Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

2021-22 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: 2R008-210080-001-CY
Award Date: 2021-11-05
Contract Value: $75,575.74 (including applicable tax)
Delivery Date: 2022-03-10

Registration Number: POR 035-21

For more information, please contact: publications@priv.gc.ca.

Ce rapport est aussi disponible en français.

Canada

2021-2022 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.
March 2022

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 research study was conducted with 751 representatives of Canadian businesses between January 12 and February 18, 2022.

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

Catalogue Number: IP54-96/2022E-PDF

International Standard Book Number (ISBN): 978-0-660-43174-1

Related publications (POR registration number: POR 035-21):
Catalogue number (Final report, French): IP54-96/2022F-PDF
ISBN: 978-0-660-43175-8

Aussi offert en français sous le titre *Sondage de 2021-2022 auprès des entreprises canadiennes concernant les enjeux liés à la protection des renseignements personnels*.

Table of Contents

Executive Summary....1

Introduction....4

Background....4
Purpose and research objectives....4
Methodology....4
Notes to readers....5

Detailed Findings....7

1. Use and storage of customer information....7
2. Company privacy practices....10
3. Managing privacy risks....17
4. Awareness and impact of federal privacy law....21

Appendix....26

1. Corporate profile of responding companies....26
2. Survey Questionnaire....27

List of Figures

Figure 1: Use of customer information collected by companies....7
Figure 2: Disclosure, collection, or use of customers' information....8
Figure 3: Methods used by companies to store personal information....9
Figure 4: Importance companies attribute to protecting customers' privacy....10
Figure 5: Importance companies attribute to protecting customers' privacy [over time]....11
Figure 6: Privacy policies....12
Figure 7: Features of privacy policies....13
Figure 8: Notifying customers about changes to privacy policies....14
Figure 9: Steps taken to inform customers about the company's privacy practices....14
Figure 10: Privacy policy practices....15
Figure 11: Privacy practices [over time]....16
Figure 12: Corporate policies in place to assess privacy risks....17
Figure 13: Privacy breach....18
Figure 14: Level of concern about a data breach....19
Figure 15: Level of concern about a data breach [over time]....19
Figure 16: Companies' awareness of responsibilities under privacy laws....21
Figure 17: Companies' awareness of responsibilities under privacy laws [over time]....22
Figure 18: Compliance with Canada's privacy laws....22
Figure 19: Level of difficulty complying with Canada's privacy laws....23
Figure 20: Compliance with Canada's privacy laws [over time]....24
Figure 21: Awareness of OPC resources....24

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 15-minute telephone survey was administered to 751 companies across Canada from January 12 to February 18, 2022. 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 (one-19 employees); medium (20-99 employees); and large (100+ employees). 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 ±3.6%, 19 times out of 20.

Contextual Note

The OPC has conducted this survey of Canadian businesses every two years since the baseline survey of 2011. For many of the issues explored, there is a decade of tracking data available to monitor businesses' privacy practices. The previous iteration of this survey was 2019, prior to the COVID-19 global pandemic. The pandemic has had well documented impacts on businesses in Canada[1] with measures adopted by firms to contain the spread of COVID-19 resulting in revenue declines, employee lay-offs and turnover, remote working, and reduced hours, among other impacts. This year, the survey was conducted at the height of the fifth wave of the pandemic (the Omicron variant) after nearly two years of pandemic-related restrictions. To manage Omicron, government-dictated restrictions on businesses increased once again in January 2022, with some jurisdictions reverting to lockdown protective measures.

The Omicron-related restrictions, and the pandemic more generally, affected this wave of the research: including the research design, in particular, the number of responses received and, quite possibly, the views of business representatives who participated in the survey. When businesses are preoccupied with pandemic-related impacts on their day-to-day operations, it is reasonable to assume that privacy responsibilities might not be top-of-mind. For instance, the reported decline in compliance with privacy practices may be more a reflection of limited recall or knowledge of

[1] See the Statistics Canada series: "COVID-19 in Canada— A One-year Update on Social and Economic Impacts"; Catalogue no. 11-631-X and "Impact of COVID-19 on small businesses in Canada"; Catalogue no. 45-28-0001).

these measures on the part of the respondent, or the fact that these matters have been given less priority amidst significant operational changes.

Key Findings

Many companies have a privacy policy in place, but fewer companies reported having one in 2022 than in 2019.

- Approximately six in 10 (59%) business representatives said their company has a privacy policy in place. This represents a small decline since 2019 when 65% of companies reported having such a policy in place. The likelihood of having a privacy policy is higher among larger businesses. Seventy-nine percent (79%) of large businesses surveyed said they have such a policy, compared to 66% of medium-sized businesses and 58% of small businesses.
- Among companies that have a privacy policy, most reported having a policy that explains in plain language the following: the purpose for which their company collects, uses, and discloses customers' personal information (84%); how their company collects, uses, and discloses this information (83%); and what personal information is being collected (78%). In addition, 72% of respondents said their company has a privacy policy that explains in plain language with which parties the personal information collected will be shared. Moreover, 66% have a policy that explains how customers' personal information is disposed, while 57% have a policy that explains the length of time the company keeps customers' personal information, and 51% have a policy that explains in plain language the risks of harm in the event of a data breach.
- Seventy percent (up from 51% in 2019) of respondents working for companies that have a privacy policy said their company makes its privacy information easily accessible to customers. Businesses with one employee (i.e., those who are self-employed) (78%), along with companies with five to nine employees (82%), are more likely than larger companies to make their privacy information easily accessible to customers. In addition, 43% of companies that have a privacy policy notify customers when making changes to their policy (up from 36% in 2019). The same proportion—43%—obtain consent from customers when making changes to their company's privacy practices (up from 34% in 2019).

Half or more of Canadian businesses have implemented most of the privacy compliance practices measured in the survey.

- Across all measures, compliance with privacy practices has decreased since 2019. Nearly six in 10 (57%) respondents said their company has a designated privacy officer (versus 62% in 2019). Following this, 51% said their company has developed and documented internal policies for staff that address privacy obligations (versus 55% in 2019), while the same proportion (51%) said their company has put in place procedures for responding to customer requests for access to their personal information (versus 60% in 2019). As well, 51% said their company has put in place procedures for dealing with customer complaints about the handling of their personal information (versus 58% in 2019). The likelihood of having implemented these practices increased with business size and was highest among large companies for nearly all measures.
- Fewer (34%) said their business regularly provides staff with privacy training and education (down from 39% in 2019).

More than nine in 10 companies have not experienced a privacy breach.

- Ninety-four percent of companies reportedly have not experienced a privacy breach (this is unchanged since 2019).
- There is no clear consensus when it comes to how concerned companies are about potential data breaches. A little more than one in four (28%) said they are concerned about a data breach (scores of six and seven), with 23% *extremely* concerned about a potential breach. On the other hand, 41% are not concerned about a potential breach (scores of one and two), including 30% that are not at all concerned about this.
- High concern (scores of six and seven) about a data breach has fluctuated over time, from a low of 24% in 2013 to a high of 37% in 2019. At 28%, high concern has declined significantly this year as compared to 2019.

Many companies are well aware of their responsibilities under privacy laws.

- Eighty-six percent of business representatives said their company is at least moderately aware of their privacy-related responsibilities, including 40% that are *extremely* aware of these responsibilities.
- Seventy-four percent of business representatives said their company has taken steps to ensure it complies with Canada's privacy laws. The likelihood of taking steps to ensure compliance increased with company size: 85% of large businesses, and 82% of medium-sized businesses reportedly have taken steps to ensure compliance compared to 73% of small companies have done so.
- One-third of businesses representatives surveyed said their company is aware that the OPC has information and tools to help companies comply with their privacy obligations. The likelihood of being aware of these resources was higher among medium-sized (41%) and large (56%) companies than among small companies (32%).

Contract Value

The contract value was $75,575.74 (including applicable tax).

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 *Communications Policy* 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.

Alethea Woods
President
Phoenix Strategic Perspectives Inc.

Introduction

Phoenix Strategic Perspectives (Phoenix SPI) was commissioned by the Office of the Privacy Commissioner of Canada (OPC) to conduct public opinion research (POR) 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; publicly report on the personal information-handling practices of public and private sector organizations; and conduct research into privacy issues.

The Privacy Commissioner of Canada is independent of government and reports directly to Parliament. Among other things, the Commissioner is responsible for enforcing the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies to commercial activities across Canada, except in Quebec, Alberta and British Columbia that each have their own law covering the private sector. 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 and what type of privacy policies and practices they have in place. The Office also needs to assess compliance with the law. To do so, it is also important that the OPC understands businesses' awareness and approaches to privacy protection. The OPC has regularly conducted quantitative surveys with businesses every two years.

The purpose of this research is to better understand the extent to which businesses are familiar with privacy issues and requirements, and to learn more about the types of privacy policies and practices that they have in place, as well as their privacy information needs. The research will also be used to inform and guide the OPC's outreach efforts with businesses.

Methodology

A 15-minute telephone survey was administered to 751 companies across Canada from January 12 to February 18, 2022. 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 businesses (1-19 employees); medium-sized businesses (20-99 employees); and large businesses (100+ employees). The sample source was Dun & Bradstreet (D&B Canada). Interviewing was conducted 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 ±3.6%, 19 times out of 20.

Note that the target sample size was intended to be 1,000 interviews, as with previous waves of this survey: 500 with small businesses, 300 with medium-sized businesses, and 200 with large

businesses. The target sample size was reduced to 750 interviews at the mid-point of the fieldwork to offset the lower contact rate encountered this year due, in large part, to workplace conditions resulting from the global pandemic. As mentioned, this survey entered the field at the height of the spread of the Omicron variant of COVID-19. In many jurisdictions across the country, businesses had employees working remotely to limit the spread of Omicron. This had a significant impact on the data collection because it made it much more difficult to reach eligible individuals.

The table below presents information about the final call dispositions for this survey, as well as the associated response rate.[2]

	Total
Total numbers attempted	**11,079**
Out-of-scope - Invalid	**1,764**
Unresolved (U)	**3,131**
No answer/Answering machine	3,131
In-scope - Non-responding (IS)	**5,365**
Language barrier	30
Incapable of completing (ill/deceased)	74
Callback (respondent not available)	1,970
Refusal	3,192
Termination	99
In-scope - Responding units (R)	**819**
Completed interview	751
Not eligible (not-for-profit)	52
Not eligible (did not know how many employees work at the company)	16
Response rate	**9%**

Contextual Note

The OPC has conducted this survey of Canadian businesses every two years since the baseline survey of 2011. For many of the issues explored, there is a decade of tracking data available to monitor businesses' privacy practices. The previous iteration of this survey was 2019, prior to the COVID-19 global pandemic. The pandemic has had well documented impacts on businesses in Canada[3] with measures adopted by firms to contain the spread of COVID-19 resulting in revenue declines, employee lay-offs and turnover, remote working, and reduced hours, among other impacts. This year, the survey was conducted at the height of the fifth wave of the pandemic (the Omicron variant) after nearly two years of pandemic-related restrictions. To manage Omicron, government-dictated restrictions on businesses increased once again in January 2022, with some jurisdictions reverting to lockdown protective measures. The Omicron-related restrictions, and the pandemic more generally, affected this wave of the research: both the research design and, quite possibly, the views of business representatives who participated in the survey.

[2] 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].

[3] See the Statistics Canada series: "COVID-19 in Canada—Updates on Social and Economic Impacts"; Catalogue no. 11-631-X and "Impact of COVID-19 on small businesses in Canada"; Catalogue no. 45-28-0001.

First, Omicron restrictions (as well as operational changes to businesses resulting from COVID-19 generally) made it much more difficult to reach eligible individuals at Canadian businesses. Business closures and telework, for example, resulted in a lower contact rate than in previous iterations of the survey and a higher rate of refusal among businesses (i.e., companies not transferring the interviewer to the individual at the company responsible for privacy-related functions). Lower contact rates have been experienced in other business-to-business research conducted during this timeframe. To offset the lower contact rate this year, the target sample size was reduced to 750 interviews at the mid-point of the fieldwork. The smaller sample size limited regional comparisons, but only resulted in a slightly higher margin of sampling error (±3.6%, 19 times out of 20 compared to ±3.1%, 19 times out of 20 for previous samples).

As well, the pandemic not only affected the research execution, but it also may have affected the survey findings in two ways. When businesses are preoccupied with very significant pandemic-related impacts on their day-to-day operations, it is reasonable to assume that privacy responsibilities might not be top-of-mind. Moreover, with employee layoffs and turnover, it would not be surprising if the person responsible for privacy compliance at some of the companies included in the survey sample was new to the position and therefore likely to be less familiar with a company's collection, storage and use of customers' personal information. Together, these two factors could be responsible for shifts in the survey data observed this year. Whether these are lasting changes, or the product of the environment in which the research was conducted, will remain unknown until this survey is conducted again in the future.

Notes to readers

- Results are compared to similar surveys conducted in 2011, 2013, 2015, 2017, and 2019.
- 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.

Detailed Findings

1. Use and storage of customer information

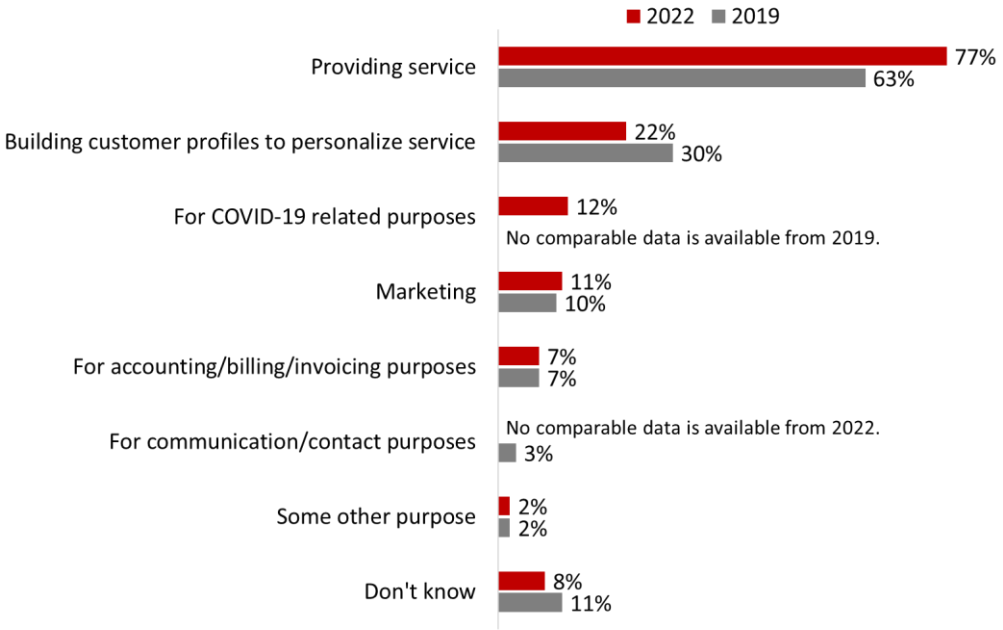
This section discusses how Canadian businesses use and store the personal information they collect from customers.

Many businesses use the personal information they collect to provide service

More than three-quarters of business representatives surveyed (77%) said their company uses the information it collects about customers to provide service. This could include, for example, collecting an email address to send an invoice. This is a significant increase since the last iteration of this survey when approximately two-thirds of companies reported using this information to provide service to customers (63% in 2019 versus 77% in 2022). In addition to providing service, 22% of respondents said their business uses this information to build profiles to personalize services for their customers (down from 30% in 2019). Fewer use it for marketing purposes (11%) or for accounting, billing or invoicing (7%).

New this year, 12% of the businesses surveyed use the personal information they collect about customers for purposes related to COVID-19. These businesses were more likely to sell only to consumers and to employ 100 or more employees. During the global pandemic, some businesses have been required to collect customer information to support public health tracing measures to limit the spread of COVID-19. This survey was administered during the height of the spread of the Omicron variant of COVID-19.

Figure 1: Use of customer information collected by companies



Q6. What does your business do with the personal information that it collects about customers? [Multiple responses accepted] Base in 2022 n=751; all respondents.

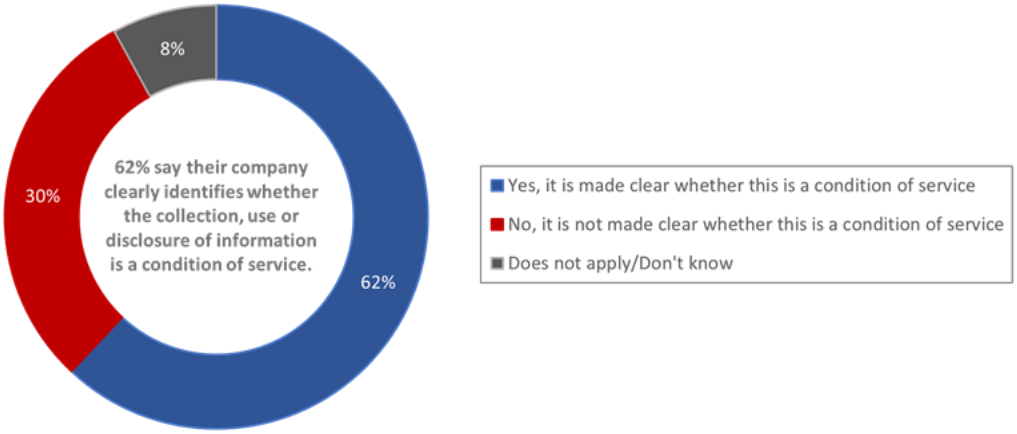
Companies selling to other business, or to both business **and** consumers, were significantly more likely than companies selling **only** to consumers to report using customers' personal information to provide service (81% and 82%, respectively). In contrast, just over two-thirds (68%) of businesses selling directly to consumers said they use personal information they collect about customers to provide service.

Many make clear whether collection, use, or disclosure of personal information is a condition of service

Approximately six in 10 (62%) companies that have a privacy policy said they clearly disclose to customers whether the collection, use, or disclosure of information is a condition of service. Conversely, 30% of respondents from these companies indicated they do not disclose this information. Eight percent of respondents said they did not know their company's practice in this area or this did not apply to their company.

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

Does your company make clear whether the collection, use or disclosure of information is a condition of service?



Q20c. 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=473; companies with privacy policies. [DK/NR: 4%].

Businesses based in western Canada are more likely than those in Ontario to make it clear to customers whether the collection, use or disclosure of information is a condition of service: 72% of respondents representing companies in the West said this compared to 55% of respondents representing companies in Ontario. Companies aware of their privacy obligations (64%) were more likely to reporting doing this than companies unaware of their obligations (31%).

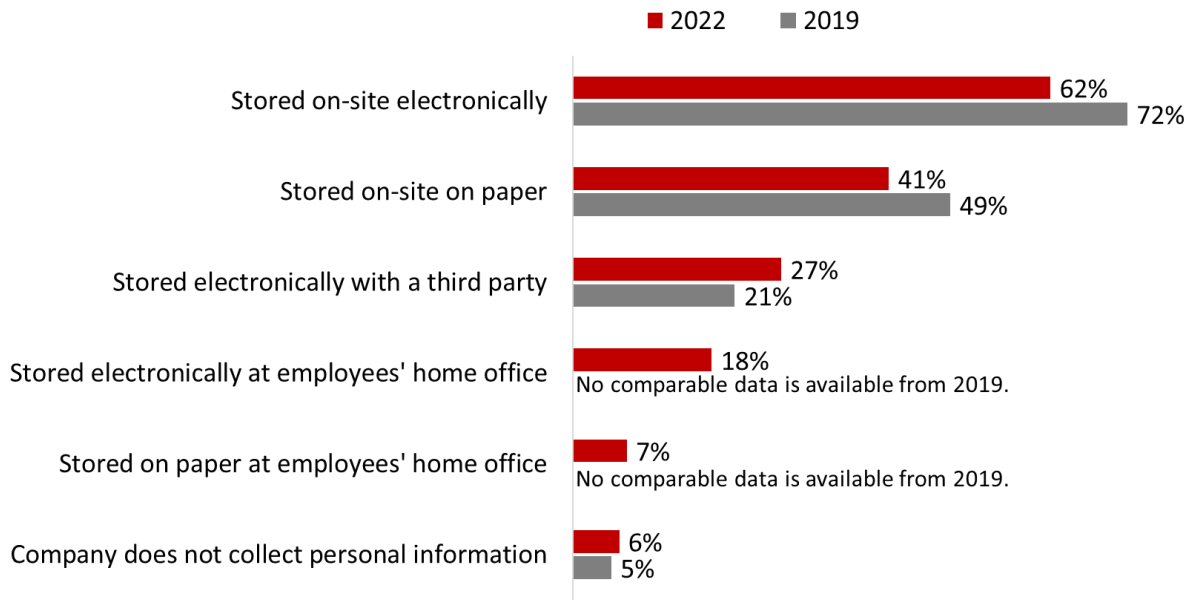
Many companies store personal information on-site electronically

Canadian businesses reported using a variety of methods to store customers' personal information. Heading the list is on-site electronic storage, mentioned by 62% of survey business representatives. The proportion of companies that said they store information on-site electronically has decreased 10 percentage points since 2019, when 72% reportedly stored information in this way. Following on-site electronic storage, 41% of business representatives said their company stores customers'

personal information on-site on paper (down from 49% in 2019), and 27% store this information electronically with a third party (up from 21% in 2019).

In addition to storing information on-site or via a third party, a number of companies said this information is stored electronically (18%), or on paper (7%), at employees' home offices. These two response options were added to the survey this year to reflect the public health environment at the time of the fieldwork.

Figure 3: Methods used by companies to store personal information



Q7. In which of the following ways does your company store personal information on your customers? Is the information…? [Multiple responses accepted] Base in 2022: n=751; all respondents.

Companies that sell to both consumers **and** businesses (71%) are more likely than those that sell directly to consumers **only** (54%) to store information electronically on-site.

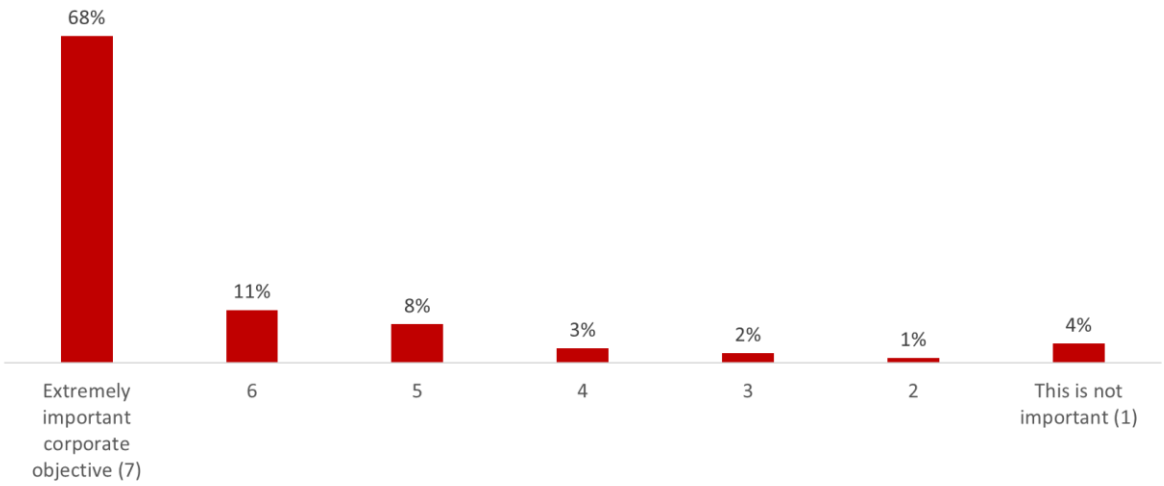
2. Company privacy practices

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 customer privacy

Business representatives were asked what level of importance their company attributes to protecting the personal information of their customers. More than nine in 10 (92%) respondents said their company considers the protection of customers' personal information to be at least moderately important. Specifically, nearly eight in 10 (79%) business representatives said their company considers the protection of customers' personal information to be of high importance (scores of six and seven), including 68% who said this is an extremely important corporate objective, and 13% of companies consider this to be of moderate importance. Very few business representatives (5%) indicated that protecting customers' personal information is not an important corporate objective for their company (scores of 1 and 2).

Figure 4: Importance companies attribute to protecting customers' privacy

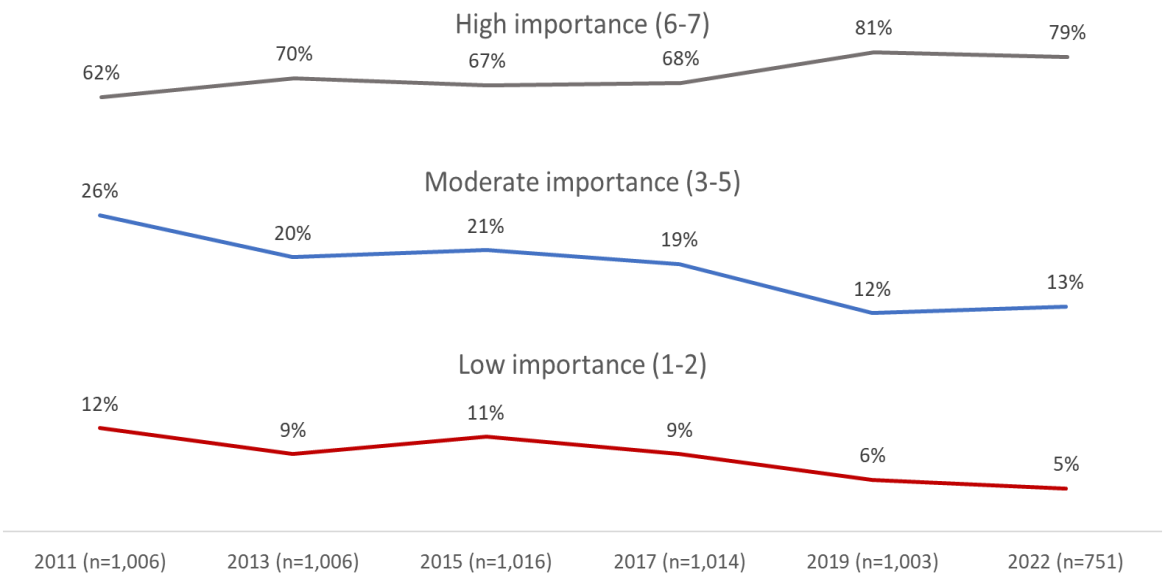


Q8. What importance does your company attribute to protecting your customers' personal information? Base: n=751; all respondents; [DK/NR=2%].

Companies aware of their privacy obligations (80%) were more likely than those unaware (31%) to attribute extreme importance to protecting their customers' personal information. In addition, companies that comply with PIPEDA (77% versus 46% of those that do not) or have a risk assessment policy in place (84% versus 60% of those that do not) were more likely to view this as something that is extremely important.

Over time, the importance companies attribute to protecting the personal information of customers has increased significantly from the baseline of 62% in 2011. The most significant increase was from 2017 to 2019 (an increase of 13 percentage points). This year, the proportion of companies attributing high importance to this is virtually the same as it was in 2019: 79% in 2022 versus 81% in 2019.

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



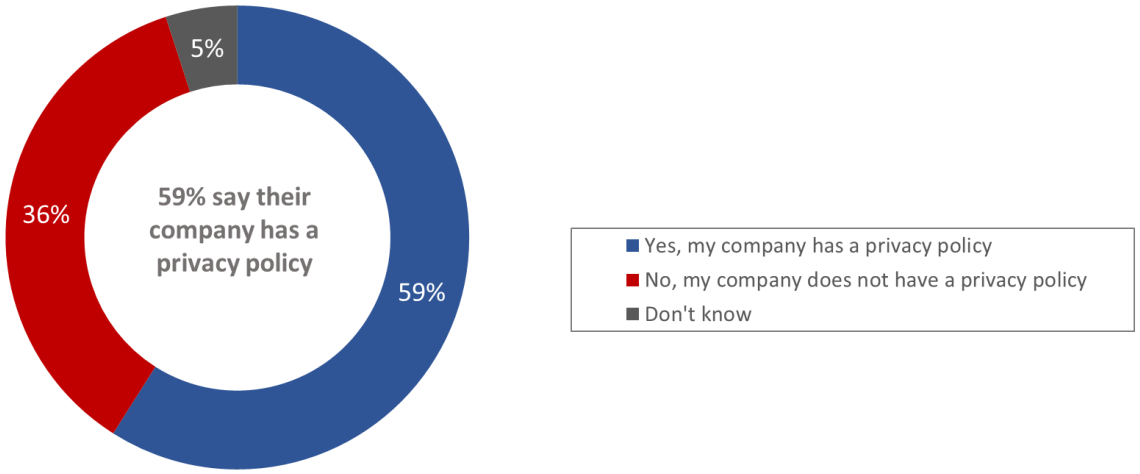
Q8. What importance does your company attribute to protecting your customers' personal information?

Over half have a privacy policy in place

Approximately six in 10 (59%) Canadian businesses surveyed said their company has a privacy policy. This represents a small decline over time, from 65% of companies reporting they have a privacy policy in 2019 to 59% in 2022. Conversely, 36% of business representatives said their company does not have a privacy policy (compared to 32% in 2019). The remainder (5%) are unaware if their company has such a policy.

As mentioned, the pandemic may have affected the survey findings, and specifically, those on compliance with privacy practices. When businesses are preoccupied with pandemic-related impacts on operations, it is reasonable to assume that privacy responsibilities might not be top-of-mind. Whether these are lasting changes, or the product of the environment in which the research was conducted, will remain unknown until this survey is conducted again in the future.

Figure 6: Privacy policies



Q18. Does your company have a privacy policy? Base: n=751; all respondents.

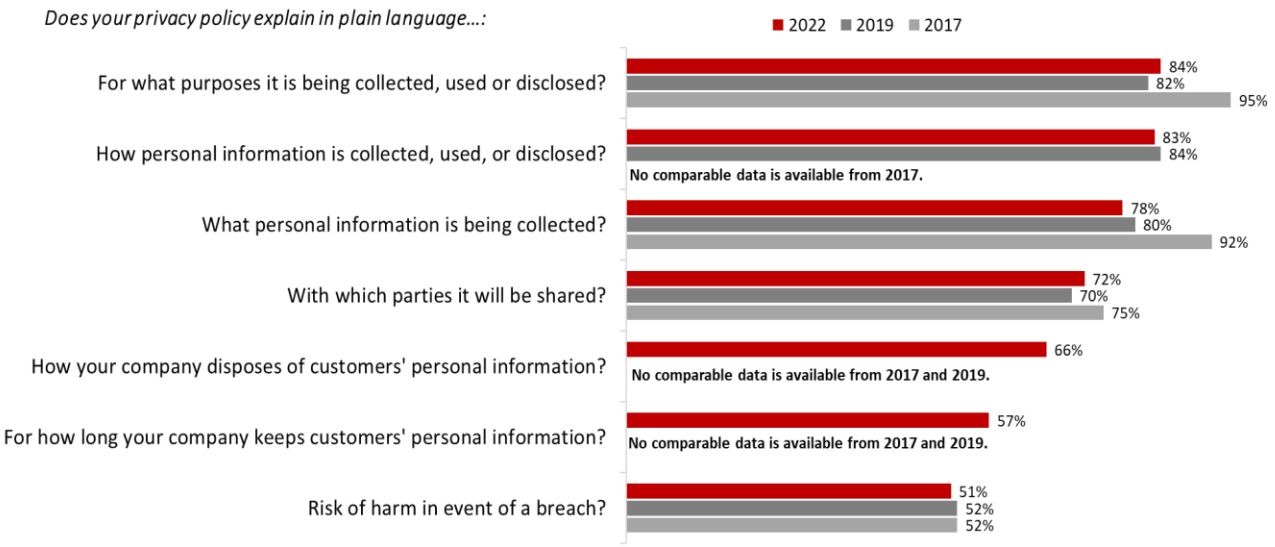
Companies based in Atlantic Canada (69%), Ontario (65%), and Western Canada (64%) are more likely than companies in Quebec (39%) to have a privacy policy. Moreover, the likelihood of having a privacy policy is higher among larger businesses. Seventy-nine percent (79%) of large businesses surveyed said they have such a policy, compared to 66% of medium-sized businesses and 58% of small businesses. In addition, companies aware of their privacy obligations (70% versus 25% of those unaware) and companies that have a risk assessment policy in place (86% versus 43% of those that do not) were more likely to report having a privacy policy.

Majority of those with a privacy policy explain a variety of features in plain language

Among companies that have a privacy policy (n=473), most said they have a policy that explains in plain language the following: the purpose for which their company collects, uses, and discloses customers' personal information (84%); how their company collects, uses, and discloses this information (83%); and what personal information is being collected (78%). In addition, approximately seven in 10 (72%) said they have a privacy policy that explains in plain language with which parties the personal information collected will be shared and half (51%) said they have a policy that explains in plain language the risks of harm in the event of a data breach.

This year respondents were also asked whether their company's privacy policy explains in plain language how their company disposes of customers' personal information and for how long their company keeps such information. In response, two-thirds (66%) of business representatives said their company's privacy policy explains how customers' personal information is disposed and nearly six in 10 (57%) reported that the company privacy policy explains the length of time the company keeps customers' personal information.

Figure 7: Features of privacy policies



Q19. Does your privacy policy explain in plain language…? Base: n=473; companies with privacy policies.

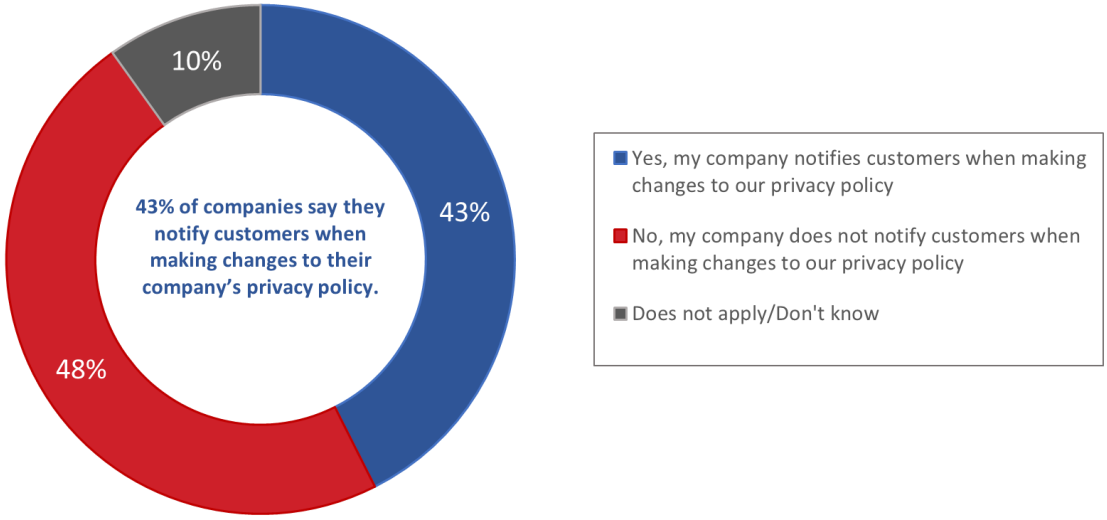
Differences between 2019 and 2022 were small, varying by no more than two percentage points, and not significant. Compared to 2017, however, fewer companies said their privacy policy explains in plain language to customers for what purpose their information is being collected, used or disclosed (84% compared to 95% in 2017) and what personal information is being collected (78% compared to 92%).

Quebec-based companies (62%) are more likely than businesses in Ontario (43%) to have a policy that clearly explains the risk of harm in the event of a breach. Additionally, businesses that sell **only** to consumers (88%) are more likely than companies that sell **only** to other businesses (70%) to have a policy that explains how they collect, use, or disclose of information. Companies aware of their privacy obligations and companies that have a risk assessment policy in place are more likely to report having a privacy policy that explains all of these of features in plain language. Differences by business size were not significant.

Four in 10 companies notify customers when making changes to their privacy policy

Forty-three percent (43%) of businesses that have a privacy policy said they notify customers when making changes to this policy. This represents an increase since 2019 when 36% of businesses reported that they notify customers of policy changes. In contrast, nearly half (48%) said they do not inform customers of these changes. The remaining 10% did 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



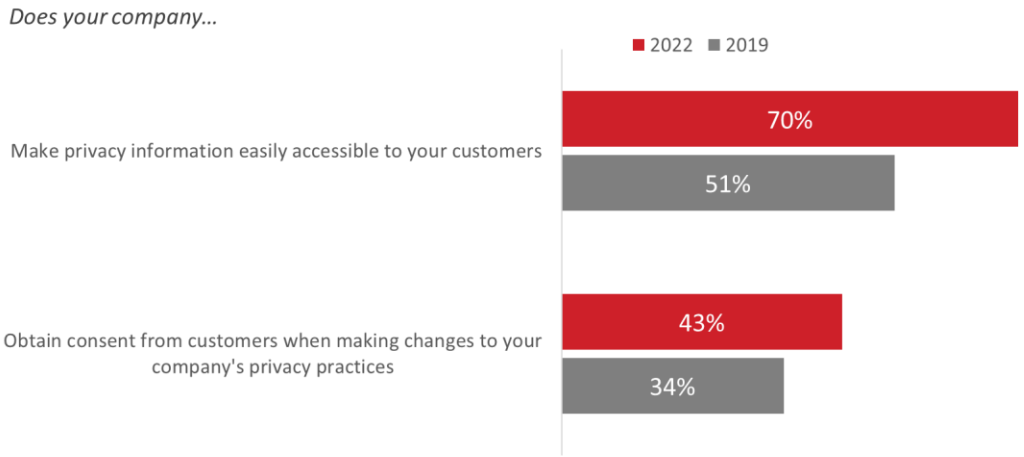
Q20a. Does your company do any of the following: Notify customers when making changes to your company's privacy policy. Base: n=479; companies with privacy policies. [DK/NR: 5%].

There are no subgroup differences to report.

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

Seven in 10 (70%) business representatives surveyed said their company makes privacy information easily accessible to customers. This represents a significant increase since 2019 when 51% of companies surveyed reported making this information easily accessible. Fewer respondents said their company obtains consent from customers when making changes to their corporate privacy practices—43% take this step when making changes to their privacy practices (up from 34% in 2019).

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



Q20b/20d. Does your company do any of the following…? Base: 2022 n=473; companies with privacy policies. [DK/NR: 7%].

Businesses with one employee (i.e., those who are self-employed) (78%), along with companies with five to nine employees (82%), are more likely than larger companies to make their privacy information easily accessible to customers.

Half or more have implemented most privacy compliance practices

Business representatives were asked whether their company has put in place a series of privacy practices. Half or more of respondents surveyed said their company has implemented the following privacy compliance practices: designated a privacy officer (57%); developed and documented internal policies for staff that address privacy obligations (51%); put in place procedures for responding to customer requests for access to their personal information (51%); and put in place procedures for dealing with customer complaints about the handling of their personal information (51%). Fewer, approximately one-third (34%), said their business regularly provides staff with privacy training and education.

Figure 10: Privacy policy practices

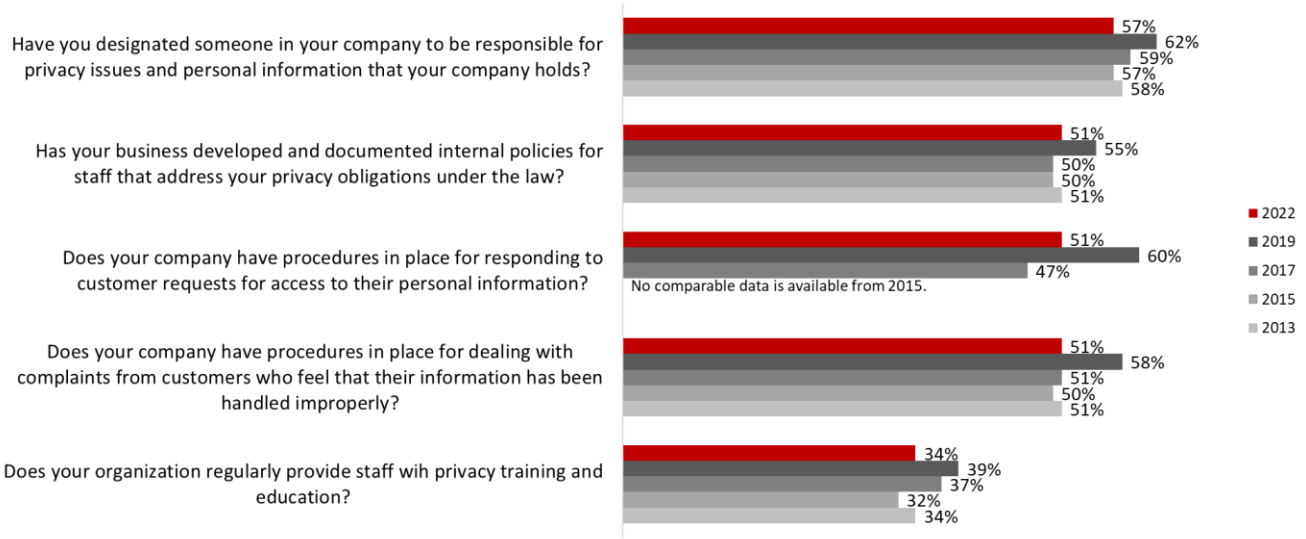
Q13 to Q17. Base: n=751; all respondents [DK/NR=2% to 6%]

Companies in Quebec were generally less likely to report having implemented these privacy compliance practices. Moreover, the likelihood of having implemented these practices increased with business size and was highest among large companies for nearly all measures. Companies aware of their privacy obligations and companies that have a risk assessment policy in place were more likely to report having implemented all of these privacy compliance practices.

Across all measures, compliance with privacy practices has decreased since 2019. While 62% of companies surveyed in 2019 reported that an individual within their company had been designated to be responsible for privacy issues, this is down five percentage points to 57% in 2022. Moreover, 60% of surveyed companies in 2019 said they had procedures in place for responding to customer requests for access to their information; this decreased nine percentage points to 51% in 2022. Additionally, 51% of businesses surveyed in 2022 said their company has procedures in place for dealing with complaints from customers; this is down from 58% in 2019.

Again, the pandemic may have affected the survey findings, and specifically, those on privacy practices. Whether these are lasting changes, or the product of the environment in which the research was conducted, will remain unknown until this survey is conducted again in the future.

Figure 11: Privacy practices [over time]



Q13 to Q17.

The results from this year are more consistent with those from 2017 and earlier than they are with 2019. Whether these are lasting changes, or the product of the pandemic environment in which the research was conducted, will remain unknown until this survey is conducted again in the future. However, as noted previously, the pandemic not only affected the research execution, but it also may be responsible for shifts in the survey data observed this year.

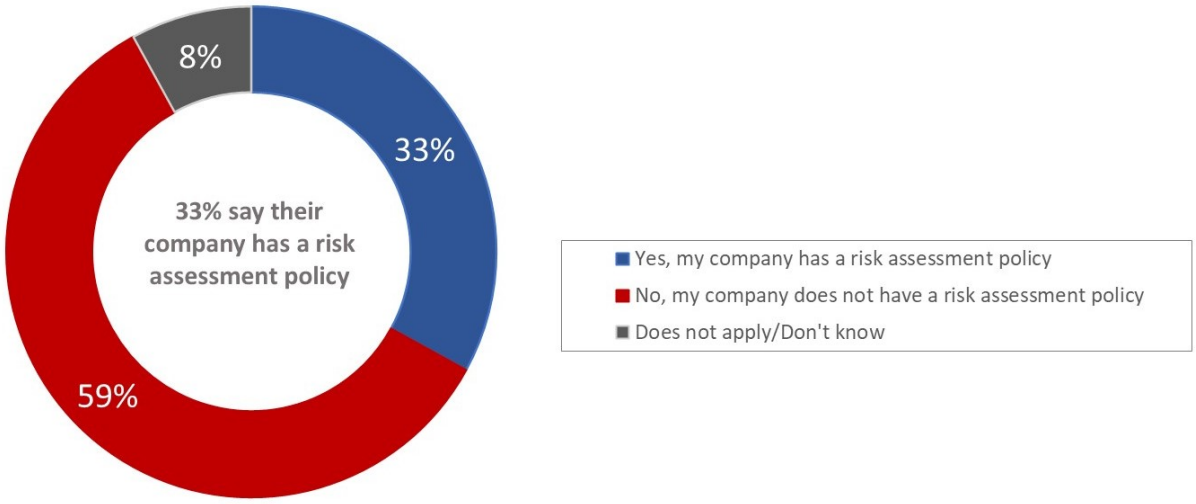
3. Managing privacy risks

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

One-third of companies have a policy in place to assess privacy risks

One-third (33%) of business representatives said their company has policies or procedures in place to assess privacy risks related to their business. This represents a slight decline since 2019 when 38% of companies reportedly had a corporate policy to assess privacy risks. More than half (59%) the business representatives surveyed said their company does not have any risk assessment policies or procedures in place. The rest (8%) did not know whether their company has any policies or procedures to assess privacy risks or volunteered that this does not apply.

Figure 12: Corporate policies in place to assess privacy risks



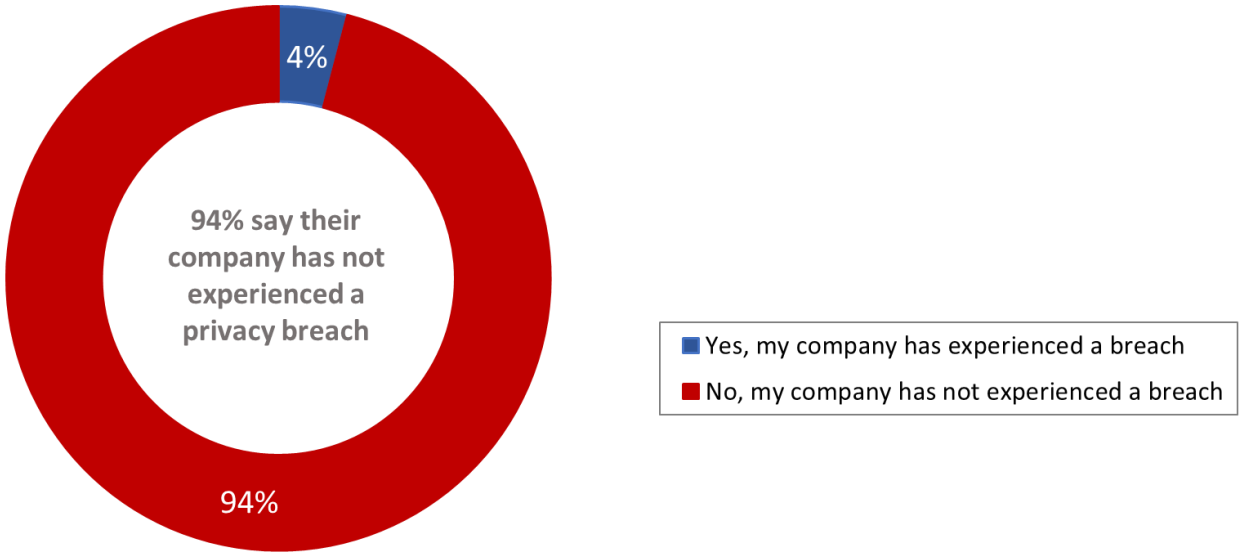
Q21. Does your company have any policies or procedures in place to assess privacy risks related to your business? Base: n=751; all respondents.

The likelihood of having policies or procedures in place to assess privacy risks was higher among larger companies. More specifically, 49% of large businesses, and 40% of medium-sized businesses said they had such policies or procedures in place, compared to approximately one-third of small businesses (32%). Companies aware of their privacy obligations (40%) were more likely than those unaware (10%) to report having policies or procedures in place to assess privacy risks related to their business.

Vast majority of companies have not experienced a privacy breach

The vast majority of business representatives (94%) said their company has not experienced a breach where the personal information of their customers was compromised. Consistent with data from previous years, very few (4%) said their company has experienced a privacy breach. The proportion of companies that have experienced a privacy breach ranges from 3% in 2010 to 4% in 2019.

Figure 13: Privacy breach



Q24. Has your company ever experienced a breach where personal information of your customers was compromised?
Base: n=751; all respondents. [DK/NR: 2%]

Small and medium-sized businesses (94% and 95% respectively) were more likely to have **not** experienced a privacy breach compared to 87% of large businesses who have **not** experienced a breach.

Among the companies that have experienced a breach (n=31), just over two-thirds (68%) said their company ensures that it keeps records of all data breaches involving customers' personal information. (Exercise caution when interpreting these findings because they reflect a very small sample base of n=31.) To address the situation, 44% of companies that experienced a breach notified affected individuals, 21% implemented a security system or enhanced their security, 16% followed corporate procedures (unspecified), 14% notified corporate head office, human resources or the company privacy department, and 11% reviewed their privacy policy or practices in response to the breach.

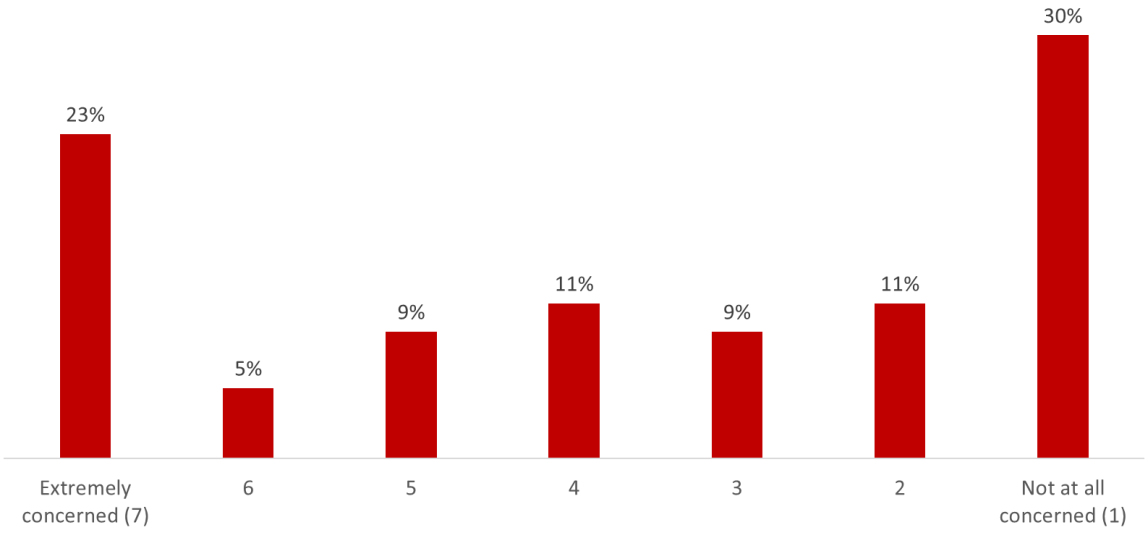
No clear consensus over level of concern of potential data breaches

Business representatives were asked to rate their level of concern about a data breach, where the personal information of their customers is compromised. 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.

In response, a little more than one in four (28%) said they are concerned about a data breach (scores of 6 and 7), with 23% extremely concerned about a potential breach. On the other hand, 41% said they are not concerned about a potential breach (scores of 1 and 2), including 30% that are not at all concerned about this.

Figure 14: Level of concern about a data breach

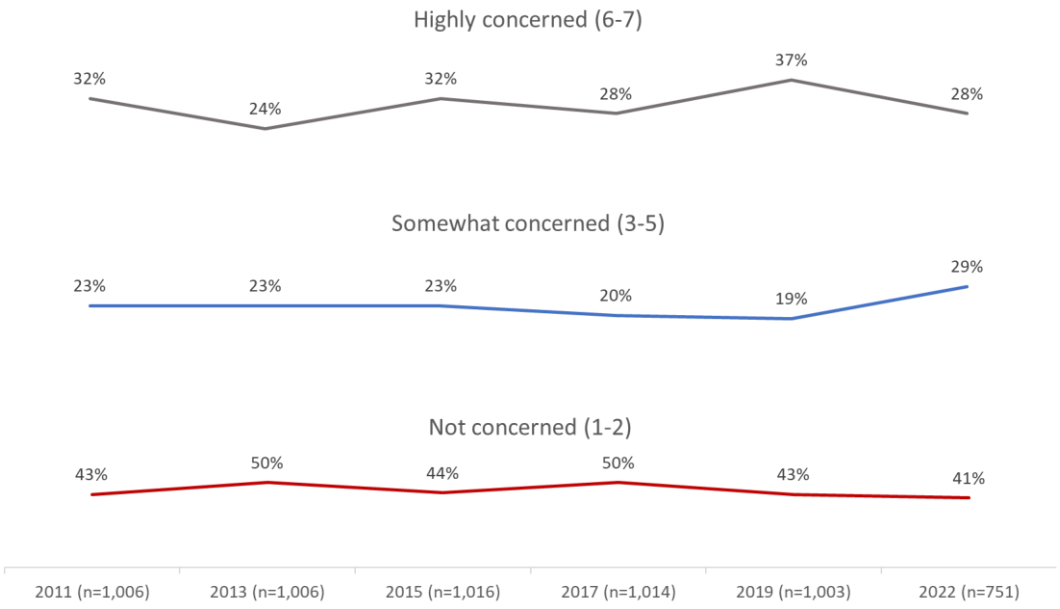


Q23. How concerned are you about a data breach, where the personal information of your customers is compromised? Base: n=751; all respondents [DK/NR=3%].

Quebec-based companies were particularly likely to say they are extremely concerned about a data breach (31% compared to the average of 23%). Along with Quebec-based companies, companies that sell to both consumers **and** businesses were also more likely to be extremely concerned (27%) as were companies aware of their privacy obligations (29%) and companies that have a risk assessment policy in place (41%).

High concern (scores of six and seven) about a data breach has fluctuated over time, from a low of 24% in 2013 to a high of 37% in 2019. At 28%, high concern has declined significantly this year as compared to 2019. As noted previously, the pandemic may be responsible for shifts in the survey data observed this year.

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



Q23. How concerned are you about a data breach, where the personal information of your customers is compromised?

4. Awareness and impact of federal privacy law

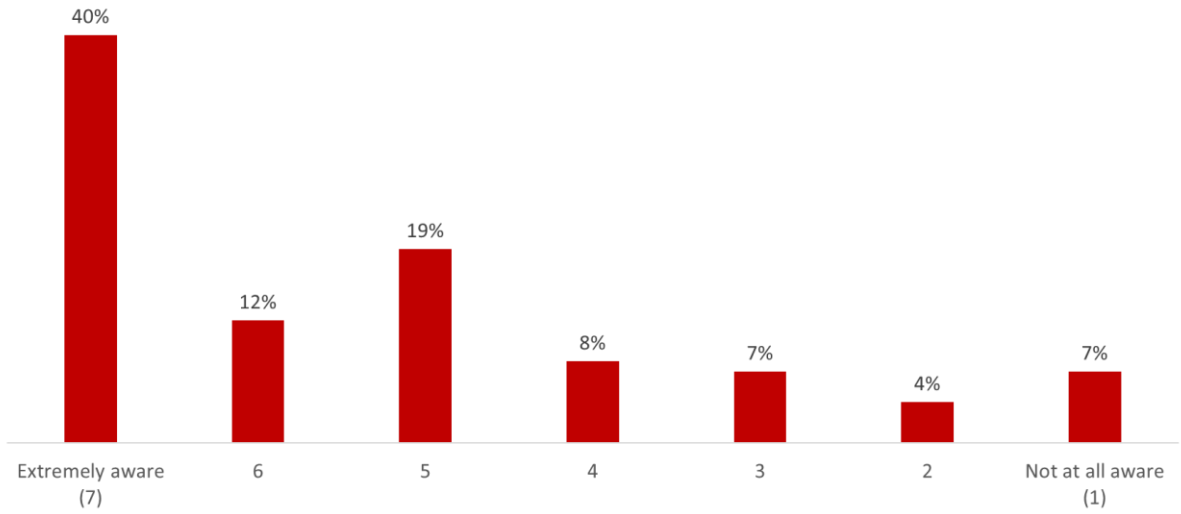
This section examines findings regarding companies' awareness of their responsibilities under privacy laws. Questions in this section were prefaced with the following description of Canada's privacy laws:

> 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 their responsibilities under privacy laws

Half of business representatives (52%) think their company is highly aware of its responsibilities under Canada's privacy laws (scores of six or seven), including 40% who said their company is extremely aware of these responsibilities. In addition, 34% rated their company as moderately aware of its privacy responsibilities (scores of three to five). Taken together, 86% of surveyed companies are at least moderately aware of their privacy-related responsibilities. Few (11%) rated their company's awareness as low (scores of one to two).

Figure 16: Companies' awareness of responsibilities under privacy laws

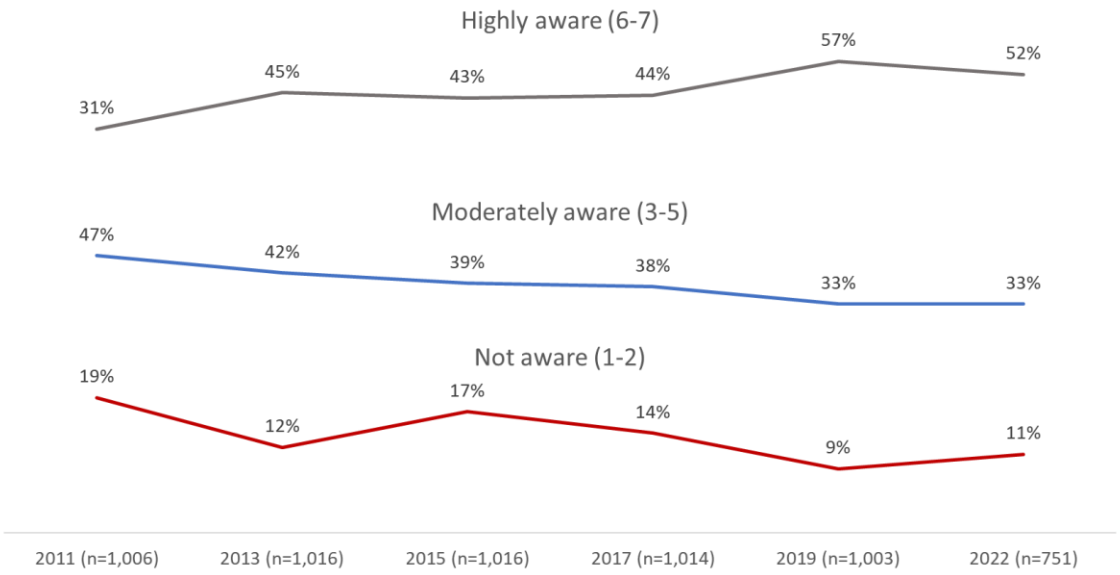


Q9. How would you rate your company's awareness of its responsibilities under Canada's privacy laws? Base: n=751; all respondents [DK/NR=4%].

There are no subgroup differences to report.

The proportion of business representatives who said their company is highly aware of its responsibilities under Canada's privacy laws has decreased slightly from the high of 57% reported in 2019.

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

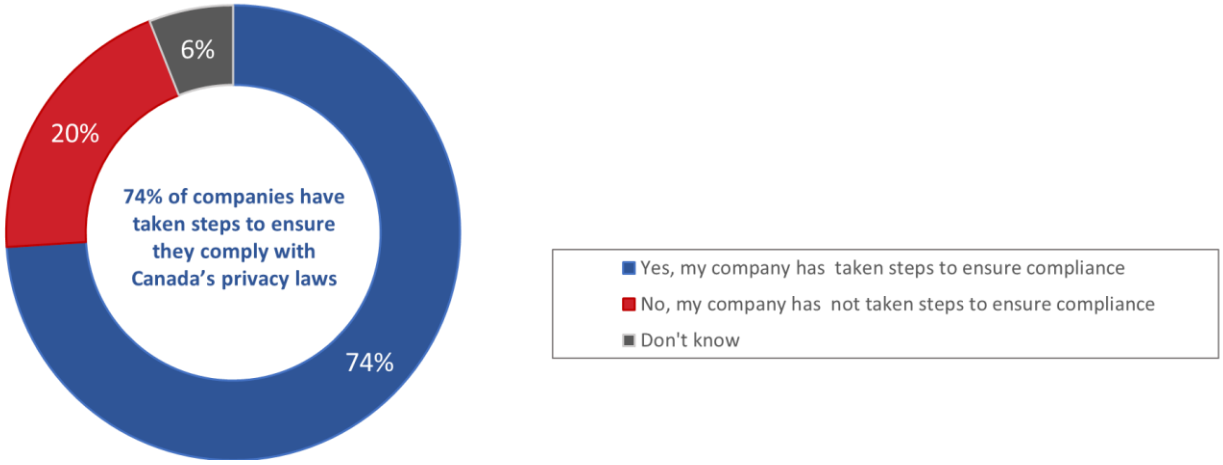


Q9. How would you rate your company's awareness of its responsibilities under Canada's privacy laws?

Three-quarters have taken steps to comply with privacy laws

Nearly three-quarters of business representatives surveyed (74%) said their company has taken steps to ensure it complies with Canada's privacy laws. Compliance has not changed in any significant way since 2019, and it remains higher than the 66% reported in 2017.

Figure 18: Compliance with Canada's privacy laws



Q10. Has your company taken steps to ensure it complies with Canada's privacy laws? Base: n=751; all respondents.

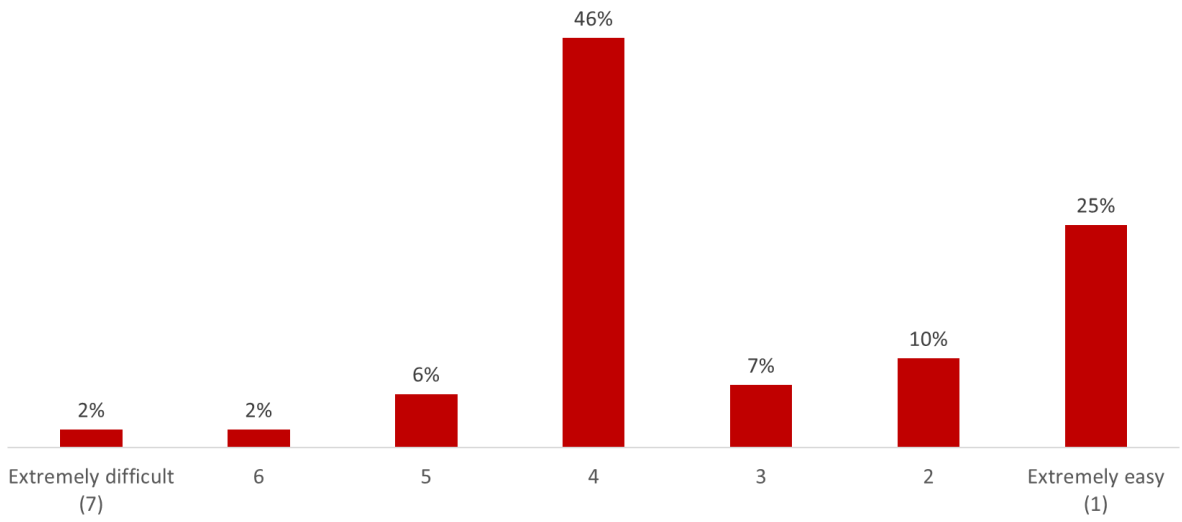
Businesses in Atlantic (86%) and western Canada (79%), as well as those in Ontario (78%), were significantly more likely to have taken steps to ensure compliance compared to businesses in Quebec (58%). In addition, the likelihood of taking steps to ensure compliance increased with the

size of the company: 85% of large businesses, and 82% of medium-sized businesses have taken steps to ensure compliance compared to 73% of small companies have done so. Companies that reported storing customers' personal information at an employee's or employer's home office in electronic format (59%) were less likely than companies that store this information on-site (77% on paper; 76% electronically) or off-site via a third party (79%) to report having taken steps to ensure compliance with Canada's privacy laws.

Half did not find it easy nor difficult to ensure compliance

More than nine in 10 (94%) companies that have taken steps to comply with Canada's privacy laws (n=584) found it moderately (scores of three to five) or extremely (scores of one to two) easy to bring their personal information handling practices into compliance. Very few business representatives (4%) said their company faced significant difficulties (scores of six and seven) ensuring compliance with Canada's privacy laws.

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

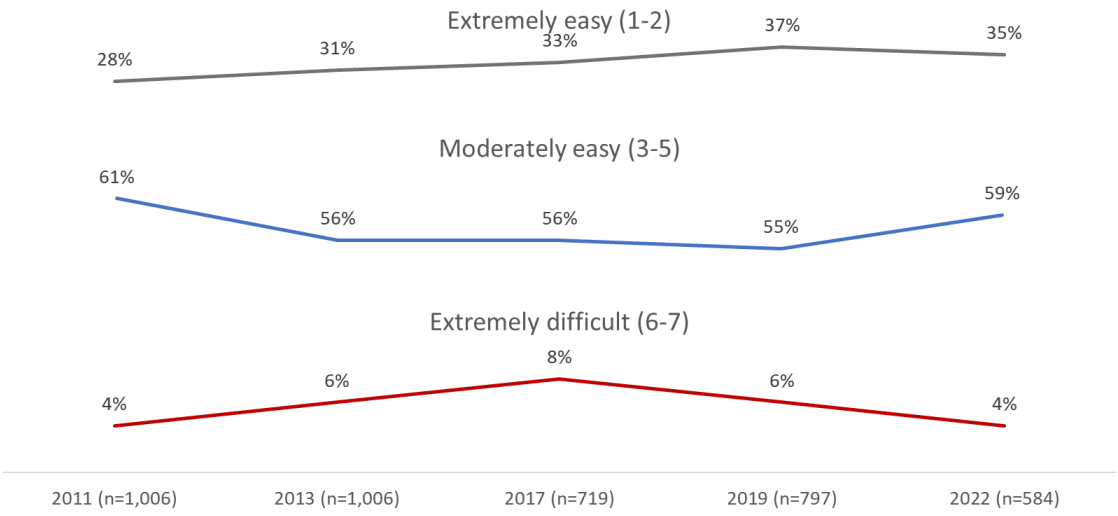


Q11. How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws? Base: n=584; companies that have taken steps to ensure compliance. [DK/NR=2%].

Businesses with two to four employees (40%) were more likely than those with 20 to 99 (22%) or 100+ (17%) employees to have found it extremely easy to bring their personal information handling practices into compliance with Canada's privacy laws.

The proportion of companies that find it extremely easy to bring personal information handling practices into compliance with Canada's privacy laws has steadily increased over time until reaching a high of 37% in 2019. Perceptions in this area remain virtually unchanged since 2019 (37% in 2019 versus 35% in 2022 said this was extremely easy).

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

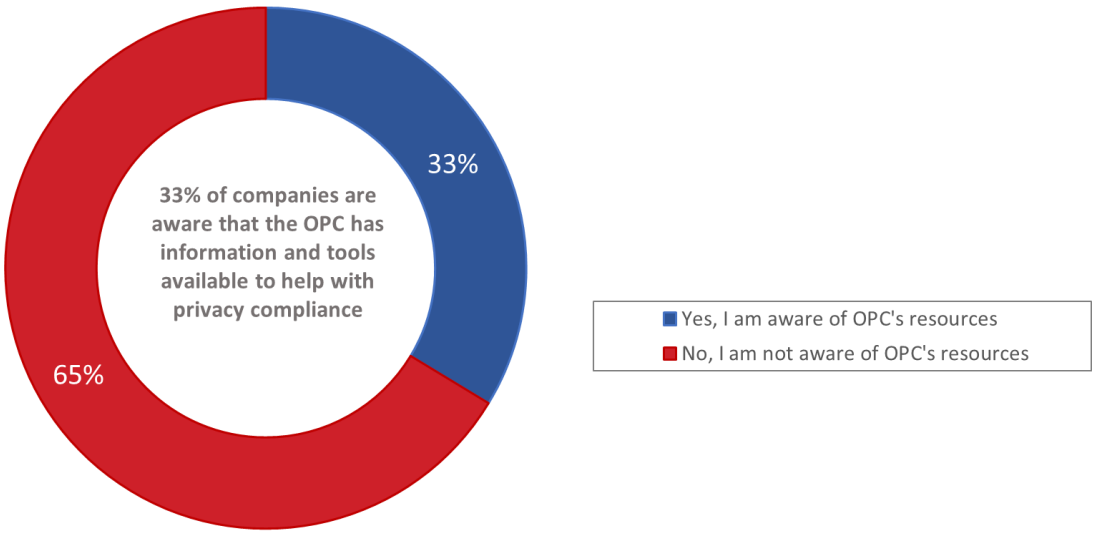


*Question differed in 2015. Data for 2015 is not represented in graph.
Q11. How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws?

One-third aware of resources provided by the OPC

Exactly one-third (33%) of businesses surveyed are aware that the OPC has information and tools to help companies comply with their privacy obligations. In contrast, approximately two-thirds (65%) of respondents said they are not aware of OPC's resources. Awareness of OPC's resources for businesses has not changed since 2019.

Figure 21: Awareness of OPC resources



Q12. 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=751 all respondents. [DK/NR: 2%].

Companies based in Ontario (39%) are more likely than those in Quebec (25%) to be aware that OPC has information and tools available to companies to help them comply with their privacy obligations. The likelihood of being aware of these resources was also higher among medium-sized (41%) and large (56%) companies than among small companies (32%).

Appendix

1. Corporate profile of responding companies

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

Customer type	Percent
Sells directly to consumers	36%
Sells directly to other businesses/organizations	22%
Sells directly to consumers and other businesses/organizations	41%
Other	1%

Use of subcontractors	Percent
Use subcontractors all the time	10%
Use subcontractors some of the time	48%
Never use subcontractors	41%
Use of subcontractors depends	1%
Do not know/refused	<1%

Involvement in 3P	Percent
Not currently involved in a public-private partnership	91%
Currently involved in a public-private partnership	3%
Previously involved in a public-private partnership	<1%
Do not know/refused	6%

Region	Percent
Atlantic Canada	7%
Quebec	23%
Prairies	7%
Alberta	14%
British Columbia	15%
Ontario (excluding the Greater Toronto Area)	19%
Greater Toronto Area	16%

Business size	Percent
1 employee (self-employed)	21%
2-4 employees	21%
5-9 employees	19%
10-19 employees	26%
20-99 employees	11%
100+ employees	2%

Revenues	Percent
Less than $100,000	16%
$100,000 to just under $250,000	12%
$250,000 to just under $500,000	12%
$500,000 to just under $1,000,000	11%
$1,000,000 to just under $5,000,000	18%
$5,000,000 to just under $10,000,000	6%
$10,000,000 to just under $20,000,000	2%
More than $20 million	2%
Don't know / no response	21%

2. 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 and background information

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

    01. It sells directly to individual consumers *
    02. It sells directly to other businesses/organizations
    03. It sells directly both to consumers and other businesses/organizations
    04. Other, please specify:
    05. DO NOT READ: Not for profit [THANK AND TERMINATE]

99. DO NOT READ: Don't know/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]

01. One (i.e., self-employed)
02. 2-4
03. 5-9
04. 10-19
05. 20-49
06. 50-99
07. 100-149
08. 150-199
09. 200-249
10. 250-299
11. 300-499
12. 500-999
13. 1,000-4,999
14. More than 5,000
99. DO NOT READ: Don't know/refusal [THANK AND TERMINATE]

3. To conduct business, does your company use subcontractors all the time, some of the time, or never?

01. All the time
02. Some of the time
03. Never
04. DO NOT READ: It depends
99. DO NOT READ: Don't know/refusal

4. Is your company currently involved in a public-private partnership, sometimes referred to as 3P or PPP contract?

01. No
02. Yes
03. DO NOT READ: The company has been, but no longer is
99. DO NOT READ: Don't know/refusal

Section 1. Customers' Personal Information

I'd like to begin by asking you about the personal information held by your company about your customers. By personal information, I mean information that could identify an individual. This includes things like a customer's name, email address, opinions, purchase history, or financial information, such as their credit card, but it can also include biometric data, such as fingerprints or voice prints, photos or videos, as well as chat or instant message histories.

To start,

5. From where does your company collect personal information? [READ LIST. ACCEPT ALL THAT APPLY]

    01. Directly from individual customers
    02. From another business, like a data broker, supply chain partner, or subcontractor
    03. From government
    04. From publicly available information sources, such as websites or social media

6. What does your business do with the personal information that it collects about customers? Is it used ...? [READ LIST. ACCEPT ALL THAT APPLY]

    01. to build customer profiles for marketing purposes
    02. to personalize services or products
    03. to provide service to customers – for example, collecting an email address to send an invoice
    04. for public health purposes related to Covid-19
    05. for some other purpose. If so, please specify:

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

    01. Stored on-site on paper
    02. Stored on-site electronically
    03. Stored off-site with a third-party, such as a cloud service
    04. Stored at an employees' home office on paper
    05. Stored at an employees' home office electronically

[VOLUNTEERED] Company does not store personal information about customers

8. 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.

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

9. 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.

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

01. Yes
02. No
03. [VOLUNTEERED] Don't know

11. [IF Q10=01] 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.

12. 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?

01. Yes
02. No
03. [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.

Section 3: Company Privacy Practices

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

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

01. Yes
02. No
03. [VOLUNTEERED] Don't know

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

01. Yes
02. No
03. [VOLUNTEERED] Don't know

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

01. Yes
02. No
03. [VOLUNTEERED] Don't know

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

01. Yes

02. No
03. [VOLUNTEERED] Don't know

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

01. Yes
02. No
03. [VOLUNTEERED] Don't know

18. Does your company have a privacy policy?

01. Yes
02. No
03. [VOLUNTEERED] Don't know

19. [IF Q18=01] Does your privacy policy explain in plain language...? [READ LIST]

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) For how long your company keeps customers' personal information?
f) The risk of harm to the individual, if any, in the event of data breach?
g) How your company disposes of customers' personal information once it is no longer needed?

RESPONSE OPTIONS:

01. Yes
02. No
98. [VOLUNTEERED] Does not apply
99. [VOLUNTEERED] Don't know

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

20. [IF Q18=01] Does your company do any of the following? [READ LIST]

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.
e) Explain how customers can raise a privacy concern or ask a privacy question
f) Explain how customers can request access to their personal information
g) Explain how customers can file a formal privacy complaint

RESPONSE OPTIONS:

01. Yes
02. No
98. [VOLUNTEERED] Does not apply
99. [VOLUNTEERED] Don't know

Section 4: Risk Assessment and Breaches

21. 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

    01. Yes
    02. No
    98. [VOLUNTEERED] Does not apply
    99. [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.

22. To what extent is your company prepared to respond to a data breach involving personal information? Please use a scale of 1 to 7, where 1 is not at all prepared to respond in the event of a privacy breach, and 7 is extremely prepared to respond.

23. 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.

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

    01. Yes
    02. No
    99. [VOLUNTEERED] Don't know

25. [IF Q24=01] Does your company ensure that it keeps records of all data breaches involving your customers' personal information?

    01. Yes
    02. No
    99. [VOLUNTEERED] Don't know

26. [IF Q24=01] What did your company do to address this situation? [DO NOT READ LIST. ACCEPT MULTIPLE RESPONSES]

    01. Notified individuals who are affected

02. Notified government agencies who oversee Canada`s privacy laws
03. Notified law enforcement
04. Followed proper procedure (general)
05. Notified company's head office, HR, or privacy department
06. Obtained legal counsel/took legal action
07. Resolved issue with individuals responsible for the breach (e.g., termination/reprimand of employee)
08. Obtained information from government (websites, 1-800 number)
09. Issued training or re-training for staff
10. Reviewed privacy policy or practices
11. Implemented security system or enhanced security
88. Other (specify):
99. Don't know

Section 5: Corporate Profile

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

27. 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]

    01. Accommodation and Food Services
    02. Administrative and Support, Waste Management and Remediation Services
    03. Agriculture, Forestry, Fishing and Hunting
    04. Arts, Entertainment and Recreation
    05. Construction
    06. Educational Services
    07. Finance and Insurance
    08. Health Care and Social Assistance
    09. Information and Cultural Industries
    10. Management of Companies and Enterprises
    11. Manufacturing
    12. Mining and Oil and Gas Extraction
    13. Other Services (except Public Administration)
    14. Professional, Scientific and Technical Services
    15. Public Administration
    16. Real Estate and Rental and Leasing
    17. Retail Trade
    18. Transportation and Warehousing
    19. Utilities
    20. Wholesale Trade
    88. Other. Please specify:

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

    01. Owner, President or CEO
    02. General Manager/Other Manager

03. IT Manager
04. Administration
05. Vice President
06. Privacy analyst/officer/coordinator
07. Legal counsel/lawyer
08. HR/Operations
88. Other: Specify

29. In which of the following categories would your company's 2020 revenues fall? [READ LIST. ACCEPT ONE RESPONSE]

01. Less than $100,000
02. $100,000 to just under $250,000
03. $250,000 to just under $500,000
04. $500,000 to just under $1,000,000
05. $1,000,000 to just under $5,000,000
06. $5,000,000 to just under $10,000,000
07. $10,000,000 to just under $20,000,000
08. More than $20 million