



Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada

## **2019-20 Survey of Canadian businesses on privacy-related issues Final report**

**Prepared for the Office of the Privacy Commissioner of Canada**

Supplier Name: Phoenix SPI  
Contract Number: 2R008-190099-001\_CY  
Contract Value: \$74,242.36 (including HST)  
Award Date: 2019-07-30  
Delivery Date: 2020-01-31

Registration Number: POR 037-19

For more information, please contact: [publications@priv.gc.ca](mailto:publications@priv.gc.ca)

Ce rapport est aussi disponible en français.

**Canada** 

## **2019-2020 Survey of Canadian businesses on privacy-related issues**

Final report

Prepared for the Office of the Privacy Commissioner of Canada

Supplier name: Phoenix Strategic Perspectives Inc.

January 2020

This public opinion research report presents the results of a telephone survey conducted by Phoenix SPI on behalf of the Office of the Privacy Commissioner of Canada. The survey was conducted with 1,003 Canadian businesses from November 29 to December 19, 2019.

This publication may be reproduced for non-commercial purposes only. Prior written permission must be obtained from the Office of the Privacy Commissioner of Canada. For more information on this report, please contact the Office of the Privacy Commissioner of Canada at: [publications@priv.gc.ca](mailto:publications@priv.gc.ca) or at:

Office of the Privacy Commissioner of Canada  
30, Victoria Street  
Gatineau, Quebec  
K1A 1H3

Aussi offert en français sous le titre *Sondage de 2019-2020 auprès des entreprises canadiennes concernant les enjeux liés à la protection des renseignements personnels.*

# Table of contents

Executive summary .....	2
Introduction .....	6
Background .....	6
Purpose and research objectives .....	6
Methodology.....	6
Notes to readers.....	7
Detailed findings .....	8
1. Use and storage of customer information .....	8
2. Company privacy practices .....	11
3. Managing privacy risks .....	18
4. Awareness and impact of federal privacy law .....	22
6. Corporate profile.....	28
Appendix .....	29
1. Survey questionnaire .....	29
2. Statement of political neutrality .....	36

# Table of figures

Figure 1: Purpose of customer information collected by companies.....	8
Figure 2: Disclosure, collection, or use of customers' information .....	9
Figure 3: Methods used by companies to store personal information .....	10
Figure 4: Importance companies attribute to protecting customers' privacy.....	11
Figure 5: Importance companies attribute to protecting customers' privacy [over time].....	12
Figure 6: Privacy policies.....	13
Figure 7: Features of privacy policies .....	14
Figure 8: Notifying customers about changes to privacy policies .....	15
Figure 9: Steps taken to inform customers about the company's privacy practices .....	16
Figure 10: Privacy policy practices.....	17
Figure 11: Privacy policy practices [over time].....	17
Figure 12: Corporate policies in place to assess privacy risks .....	18
Figure 13: Proportion of companies that have experienced a privacy breach.....	19
Figure 14: Level of concern about a data breach .....	20
Figure 15: Level of concern about a data breach [over time] .....	21
Figure 16: Companies' awareness of responsibilities under privacy laws.....	22
Figure 17: Companies' awareness of responsibilities under privacy laws [over time].....	23
Figure 18: Compliance with Canada's privacy laws .....	23
Figure 19: Level of difficulty complying with Canada's privacy laws.....	25
Figure 20: Compliance with Canada's privacy laws [over time] .....	26
Figure 21: Awareness of OPC resources .....	27

## Executive summary

The Office of the Privacy Commissioner of Canada (OPC) commissioned Phoenix Strategic Perspectives (Phoenix SPI) to conduct quantitative research with Canadian businesses on privacy-related issues.

### Purpose, objectives and use of findings

To address its information needs, the OPC conducts surveys with businesses every two years to inform and guide outreach efforts. The objectives of this research were to collect data on the type of privacy policies and practices businesses have in place; on businesses' compliance with the law; and on businesses' awareness and approaches to privacy protection. The findings will be used to help the OPC provide guidance to both individuals and organizations on privacy issues; and enhance its outreach efforts with small businesses, which can be an effective way to achieve positive change for privacy protection.

### Methodology

A 13-minute telephone survey was administered to 1,003 companies across Canada between November 29 and December 19, 2019. The target respondents were senior decision makers with responsibility and knowledge of their company's privacy and security practices. Businesses were divided by size for sampling purposes: small (1 to 19 employees); medium (20 to 99 employees); and large (100 employees or more). The results were weighted by size, sector and region using Statistics Canada data to ensure that they reflect the actual distribution of businesses in Canada. Based on a sample of this size, the results can be considered accurate to within  $\pm 3.1\%$ , 19 times out of 20.

### Key findings

- **When it comes to meaningful consent, at least one-third of Canadian businesses incorporate some of the guiding principles in their privacy practices.**
  - Approximately half (51%) of the companies surveyed make their privacy information easily accessible to their customers.
  - Forty-five percent (45%) make it clear to customers whether the collection, use or disclosure of information is a condition of service.
  - About one-third each notify customers when making changes to their company's privacy policy (36%) and obtain consent from customers when making changes to their company's privacy practices (34%).
- **Many companies have a privacy policy in place.**
  - Roughly two-thirds (65%) of companies surveyed have a privacy policy in place.
  - Among the companies that have a privacy policy, many have a policy that explains in plain language how their company collects, uses and discloses customers' information (84%), the purpose for which customers' personal information is being collected (82%), what personal information is being collected (80%), and with which parties the collected personal information will be shared (70%).

- Approximately one-third (36%) of companies that have a privacy policy notify customers when making changes to this policy.
- **Half or more of Canadian businesses have implemented most of the privacy compliance practices measured in the survey.**
  - Sixty-two percent (62%) of companies have designated someone to be responsible for privacy issues and the personal information that their company holds (up from 59% in 2017 and 57% when tracking began in 2011).
  - Six in 10 (60%) companies have procedures in place for responding to customer requests for access to their personal information (up from 47% in 2017).
  - More than half (58%) have procedures in place for dealing with complaints from customers who have concerns about how their information has been handled (up from 51% in 2017 and 48% in 2011 when tracking began).
  - Fifty-five percent (55%) have developed and documented internal policies for staff that address privacy obligations under the law (up from 50% in 2017).
  - Four in 10 (39%) regularly provide staff with privacy training and education.
- **Most companies have not experienced a privacy breach.**
  - More than 9 in 10 (95%) companies have not experienced a privacy breach.
  - Concern about data breaches is polarized. Three in 10 (30%) companies are extremely concerned about a data breach, whereas exactly one-third (33%) are not at all concerned about a data breach.
  - High concern about a data breach has fluctuated over time, from a low of 24% in 2013 to this year's high of 37%.
- **Many companies have a high level of awareness of their responsibilities under Canada's privacy laws.**
  - More than half of business representatives think their company is highly aware of its responsibilities under Canada's privacy laws (scores of 6 or 7 on the 7-point scale), including 40% who say their company is extremely aware of these responsibilities.
  - More than 7 in 10 (77%) companies have taken steps to ensure they comply with Canada's privacy laws. Forty-six percent (46%) of companies that have taken steps to comply say that compliance was moderately easy (scores of 3 to 5 on the 7-point scale), and 37% say compliance was easy (scores of 1 or 2 on the 7-point scale).
  - Slightly more than one-third (36%) of companies are aware that the OPC has information and tools to help companies comply with their privacy obligations. However, nearly two-thirds (63%) are not aware that the OPC has resources available to help companies comply with their privacy obligations.
- **Company size continues to be the strongest predictor of a company's privacy practices.**
  - Large companies (i.e., companies with at least 100 employees) are more likely to have put in place a series of privacy practices, to have policies or procedures in place to assess privacy risks, and to have a privacy policy.

---

The contract value was \$74,242.36 (including HST).



## Introduction

Phoenix Strategic Perspectives (Phoenix SPI) was commissioned by the Office of the Privacy Commissioner of Canada (OPC) to conduct public opinion research with Canadian businesses on privacy-related issues.

## Background

The Privacy Commissioner of Canada is an advocate for the privacy rights of Canadians, with the powers to investigate complaints and conduct audits under two federal laws, publish information about personal information-handling practices in the public and private sectors, and conduct research into privacy issues. Mandated by Parliament to act as an ombudsman and guardian of privacy in Canada, the Commissioner is responsible for enforcing the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies to commercial activities in the Atlantic provinces, Ontario, Manitoba, Saskatchewan and the Territories. Quebec, Alberta, and British Columbia each has its own law covering the private sector. However, even in these provinces, PIPEDA continues to apply to the federally regulated private sector and to personal information in interprovincial and international transactions.

## Purpose and research objectives

Given its mandate, the OPC needs to understand the extent to which businesses are familiar with privacy issues; what type of privacy policies and practices businesses have in place; businesses' compliance with the law; and businesses' awareness and approaches to privacy protection. To address its information needs, the OPC conducts surveys with businesses every two years to inform and guide outreach efforts with businesses. The findings will be used to help the Office: 1) provide guidance to both individuals and organizations on privacy issues; and 2) enhance its outreach efforts with small businesses, which can be an effective way to achieve positive change for privacy protection.

## Methodology

A telephone survey was administered to 1,003 companies across Canada. Businesses were divided by size for sampling purposes. Interviewing was conducted by Phoenix SPI's subcontractor, Elemental Data Collection Inc. (EDCI), using Computer Aided Telephone Interviewing (CATI) technology. The results were weighted by size, sector and region using Statistics Canada data to ensure that they reflect the actual distribution of businesses in Canada. Based on a sample of this size, the results can be considered accurate to within  $\pm 3.1\%$ , 19 times out of 20.

The following specifications applied to the survey:

- The target respondents were senior decision makers with responsibility and knowledge of their company's privacy and security practices.
- The sampling frame was purchased from Dun & Bradstreet (D&B). A random sample frame was generated for each of three target business size quotas: small (one-19 employees); medium (20-99 employees); and large (100+ employees).
- A telephone pre-test was conducted in English and French, with 10 interviews in each official language. Interviews were digitally recorded for review afterwards.
- Interviews were conducted in the respondent's official language of choice. In total, 80% of interviews were completed in English and 20% were completed in French.



- Respondents were informed that the survey was commissioned by the OPC.
- The survey was conducted from November 29, 2019 to December 19, 2019.

The table below presents information about the final call dispositions for this survey, as well as the associated response rate.<sup>1</sup>

	Total
<b>Total numbers attempted</b>	<b>10,047</b>
<b>Out-of-scope - Invalid</b>	<b>1,288</b>
<b>Unresolved (U)</b>	<b>3,974</b>
<i>No answer/Answering machine</i>	3,974
<b>In-scope - Non-responding (IS)</b>	<b>3,756</b>
<i>Language barrier</i>	47
<i>Incapable of completing (ill/deceased)</i>	138
<i>Callback (respondent not available)</i>	1,717
<i>Refusal</i>	1,744
<i>Termination</i>	110
<b>In-scope - Responding units (R)</b>	<b>1,029</b>
<i>Completed interview</i>	1,003
<i>Not eligible (not-for-profit)</i>	26
<b>Response rate</b>	<b>11.8%</b>

## Notes to readers

- Results are compared to similar surveys conducted in 2011, 2013, 2015 and 2017.
- All results are expressed as percentages, unless otherwise noted. Throughout the report, percentages may not always add to 100 due to rounding and/or multiple responses being offered by respondents.
- At times, the number of respondents changes in the report because questions were asked of sub-samples of the survey population. Accordingly, readers should be aware of this and exercise caution when interpreting results based on smaller numbers of respondents.
- Where base sizes are reported in graphs, they reflect the actual number of respondents who were asked the question.
- Subgroup differences are identified in the report. When reporting subgroup variations, only differences that are significant at the 95% confidence level and that pertain to a subgroup sample size of more than n=30 are discussed in the report. If one or more categories in a subgroup are not mentioned in a discussion of subgroup differences (for example, if two out of six regions are compared), it can be assumed that significant differences were found only among the categories reported.
- Only subgroup differences that are statistically significant at the 95% confidence level or are part of a pattern or trend are reported.
- The survey questionnaire is appended to the report.

<sup>1</sup> The response rate formula is as follows:  $[R=R/(U+IS+R)]$ . This means that the response rate is calculated as the number of responding units [R] divided by the number of unresolved [U] numbers plus in-scope [IS] non-responding households and individuals plus responding units [R].

# Detailed findings

## 1. Use and storage of customer information

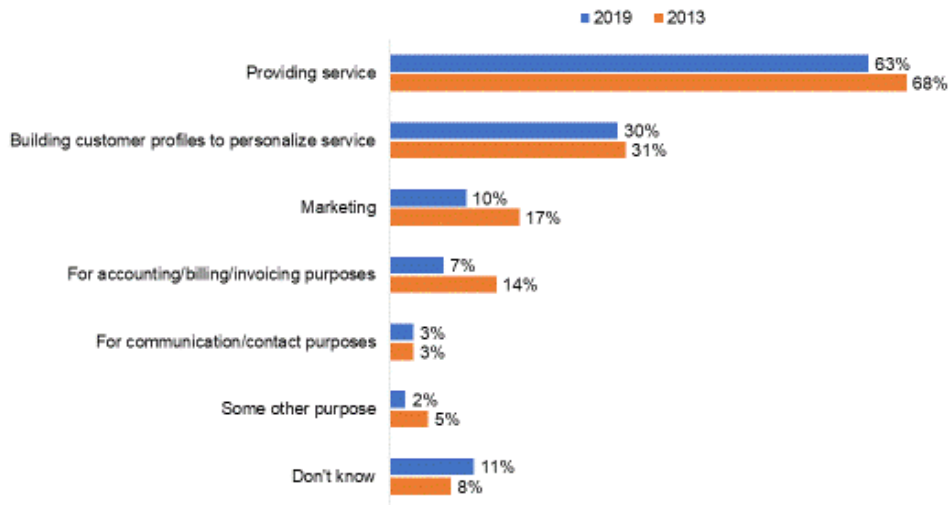
This section discusses how Canadian businesses use and store the personal information they collect from customers.

### Many businesses use the customers' personal information they collect to provide service

Nearly two-thirds of companies (63%) use the information they collect about their customers to provide services. Slightly less than one-third (30%) use this information to build profiles to personalize services for their customers. Ten percent or fewer use this information for other purposes: for marketing (10%), for accounting/billing/invoicing (7%), and for communicating or contacting customers (3%).

Figure 1: Purpose of customer information collected by companies

Figure 1: Purpose of customer information collected by companies



Q3. What does your business do with the personal information that it collects about your customers? [Multiple responses accepted] Base in 2019: n=1,003; all respondents.

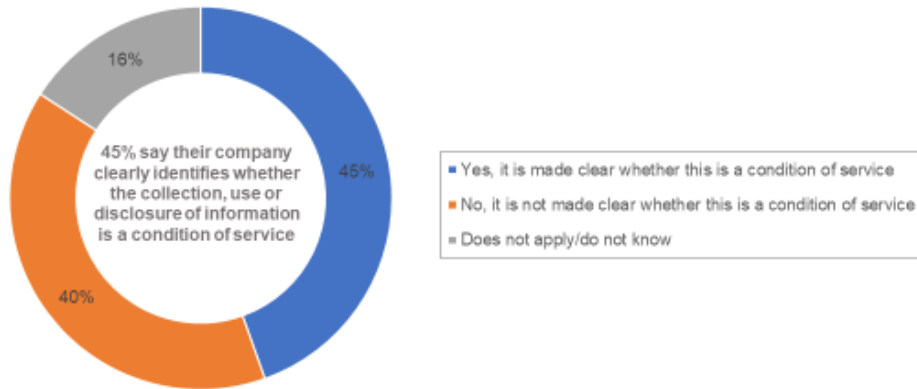
This question was previously asked of Canadian businesses in 2013. As was the case in 2013, providing service and building customer profiles were the most frequently mentioned uses of customers' personal information.

### Significant minority discloses whether personal information collection/use/disclose is a condition of service

More than 4 in 10 business representatives (45%) say their company makes clear to customers whether the collection, use or disclosure of information is a condition of service. In contrast, 40% say their company does not do this, while the remainder feel this does not apply to their company (9%) or do not know whether their company has such a practice (7%).

Figure 2: Disclosure, collection, or use of customers' information

Figure 2: Disclosure, collection, or use of customers' information



Q17c: Does your company do any of the following: Make clear whether the collection, use or disclosure of information is a condition of service. Base: n=1,003; all respondents. [DK/NR: 7%].

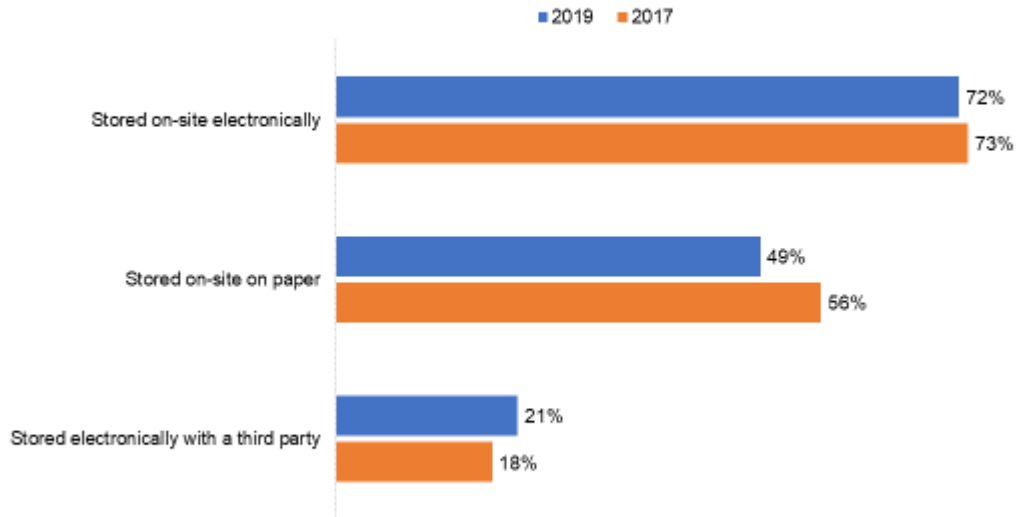
Companies in Ontario (51%) are more likely than companies in the Prairies (27%) to make it clear to customers whether the collection, use or disclosure of information is a condition of service. In addition, self-employed individuals (33%) are less likely than medium (53%) and large (48%) companies to make this information clear to customers.

### Most companies store personal information on-site electronically

While Canadian businesses use a variety of methods to store customers' personal information, storing information on-site electronically is by far the most common method. The clear majority of business representatives (72%) say their company stores information about their customers on-site electronically. Following this, approximately half (49%) say their business stores customers' personal information on-site on paper, and one in four (25%) store information electronically with a third party.

Figure 3: Methods used by companies to store personal information

**Figure 3: Methods used by companies to store personal information**



Q4. In which of the following ways does your company store personal information on your customers? Is the information...? [Multiple responses accepted] Base in 2019: n=1,003; all respondents; DK/NR=1%.

Companies located in Quebec (78%) are more likely to store customers' personal information on-site electronically than companies based in Ontario, including those specifically located in the Greater Toronto Area (GTA) (67% and 65% respectively, who say they store customer information on-site electronically). The likelihood of storing customer information on-site electronically generally increased with company size, from 64% of the self-employed to 81% of large companies (i.e., companies with 100 or more employees).

Compared to 2017, fewer companies are storing customer information on-site on paper. In 2017, 56% of companies surveyed stored information on-site on paper; in 2019, 49% of companies store information in this way. Use of electronic storage, whether on site or via a third party, has not changed in any significant way.

## 2. Company privacy practices

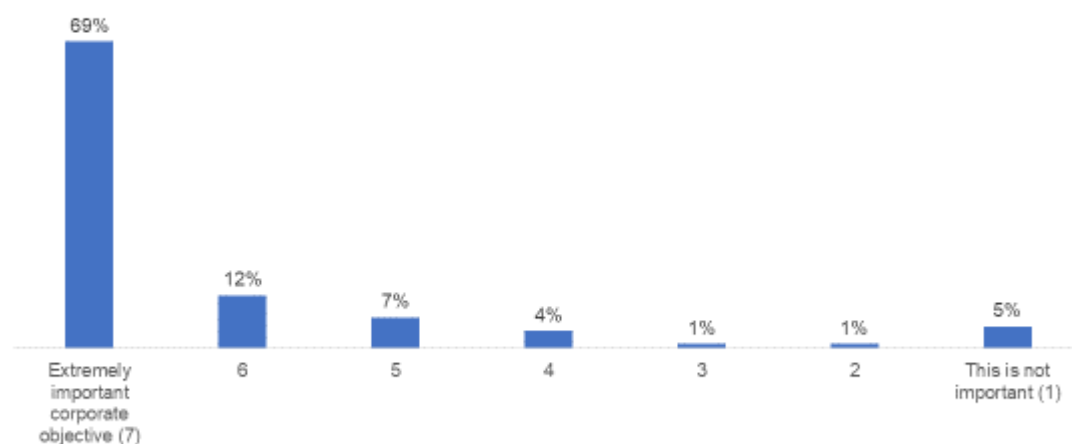
This section identifies the procedures and policies companies have in place to protect the personal information they collect about their customers.

### Majority attribute significant importance to protecting their customers' privacy

Before exploring company privacy practices, business representatives were asked what level of importance their company attributes to protecting customers' personal information. Most Canadian businesses attribute significant importance to protecting their customers' privacy. Four in five business representatives say their company considers the protection of customers' personal information to be of high importance (scores of 6 and 7), with 69% saying it is an extremely important corporate objective. At the other end of the spectrum, very few companies (5%) indicated clearly that protecting customers' personal information is not an important corporate objective.

Figure 4: Importance companies attribute to protecting customers' privacy

Figure 4: Importance companies attribute to protecting customers' privacy



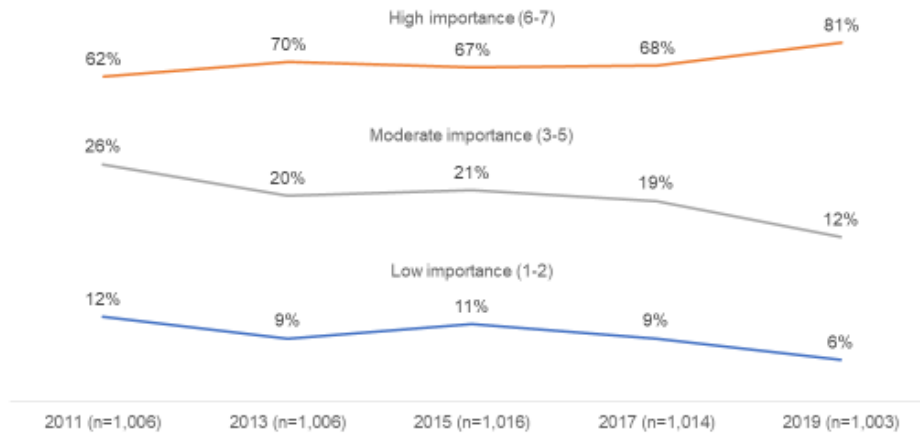
Q5. What importance does your company attribute to protecting your customers' personal information? Base: n=1,003; all respondents; [DK/NR=1%].

Companies that only sell to consumers (77%) are significantly more likely to attribute extreme importance to protecting their customers' personal information than companies that sell to other businesses (63%) or to both businesses and consumers (66%). The likelihood of attributing extreme importance to this as a corporate objective was highest among large companies (83% compared to 62% to 74% of small and medium-sized companies).

Over time, the importance companies attribute to protecting customers' personal information has increased significantly, from 62% in 2011 to 81% in 2019.

Figure 5: Importance companies attribute to protecting customers' privacy [over time]

**Figure 5: Importance companies attribute to protecting customers' privacy [over time]**



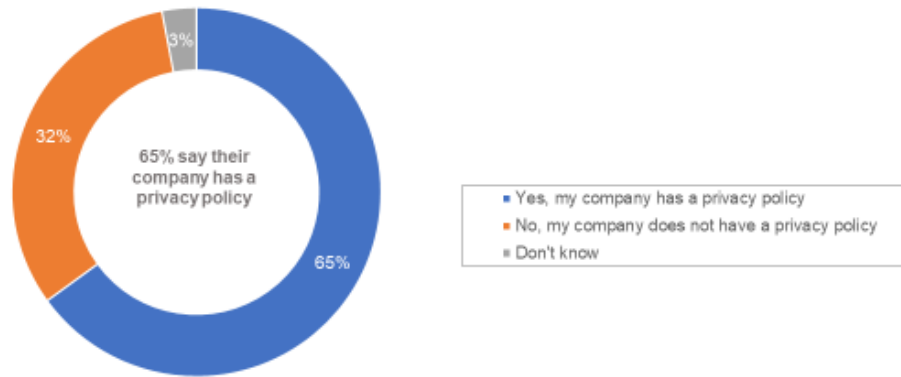
Q5. What importance does your company attribute to protecting your customers' personal information?

**Nearly two-thirds of companies have a privacy policy**

Approximately two-thirds of business representatives (65%) say their company has a privacy policy. Conversely, 32% of Canadian businesses do not have a privacy policy (the remainder – 3% – do not know whether their company has such a policy).

Figure 6: Privacy policies

Figure 6: Privacy policies



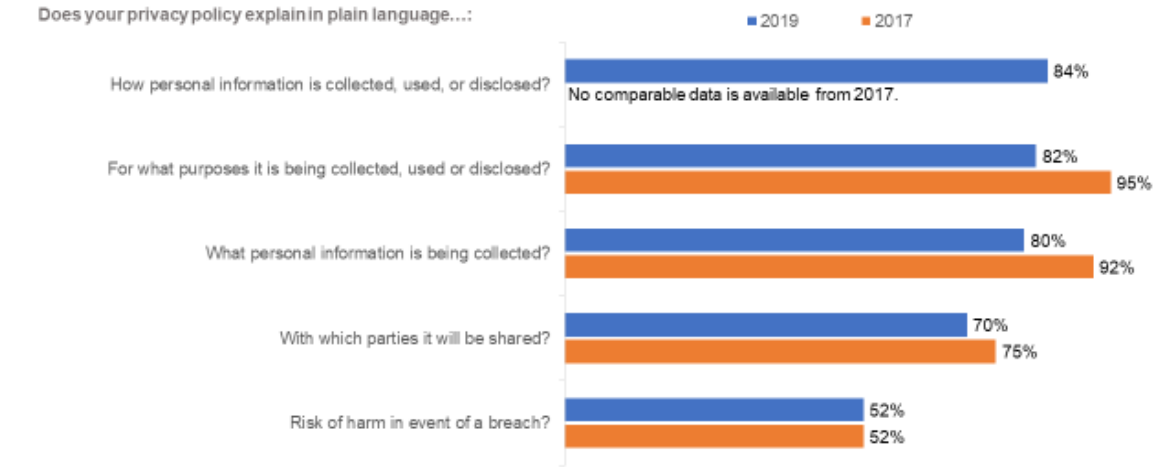
Q15. Does your company have a privacy policy? Base: n=1,003; all respondents.

Respondents who are self-employed (44%) are least likely to have a privacy policy and companies employing 100 or more staff (83%) are most likely to have one. Moreover, companies based in Quebec (48%) are less likely than companies in Ontario (75%; 73% in the Greater Toronto Area), British Columbia (71%), and Alberta (64%) to have such a policy.

Among the companies that do have a privacy policy (n=717), many have a policy that explains in plain language how their company collects, uses and discloses customers' information (84%), the purpose for which customers' personal information is being collected (82%), and what personal information is being collected (80%). In addition, 7 in 10 of these companies have a privacy policy that explains plainly which parties the collected personal information will be shared with (70%). Among the companies with a privacy policy, only 52% say their company's policy explains the risk of harm in the event of a breach.

Figure 7: Features of privacy policies

Figure 7: Features of privacy policies



Q16. Does your privacy policy explain in plain language...? Base: n=717; all companies with privacy policies.

Compared to 2017, fewer companies say their privacy policy explains in plain language to customers for what purpose their information is being collected, used or disclosed (82% compared to 95% in 2017), what personal information is being collected (80% compared to 92%), and with which parties their information will be shared (70% compared to 75%).

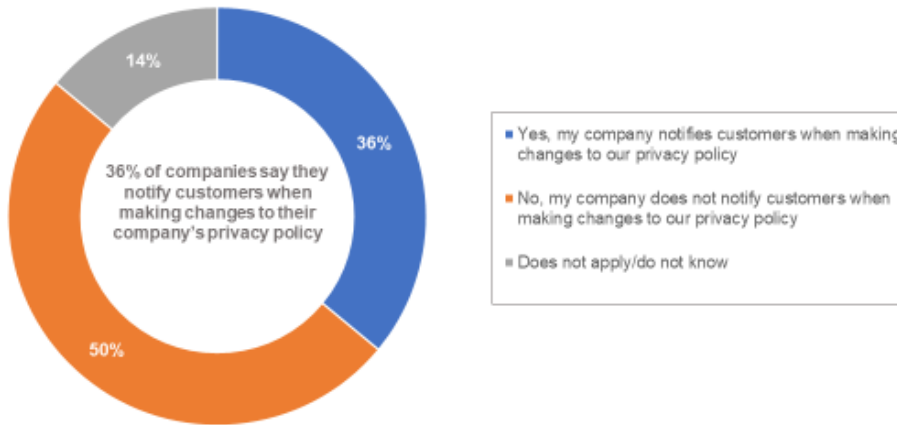


### One-third of companies notify customers when making changes to their privacy policy

Approximately one-third (36%) of companies that have a privacy policy notify customers when making changes to this policy. Exactly half (50%) do not. The remainder – 14% – do not know whether their company makes such a disclosure to customers or feel this does not apply to their company.

Figure 8: Notifying customers about changes to privacy policies

Figure 8: Notifying customers about changes to privacy policies



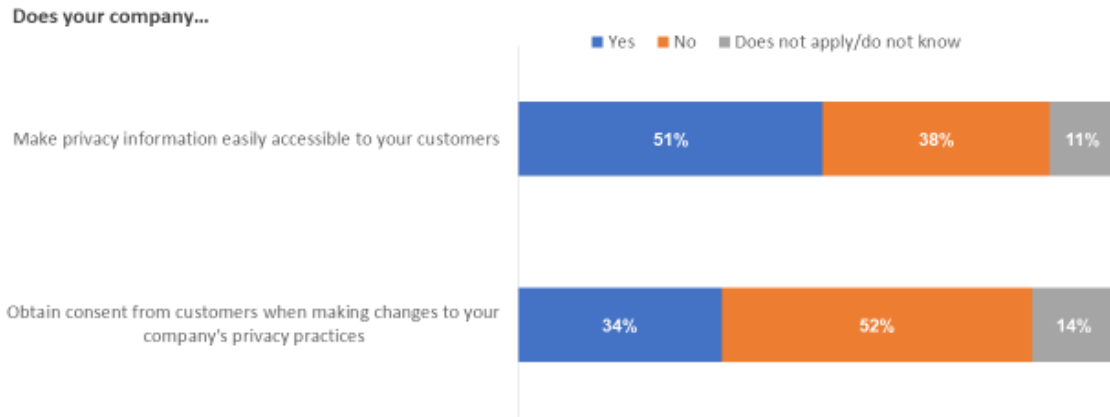
Q17a. Does your company do any of the following: Notify customers when making changes to your company's privacy policy. Base: n=717; all companies with privacy policies. [DK/NR: 7%]

### Half make privacy information accessible to customers; fewer obtain customer consent when making changes to their privacy policy

Approximately half (51%) of companies surveyed make their privacy information easily accessible to customers and roughly one-third (34%) say they obtain consent from customers when making changes to their company's privacy practices.

Figure 9: Steps taken to inform customers about the company's privacy practices

Figure 9: Steps taken to inform customers about the company's privacy practices



Q17b/17d. Does your company do any of the following...? Base: n=1,003; all respondents. [DKNR: 4%]

Respondents who are self-employed (businesses with one employee) are significantly more likely than larger companies to say they do **not** obtain consent from customers when making changes to corporate privacy practices nor make privacy information easily accessible to customers.

### Half or more have implemented most privacy compliance practices

Business representatives were asked whether their company had put in place a series of privacy practices. These included:

- Having designated someone in their company to be responsible for privacy issues and personal information that the company holds;
- Having developed and documented internal policies for staff that address their privacy obligations under the law;
- Having staff regularly receive privacy training and education;
- Having procedures in place for responding to customer requests for access to their personal information; and
- Having procedures in place for dealing with complaints from customers who feel that their information has been handled improperly.

Half or more of Canadian businesses surveyed have implemented the following privacy compliance practices: having a designated privacy officer (62%); having procedures in place for responding to customer requests for access to their personal information (60%); having procedures in place for dealing with customer complaints about the handling of their personal information (58%); and having internal policies for staff that address privacy obligations (55%). Approximately four in 10 (39%) say their business regularly provides staff with privacy training and education.

Figure 10: Privacy policy practices

**Figure 10: Privacy policy practices**



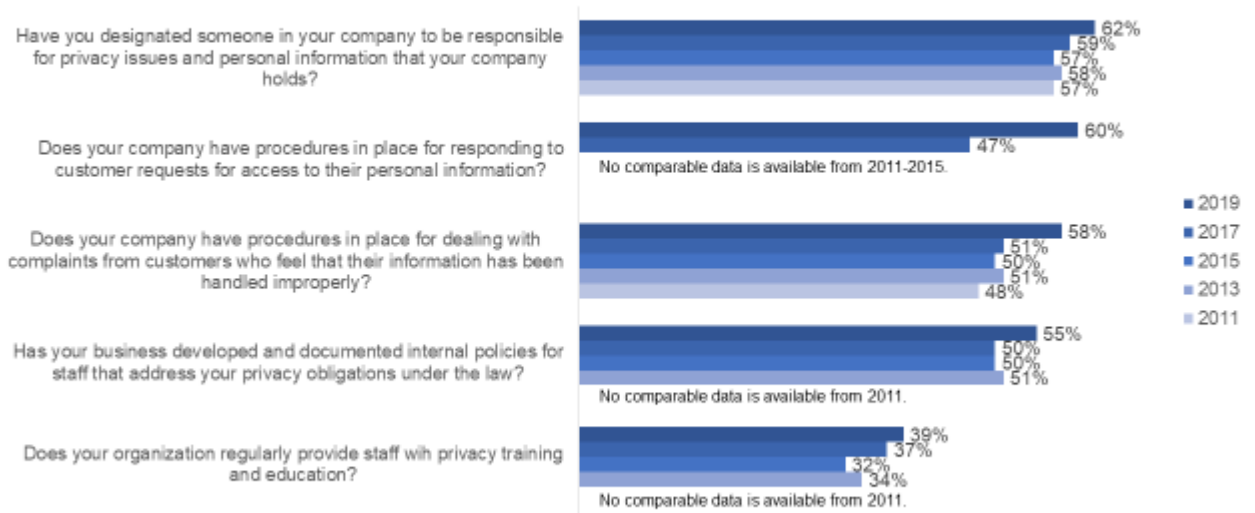
Q10 to Q14. Base: n=1,003; all respondents [DK/NR=3% to 6%]

Companies in Quebec are generally less likely to have implemented these privacy compliance practices. In addition, the likelihood of having implemented these practices increased with business size and was highest among large companies.

Across all measures, compliance has improved over time.

Figure 11: Privacy policy practices [over time]

**Figure 11: Privacy policy practices [over time]**



Q10 to Q14. Base: n=1,003; all respondents [DK/NR=3% to 6%]

### 3. Managing privacy risks

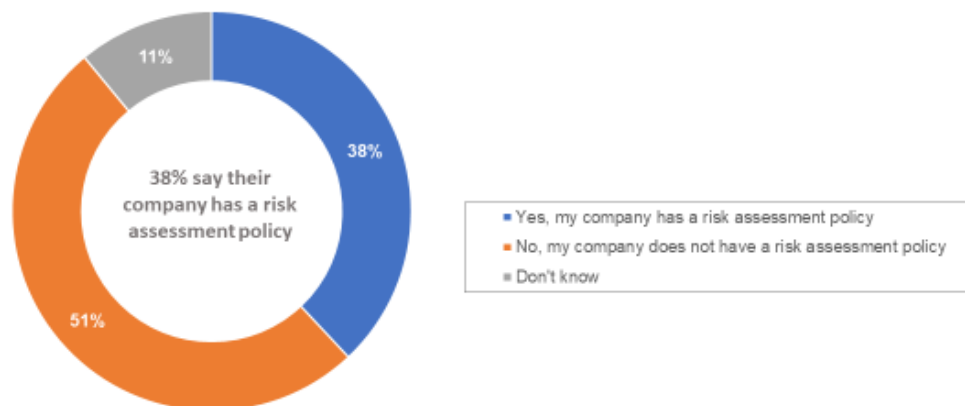
This section examines how Canadian business manage privacy risks, include data breaches.

#### More than one-third say their company has a policy in place to assess privacy risks

Just under 2 in 5 business representatives (38%) say their company has policies or procedures in place to assess privacy risks related to the business. Approximately half (51%) do not have such a policies or procedures. The rest (11%) do not know whether their company has policies or procedures to assess privacy risks.

Figure 12: Corporate policies in place to assess privacy risks

Figure 12: Corporate policies in place to assess privacy risks



Q18. Does your company have any policies or procedures in place to assess privacy risks related to your business? Base: 1,003; all respondents.

The likelihood of having policies or procedures in place to assess privacy risks increased with business size and was highest among large companies.

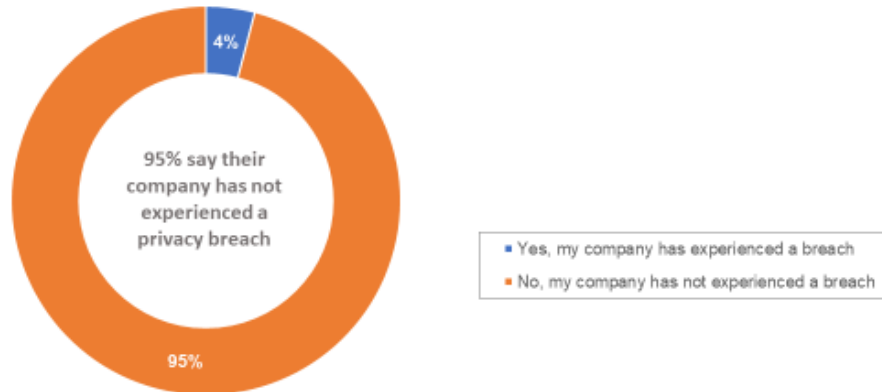
Since tracking of this measure began in 2013, the number of companies that have policies or procedures in place to assess privacy risks has increased 10 percentage points. While 28% of companies surveyed in 2013 had such policies and procedures in place to assess privacy risks, that proportion increased to 37% in 2017, and is virtually unchanged at 38% in 2019.

### Vast majority say their company has not experienced a privacy breach

Most business representatives (95%) say their company has not experienced a breach where the personal information of their customers was compromised. Consistent with previous data, very few (4%) say their company has experienced a privacy breach.<sup>2</sup>

Figure 13: Proportion of companies that have experienced a privacy breach

Figure 13: Proportion of companies that have experienced a privacy breach



Q21. Has your company ever experienced a breach where personal information of your customers was compromised? Base: n=1,003; all respondents. [DK/NR: 1%]

The smaller the company is in size, the more likely the company is to have **not** experienced a privacy breach.

### Many companies addressed privacy breach by notifying affected customers

Of the companies that have experienced a privacy breach (n=38), almost half notified individuals who were affected by the breach. Following this, companies report addressing the breach by following proper procedures or implementing a security system or enhancing existing security systems.

### Polarized levels of concern over data breaches

Business representatives were asked to rate their level of concern about a data breach, where the personal information of their customers is compromised. Three in 10 (30%) say they are extremely concerned about a data breach, whereas exactly one-third (33%) say they are not at all concerned about a data breach.

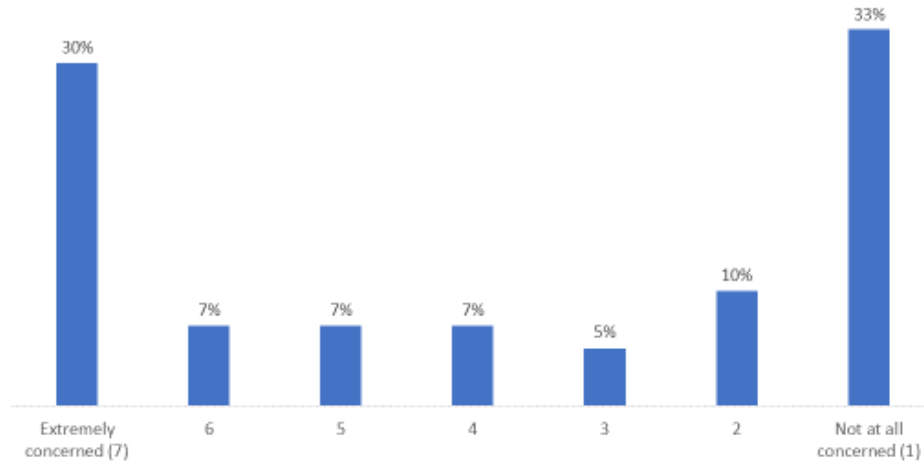
Before being asked this question, interviewers provided the following information:

*Data breaches can be caused by criminal activity, theft, hacking, or employee error such as misplacing a laptop or portable device.*

<sup>2</sup> The proportion of companies that have experienced a privacy breach ranges from 3% in 2010 to 4% in 2019.

Figure 14: Level of concern about a data breach

Figure 14: Level of concern about a data breach



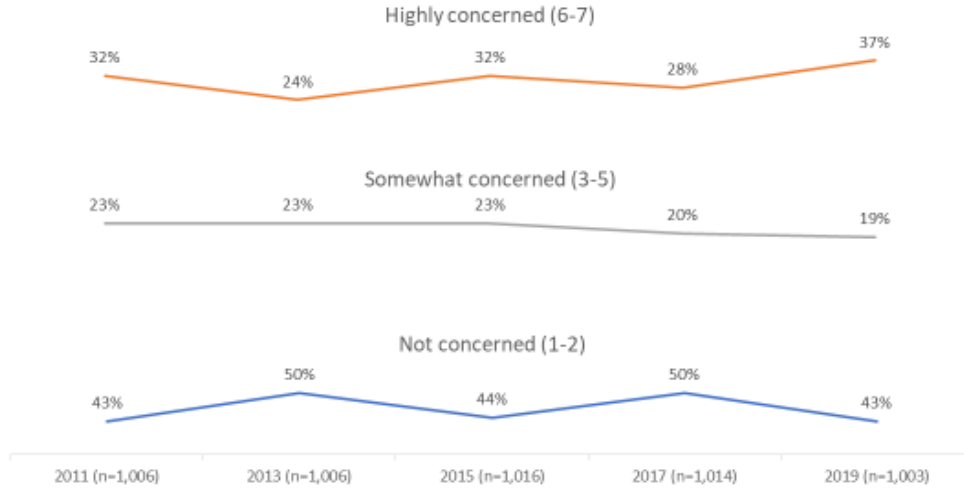
Q19. How concerned are you about a data breach, where the personal information of your customers is compromised? Base: n=1,003; all respondents [DKNR=1%].

With 45% of business representatives from Quebec-based companies selecting the highest score of seven on the scale, companies located in Quebec are the most likely to be extremely concerned about a data breach.

High concern about a data breach has fluctuated over time, from a low of 24% in 2013 to this year's high of 37%.

Figure 15: Level of concern about a data breach [over time]

**Figure 15: Level of concern about a data breach [over time]**



Q19. How concerned are you about a data breach, where the personal information of your customers is compromised? Base: n=1,003; all respondents [DK/NR=1%].

## 4. Awareness and impact of federal privacy law

This section examines findings regarding companies' awareness of their responsibilities under privacy laws. Questions in this section were prefaced with the following description of Canada's privacy laws:

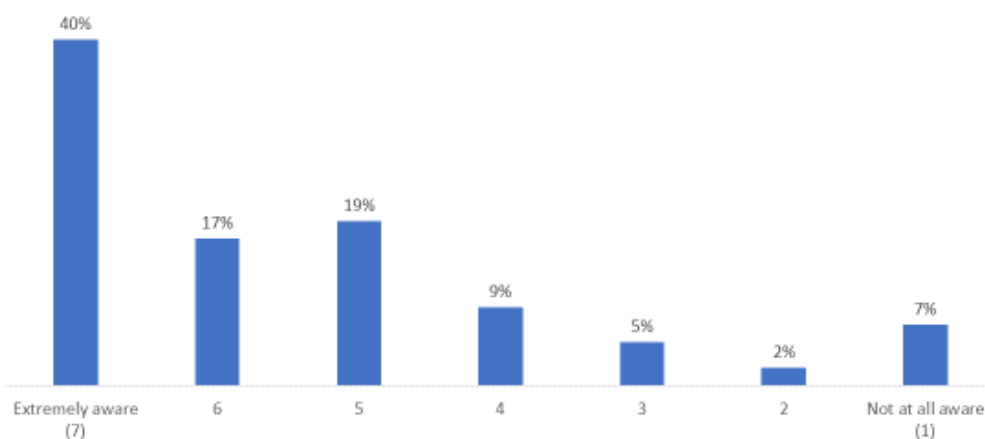
*The federal government's privacy law, the Personal Information Protection and Electronic Documents Act or PIPEDA, sets out rules that govern how businesses engaged in commercial activities should protect personal information. In Alberta, BC and Quebec, the private sector is governed by provincial laws, which are considered to be similar to the federal law.*

### Many companies have a high level of awareness of responsibilities under privacy laws

More than half of business representatives think their company is highly aware of its responsibilities under Canada's privacy laws (scores of six or seven), including 40% who say their company is extremely aware of these responsibilities. One-third (33%) rate their company as moderately aware of its privacy responsibilities (scores of three to five). Few (9%) rate their company's awareness as low (scores of one to two).

Figure 16: Companies' awareness of responsibilities under privacy laws

Figure 16: Companies' awareness of responsibilities under privacy laws



Q6. How would you rate your company's awareness of its responsibilities under Canada's privacy laws? Base: n=1,003; all respondents [DK/NR=1%].

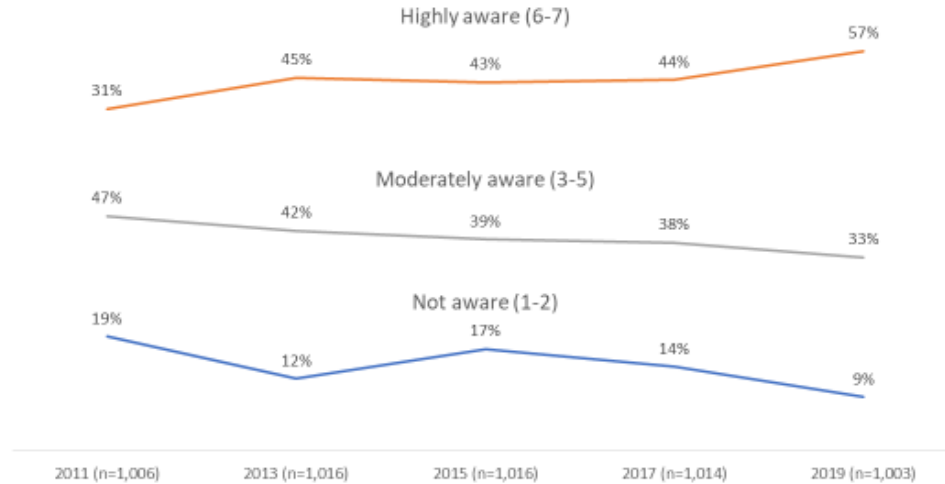
Companies based in Quebec (50%) and Ontario (43%) are more likely than companies in the Prairies (23%) and British Columbia (30%) to be extremely aware of their responsibilities under Canada's privacy laws.

The proportion of business representatives who say their company is highly aware of its responsibilities under Canada's privacy laws has increased significantly this year, from 44% in 2017 to 57% in 2019.



Figure 17: Companies' awareness of responsibilities under privacy laws [over time]

**Figure 17: Companies' awareness of responsibilities under privacy laws [over time]**



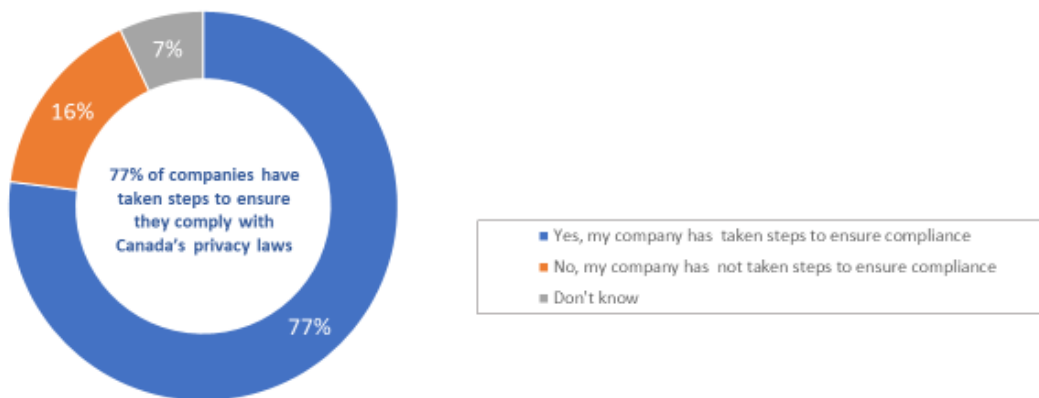
Q6. How would you rate your company's awareness of its responsibilities under Canada's privacy laws? Base: n=1,003; all respondents [DK/NR=1%].

**More than three-quarters have taken steps to comply with privacy laws**

More than three-quarters of business representatives (77%) say their company has taken steps to ensure it complies with Canada's privacy laws. This represents a significant increase since 2017, when 66% of companies had taken steps to ensure compliance.

Figure 18: Compliance with Canada's privacy laws

**Figure 18: Compliance with Canada's privacy laws**



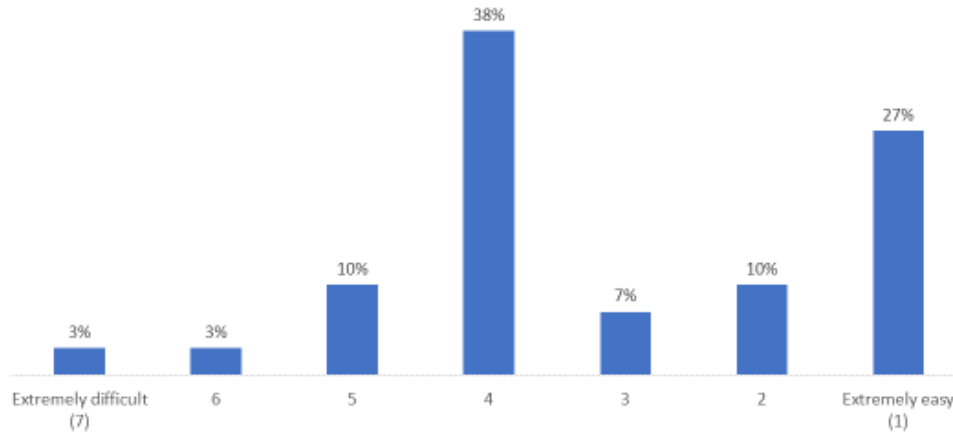
Q7. Has your company taken steps to ensure that it complies with Canada's privacy laws? Base: n=1,003; all respondents.

Companies in Alberta (86%) and Ontario (84%) were more likely than those in the Prairies (64%) and Quebec (68%) to have taken steps to ensure compliance. In addition, respondents who are self-employed are most likely to have **not** taken steps to ensure that their company complies with Canada's privacy laws.

## Large majority did not find compliance difficult

Figure 19: Level of difficulty complying with Canada's privacy laws

Figure 19: Level of difficulty complying with Canada's privacy laws



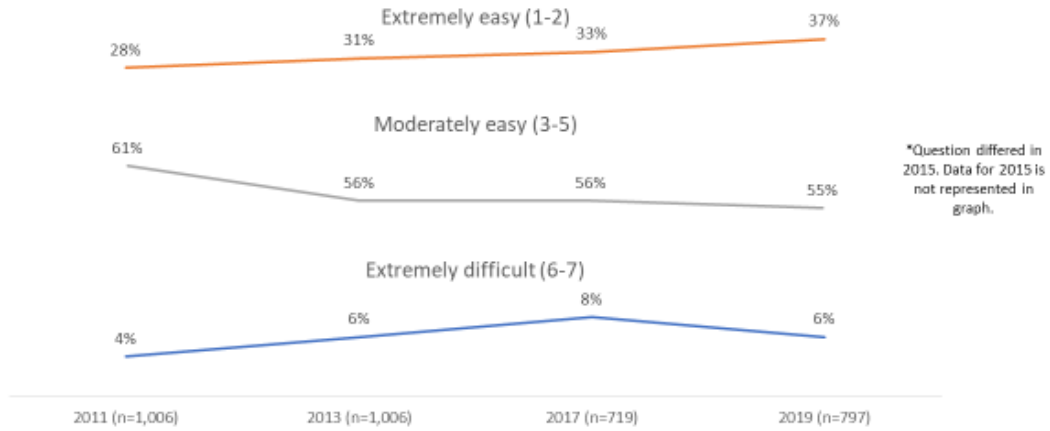
Q8. How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws? Base: n=797; companies that have taken steps to ensure compliance. [DK/NR=3%].

Roughly nine in 10 (92%) companies that have taken steps to comply with Canada's privacy laws (n=797) did not find it difficult to bring their personal information handling practices into compliance.

The proportion of companies that find it very easy to bring personal information handling practices into compliance with Canada's privacy laws has steadily increased over time, from 28% in 2011 to this year's high of 37%.

Figure 20: Compliance with Canada's privacy laws [over time]

Figure 20: Compliance with Canada's privacy laws [over time]



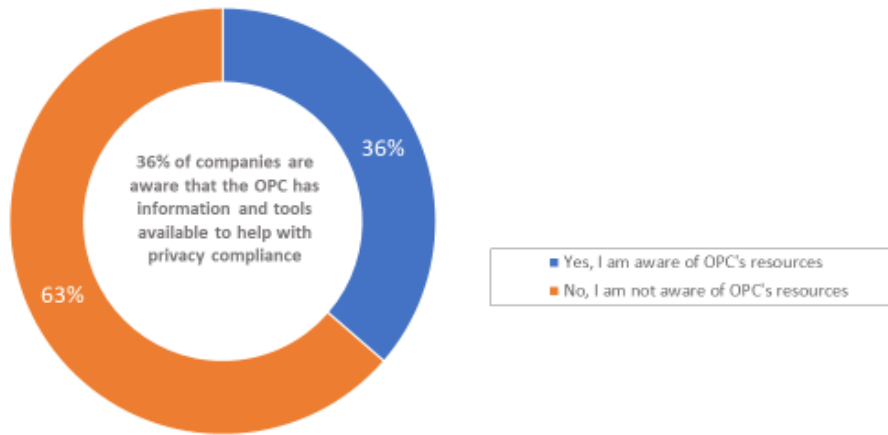
Q8. How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws? Base: n=797; companies that have taken steps to ensure compliance. [DK/NR=3%].

### Over one-third aware of resources provided by the OPC

Slightly more than one-third (36%) of companies are aware that the OPC has information and tools to help companies comply with their privacy obligations. Conversely, nearly two-thirds (63%) say they are not aware of the OPC's resources. Awareness of OPC's resources for business has declined this year from the high of 44% recorded in 2017.

Figure 21: Awareness of OPC resources

Figure 21: Awareness of OPC resources



Q9. Are you aware that the Office of the Privacy Commissioner of Canada has information and tools available to companies to help them comply with their privacy obligations?  
Base: n=1,003 all respondents. [DK/NR: 1%].

Companies based in Quebec (25%) are less likely than those in Atlantic Canada (50%) or Ontario (43%) to be aware that the Office of the Privacy Commissioner of Canada has information and tools available to companies to help them comply with their privacy obligations. The likelihood of being aware of these resources was higher among medium (48%) and large (49%) companies than among smaller companies.

## 5. Corporate profile

The following tables present the characteristics of Canadian businesses included in the survey sample (using weighted data).

Customer type	Percent
Sells directly to consumers	32%
Sells directly to other businesses/organizations	26%
Sells directly to consumers and other businesses/organizations	41%
Other	<1%

Region	Percent
Atlantic Canada	6%
Quebec	21%
Manitoba and Saskatchewan	7%
Alberta	16%
British Columbia	14%
Ontario (excluding the Greater Toronto Area)	16%
Greater Toronto Area	21%

Business size	Percent*
1 employee (self-employed)	15%
2-4 employees	24%
5-9 employees	22%
10-19 employees	25%
20-99 employees	10%
100+ employees	4%
Don't know/No response	2%

Revenues	Percent
Less than \$100,000	15%
\$100,000 to just under \$250,000	9%
\$250,000 to just under \$500,000	10%
\$500,000 to just under \$1,000,000	10%
\$1,000,000 to just under \$5,000,000	18%
\$5,000,000 to just under \$10,000,000	4%
\$10,000,000 to just under \$20,000,000	2%
More than \$20 million	1%
Don't know / no response	31%

# Appendix

## 1. Survey questionnaire

### INTRODUCTION

Hello/bonjour, my name is [Interviewer's name]. Would you prefer to continue in English or French? / Préférez-vous continuer en anglais ou en français?

I'm calling on behalf of Phoenix SPI, a public opinion research company. We're conducting a survey for the Privacy Commissioner of Canada to better understand the needs and practices of businesses across the country in relation to Canada's privacy laws.

May I speak to the person in your company who is the most familiar with the types of personal information collected about your customers, and how this information is stored and used. This may be your company's Privacy Officer if you have one.

- IF PERSON IS AVAILABLE, CONTINUE. REPEAT INTRODUCTION IF NEEDED.
- IF NOT AVAILABLE, SCHEDULE CALL-BACK.

This survey should take no more than 15 minutes to complete. Participation is voluntary and completely confidential, and your answers will remain anonymous.

May I continue?

- Yes, now [CONTINUE]
- No, call later. Specify date/time: Date: Time:
- Refused [THANK/DISCONTINUE]

### SCREENING

1. Which of the following best describes your company? [READ LIST, ACCEPT ONE RESPONSE]

It sells directly to individual consumers\*

It sells directly to other businesses/organizations

It sells directly both to consumers and other businesses/organizations

Other, please specify: \_\_\_\_\_

DO NOT READ: Not for profit

[THANK AND TERMINATE]

DO NOT READ: Don't now/refusal

[THANK AND TERMINATE]

\*INTERVIEWER NOTE: IF ASKED ABOUT RESPONSE OPTION (1) "CONSUMERS", SAY: This refers to an individual not a business or organization.

2. Approximately how many employees work for your company in Canada? Please include part-time employees as full-time equivalents. [DO NOT READ LIST]

- One (i.e. self-employed)
- 2-4
- 5-9
- 10-19
- 20-49
- 50-99
- 100-149
- 150-199
- 200-249
- 250-299
- 300-499
- 500-999
- 1,000-4,999
- More than 5,000

**Section 1. Customers' Personal Information**

I'd like to begin by asking you about the personal information held by your company about your customers.

INTERVIEWER NOTE: If asked what is meant by "personal information", say: By personal information, I mean things like a customer's name, email address, opinions, purchase history, or financial information, such as their credit card.

3. What does your business do with the personal information that it collects about your customers? Do you use it for...? [READ LIST. ACCEPT ALL THAT APPLY] T-2013

- Marketing
- Providing service\*
- Building customer profiles to personalize service
- Or for some other purpose. If so, please specify:

\*IF ASKED WHAT IS MEANT BY USING PERSONAL INFORMATION TO PROVIDE A SERVICE, SAY: An example of this would be the collection of a credit card number from a customer to complete a purchase, or the collection of an email address to send an invoice.

4. In which of the following ways does your company store personal information on your customers? Is the information...? [READ LIST. ACCEPT ALL THAT APPLY] T2017 – MODIFIED

- Stored on-site on paper
- Stored on-site electronically
- Stored off-site with a third-party, such as a cloud service

[VOLUNTEERED] Company does not collect personal information about customers

5. What importance does your company attribute to protecting your customers' personal information? Please use a scale from 1 to 7, where 1 means that this is not an important corporate objective at all, and 7 means it is an extremely important objective. T2017



## Section 2: Canada's Privacy Laws and Compliance

The federal government's privacy law, the *Personal Information and Protection and Electronic Documents Act* or PIPEDA (PRONOUNCED PIP-EE-DAH) sets out rules that govern how businesses engaged in commercial activities should protect personal information. In Alberta, BC and Quebec, the private sector is governed by provincial laws, which are considered to be similar to the federal law. T2017

6. How would you rate your company's awareness of its responsibilities under Canada's privacy laws? Please use a scale from 1 to 7, where 1 is not at all aware, and 7 is extremely aware. T2017

7. Has your company taken steps to ensure that it complies with Canada's privacy laws? T2017

Yes	<b>CONTINUE</b>
No	<b>SKIP TO Q9</b>
[VOLUNTEERED] Don't know	<b>SKIP TO Q9</b>

**[IF Q7 = "YES"]**

8. How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws? Please use a scale from 1 to 7, where 1 is extremely easy, and 7 is extremely difficult. MODIFIED-T2017

**[ALL]**

9. Are you aware that the Office of the Privacy Commissioner of Canada, or the OPC, has information and tools available to companies to help them comply with their privacy obligations? MODIFIED-T2017

Yes
No
[VOLUNTEERED] Not aware of the OPC

INTERVIEWER NOTE: If asked about the OPC/how to reach the OPC, please share the website: [priv.gc.ca](http://priv.gc.ca).

## Section 3: Company Privacy Practices

Now I'd like to ask you about your company's privacy practices.

10. Have you designated someone in your company to be responsible for privacy issues and personal information that your company holds? T2017

Yes
No
[VOLUNTEERED] Don't know

11. Has your business developed and documented internal policies for staff that address your privacy obligations under the law? T2017

Yes

No

[VOLUNTEERED] Don't know

12. Does your organization regularly provide staff with privacy training and education? T2017

Yes

No

[VOLUNTEERED] Don't know

13. Does your company have procedures in place for responding to customer requests for access to their personal information? T2017

Yes

No

[VOLUNTEERED] Don't know

14. Does your company have procedures in place for dealing with complaints from customers who feel that their information has been handled improperly? T2017

Yes

No

[VOLUNTEERED] Don't know

15. Does your company have a privacy policy?

Yes

No

[VOLUNTEERED] Don't know

**CONTINUE**

**SKIP TO Q17**

**SKIP TO Q17**

16. Does your privacy policy explain in plain language...? [READ LIST] T2017

- a) How your company collects, uses and discloses customers' personal information
- b) What personal information your company is collecting from customers
- c) For what purposes customers' personal information is being collected, used or disclosed
- d) With which parties customers' personal information will be shared
- e) The risk of harm to the individual, if any, in the event of data breach

RESPONSE OPTIONS:

Yes

No

[VOLUNTEERED] Don't know

[VOLUNTEERED] Does not apply

**[ALL]**

Still thinking about your company's collection and use of customers' personal information ...

17. Does your company do any of the following? [READ LIST] NEW-2019

- a) Notify customers when making changes to your company's privacy policy.
- b) Obtain consent from customers when making changes to your company's privacy practices.
- c) Make clear whether the collection, use or disclosure of information is a condition of service.
- d) Make privacy information easily accessible to your customers.

RESPONSE OPTIONS:

Yes

No

[VOLUNTEERED] Don't know

[VOLUNTEERED] Does not apply

#### **Section 4: Risk Assessment and Breaches**

18. Does your company have any policies or procedures in place to assess privacy risks related to your business? This includes assessing privacy risks associated with the development or use of new products, services, or technologies. T2017

Yes

No

[VOLUNTEERED] Don't know

Data breaches can be caused by criminal activity, theft, hacking, or employee error such as misplacing a laptop or other portable device. T2017

19. How concerned are you about a data breach, where the personal information of your customers is compromised? Please use a scale of 1 to 7, where 1 is not at all concerned, and 7 is extremely concerned. T2017

20. Does your company ensure that it keeps records of all data breaches involving your customers' personal information? NEW-2019

Yes

No

[VOLUNTEERED] Does not apply; have not had a breach

**CONTINUE**

**CONTINUE**

**SKIP TO Q23**

**[IF Q20 ≠ "DOES NOT APPLY"]**

21. Has your company ever experienced a breach where the personal information of your customers was compromised? T2011

Yes **CONTINUE**  
No **SKIP TO Q23**  
[VOLUNTEERED] Don't know **SKIP TO Q23**

**[IF Q21 = YES]**

22. What did your company do to address this situation? [DO NOT READ LIST. ACCEPT MULTIPLE RESPONSES] T2011

Notified individuals who are affected  
Notified government agencies who oversee Canada's privacy laws  
Notified law enforcement  
Followed proper procedure (general)  
Notified company's head office, HR, or privacy department  
Obtained legal counsel/took legal action  
Resolved issue with individuals responsible for the breach (e.g. termination/reprimand of employee)  
Obtained information from government (websites, 1-800 number)  
Issued training or re-training for staff  
Reviewed privacy policy or practices  
Implemented security system or enhanced security  
Other (specify): \_\_\_\_\_

### **Section 5: Corporate Profile**

These last questions are for statistical purposes only, and all answers are confidential.

23. In what industry or sector do you operate? If your company is active in more than one sector, please identify the main sector. [DO NOT READ LIST. ACCEPT ONE RESPONSE]

Accommodation and Food Services  
Administrative and Support, Waste Management and Remediation Services  
Agriculture, Forestry, Fishing and Hunting  
Arts, Entertainment and Recreation  
Construction  
Educational Services  
Finance and Insurance  
Health Care and Social Assistance  
Information and Cultural Industries  
Management of Companies and Enterprises  
Manufacturing  
Mining and Oil and Gas Extraction  
Other Services (except Public Administration)  
Professional, Scientific and Technical Services  
Public Administration

Real Estate and Rental and Leasing  
Retail Trade  
Transportation and Warehousing  
Utilities  
Wholesale Trade  
Other. Please specify:

24. What is your own position within the organization? [DO NOT READ LIST. ACCEPT ONE RESPONSE]

Owner, President or CEO  
General Manager/Other Manager  
IT Manager  
Administration  
Vice President  
Privacy analyst/officer/coordinator  
Legal counsel/lawyer  
HR/Operations  
Other: Specify

25. In which of the following categories would your company's 2018 revenues fall? [READ LIST. ACCEPT ONE RESPONSE]

Less than \$100,000  
\$100,000 to just under \$250,000  
\$250,000 to just under \$500,000  
\$500,000 to just under \$1,000,000  
\$1,000,000 to just under \$5,000,000  
\$5,000,000 to just under \$10,000,000  
\$10,000,000 to just under \$20,000,000  
More than \$20 million  
DO NOT READ: PREFER NOT TO SAY

**This concludes the survey.  
Thank you for your time and feedback, it is much appreciated.**

## 2. Statement of political neutrality

I hereby certify, as a Senior Officer of Phoenix Strategic Perspectives, that the deliverables fully comply with the Government of Canada political neutrality requirements outlined in the Policy on Communications and Federal Identity of the Government of Canada and Procedures for Planning and Contracting Public Opinion Research. Specifically, the deliverables do not contain any reference to electoral voting intentions, political party preferences, standings with the electorate, or ratings of the performance of a political party or its leader.

Signed:



Alethea Woods, President  
Phoenix Strategic Perspectives