, and is neither owned, controlled nor operated by any other Interactive Advertising Bureau, Inc. and all trademarks and names are used under license. IAB Canada and global IABs work together closely on major projects and endeavours, but each country requires individual memberships. For more information visit www.iabcanada.com

Key Contacts

Gowling WLG Team

Antoine Guilmain

Associate Counsel, Co-Lead National Cyber Security and Data Protection Law Group

Montréal

+1 514 392 9521

antoine.guilmain@gowlingwlg.com

Melissa Tehrani

Partner, Lead National Advertising & Product Regulatory Group

Montréal

+1 514 392 9561

melissa.tehrani@gowlingwlg.com

Wendy Wagner

Partner, , Co-Lead National Cyber Security and Data Protection Law Group

Ottawa

+1 613 786 0213

wendy.wagner@gowlingwlg.com

Caitlin Schropp

Associate

Ottawa

+1 613 786 0278

caitlin.schropp@gowlingwlg.com

Marc-Antoine Bigras

Associate

Montréal

+1 514 392 9563

Marc-Antoine.bigras@gowlingwlg.com

Nayla El Zir

Associate

Montréal

+1 514 392 9585

Nayla.ElZir@gowlingwlg.com

Justine Simoneau

Associate

Montréal

+1 514 878 9641

justine.Simoneau@gowlingwlg.com

IAB Canada Team

Sonia Carreno

President, IAB Canada

scarreno@iabcanada.com

Jill Briggs

Head of Policy, IAB Canada

jbriggs@iabcanada.com


GOWLING WLG


iab. canada