Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

2023-24 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: CW2334458
Award Date: 2023-10-18
Contract Value: $72,252.20 (including applicable tax)
Delivery Date: 2024-03-06

Registration Number: POR No.: 073-23

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

Ce rapport est aussi disponible en français.

Canada

2023-24 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 2024

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 800 representatives of Canadian businesses between November 21 and December 21, 2023.

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

Catalogue Number: IP54-96/2024E-PDF

International Standard Book Number (ISBN): 978-0-660-71662-6

Related publications (POR registration number: POR 073-23):
Catalogue number (Final report, French): IP54-96/2024F-PDF
ISBN: 978-0-660-71663-3

Aussi offert en français sous le titre : « Sondage de 2023 mené auprès des entreprises canadiennes concernant les enjeux liés à la protection des renseignements personnels ».

Table of Contents

List of Figures

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 800 companies across Canada from November 21 to December 21, 2023. 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 (1-19 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 ±3.5%, 19 times out of 20.

Key Findings

Most Canadian companies are aware of their responsibilities under Canada's privacy laws and have taken steps to ensure they comply with these laws.

- Eighty-eight percent of business representatives said their company is at least moderately aware of its privacy-related responsibilities, including close to half (47%) that are highly aware of these responsibilities. Since 2019, the proportion of companies highly aware of their privacy-related responsibilities has steadily declined, from 57% in 2019, to 52% in 2022, to 47% this year.
- Three-quarters (76%) of business representatives 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 baseline of 66% reported in 2017. The likelihood of taking steps to ensure compliance increased with company size, from 75% of small businesses to 94% of large businesses.
- Ninety-three percent of companies that have taken steps to comply with Canada's privacy laws found it moderately or extremely easy to bring their personal information handling practices into compliance. The proportion of companies that found it very easy to comply has increased significantly this year, from 35% in 2022 to 56% in 2023.
- Underscoring the ease with which companies were able to comply with Canada's privacy laws, few challenges with respect to compliance were identified: lack of knowledge (6%) or understanding of privacy laws (6%), difficulty integrating privacy measures with existing

systems/processes (5%), lack of internal resources or a dedicated privacy team (4%), lack of technical skills (2%), and the financial cost of compliance (2%).

Awareness of the OPC's information and tools for businesses has increased significantly, but only one in four have used these resources to comply with privacy obligations.

- Four in 10 (41%; up from 33% in 2022) surveyed business representatives are aware that the OPC has information and tools to help companies comply with their privacy obligations. Self-reported use of these resources has increased this year, from 17% in 2013 to 26% in 2023, but use continues to fall short of awareness due, at least in part, to lack of need, which was mentioned by 31% of those knew of the OPC's resources but who said their company had not used them.

Half or more of Canadian businesses have implemented most of the privacy practices measured in the survey. Implementation is virtually unchanged since 2022, when a decline was reported across all measures. In addition to fulfilling their privacy-related responsibilities, many companies also reported using measures to safeguard personal information.

- Half or more of business representatives said their company has implemented the following privacy practices: designated a privacy officer (56%); put in place procedures for dealing with customer complaints about the handling of personal information (53%) as well as for responding to customer requests for access to their personal information (50%); and developed internal policies for staff that address privacy obligations (50%). Exactly one-third (33%) said their business regularly provides staff with privacy training and education. The likelihood of having implemented these practices increased with business size and was highest among large companies for nearly all measures.
- New this year, respondents were asked about security measures used to safeguard customer and employee information. Approximately eight in 10 business representatives said their company requires passwords to access accounts (83%) and controls employee access to electronic files (79%). Roughly half reported that their company uses multi-factor authentication (53%) and encrypts stored data (49%), while exactly one-third (33%) encrypt communications.

Many companies have a privacy policy in place, but over time, fewer companies report having one. Most companies that have a privacy policy use plain language to explain their practices with respect customers' personal information.

- Just over half (55%) of the business representatives surveyed said their company has a privacy policy. Over time, the proportion of companies with a privacy policy has declined, from a high of 65% in 2019, to 59% in 2022, to 55% this year. The likelihood of having a privacy policy is higher among larger businesses. Nearly nine in 10 (87%) large businesses have such a policy, compared to two-thirds (67%) of medium-sized businesses and approximately half (53%) of small businesses.
- When looking at whether companies have plain language disclosures in their privacy policies, the 2023 results are generally consistent with previous years. Most privacy policies explain in plain language the following: the purpose for which personal information is collected, used, and disclosed (85%); which personal information is being collected (81%); and the methods by which the company collects, uses, and discloses this information (80%). In addition, many said their company's policy explains with which parties the information collected will be shared (70%) and how it will be disposed (62%), while just over half (55%) said their policy explains the

risks of harm in the event of a data breach. The one noteworthy change over time has been the proportion of companies that disclose, in plain language, for how long customers' personal information is kept. This increased from 57% in 2022 to 67% in 2023.

- Business representatives who said their company has a privacy policy were also asked whether their company communicates with customers about different aspects of its privacy practices. The most significant year-over-year change includes a decline in the proportion of companies that explain how customers can file a formal privacy complaint (from 60% in 2022 to 49% in 2023), that make privacy information easily accessible (from 70% in 2022 to 60% in 2023), and that explain how customers can request access to personal information (from 69% in 2022 to 59% this year).

Few companies have experienced a data breach, but half are prepared to respond to a breach involving personal information.

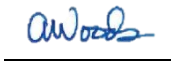
- Ninety-three percent of companies reportedly have not experienced a privacy breach. The incidence of reported data breaches has been consistent for the last decade (4% in 2013, 2019, and 2022 and 6% in 2023).
- More than eight in 10 (84%) respondents said their company is at least somewhat prepared to respond to a data breach involving personal information, including close to half (46%) who said their company is highly prepared for such an event.

Contract Value

The contract value was $72,252.20 (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.

Mandated by Parliament to function 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 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 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 800 companies across Canada from November 21 to December 21, 2023. 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 ±3.5%, 19 times out of 20.

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

	Total
Total numbers attempted	**12,598**
Out-of-scope - Invalid	**2,226**
Unresolved (U)	**5,759**
No answer/Answering machine	5,759
In-scope - Non-responding (IS)	**5,365**
Language barrier	74
Incapable of completing (ill/deceased)	91
Callback (respondent not available)	1,722
Refusal	3,473
Termination	128
In-scope - Responding units (R)	**938**
Completed interview	800
Not eligible (not-for-profit)	127
Not eligible (did not know how many employees work at the company)	11
Response rate	**8%**

Notes to readers

- Results are compared to similar surveys conducted in 2011, 2013, 2015, 2017, 2019 and 2022.
- 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.
    - Where subgroup differences are not discussed for certain questions, it can be assumed that there were no significant differences of note.
    - When reporting subgroup variations, if one or more categories in a subgroup are not mentioned in a discussion of differences (for example, if two out of four 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, pertain to a subgroup sample size of more than n=30 are, or are part of a pattern or trend are discussed in the report.
- The survey questionnaire is appended to the report.

Detailed Findings

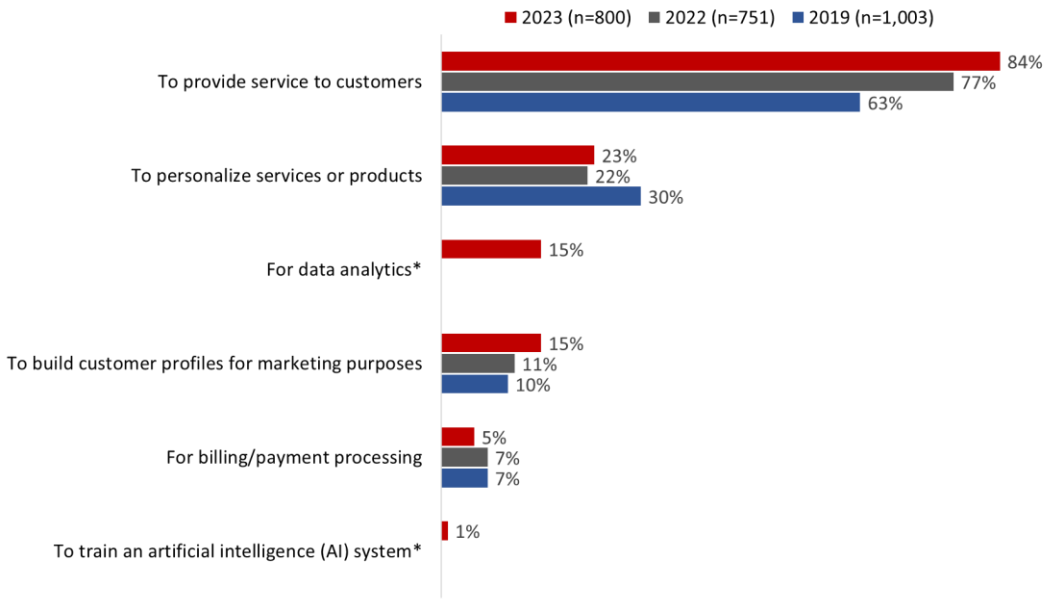
1. Customers' personal information

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

Most businesses use the personal information they collect to provide service

More than eight in 10 business representatives surveyed (84%) 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. Use of customers' personal information to provide service has steadily increased, from 63% in 2019 to 84% this year. Unchanged from 2022, almost one-quarter (23%) of respondents said their company uses this information to personalize services or products. Fifteen percent each reported that their company uses customers' personal information for data analytics (15%) and to build customer profiles for marketing purposes (15%; up from 11% in 2022). Fewer said their company uses this information for billing or payment processing (5%) and to train an aritificial intelligence (AI) system (1%).

Figure 1: Use of customer information collected by companies



Q3. What does your company do with the personal information that it collects about customers? Is it used...? Multiple responses accepted. Base: all respondents. *New categories this year.

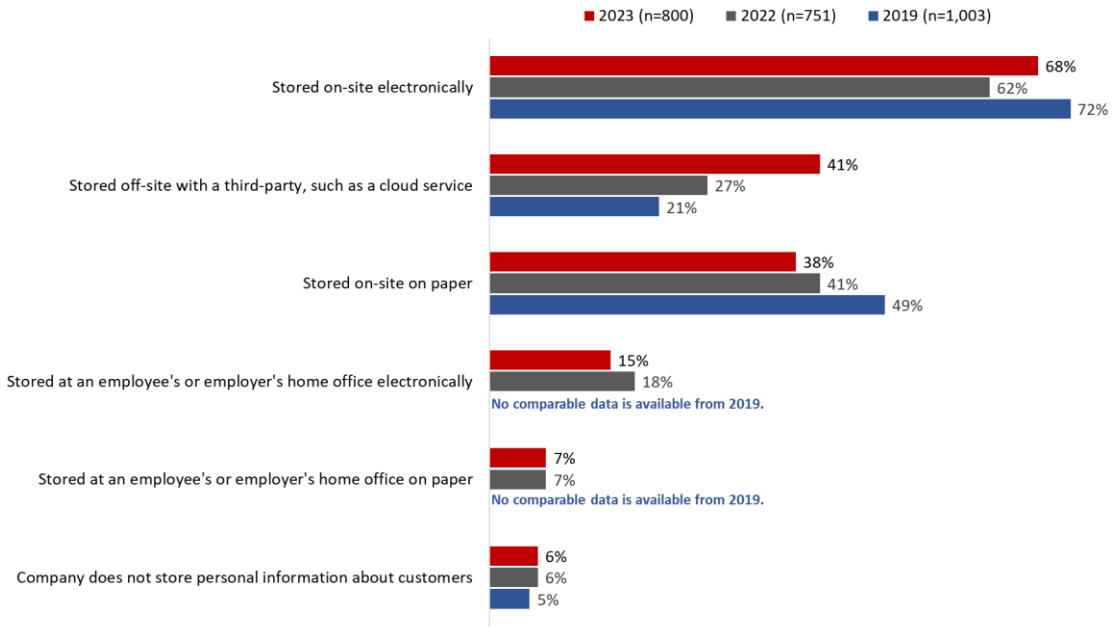
Companies selling to other businesses, or to both business **and** consumers, were significantly more likely than companies selling **only** to consumers to report using customers' personal information to provide service (94% and 89%, respectively) compared to 63% of businesses selling directly to consumers).

Many companies store personal information on-site electronically

Canadian businesses reported using a variety of methods to store customers' personal information. Consistent with previous years, on-site electronic storage topped the list, mentioned by 68% of survey business representatives (up from 62% in 2022). Following on-site electronic storage, 41% of business representatives said their company stores customers' personal information off-site with a third-party, such as a cloud service.[1] Use of third parties for electronic storage has increased significantly this year, from 27% in 2022 to 41% in 2023. Finally, almost as many (38%; virtually unchanged from 41% in 2022) respondents said their company stores this information on-site on paper.

In addition to storing information on-site or via a third party, a number of companies said this information is stored electronically (15%), or on paper (7%), at employees' or employers' home offices.

Figure 2: Methods used by companies to store personal information



Q4. How does your company store the personal information of customers? Is the information…? Multiple responses accepted. Base: all respondents.

Businesses in western Canada (79%) were the most likely to store customers' personal information on-site electronically. In addition, the likelihood of storing data on-site electronically increased with business size, from 48% of sole proprietorships to 74% of businesses with 20 or more employees. Large (17%) and small (15%) businesses were more likely than medium-sized businesses (7%) to store customers' personal information electronically at an employee's or employers' home office.

The likelihood of using a third-party for storage, such as a cloud service, was higher in Atlantic Canada (57%), Ontario (45%) and western Canada (43%) compared to Quebec (24%), as well as among companies that sell to businesses only (47%) or to businesses and consumers (45%)

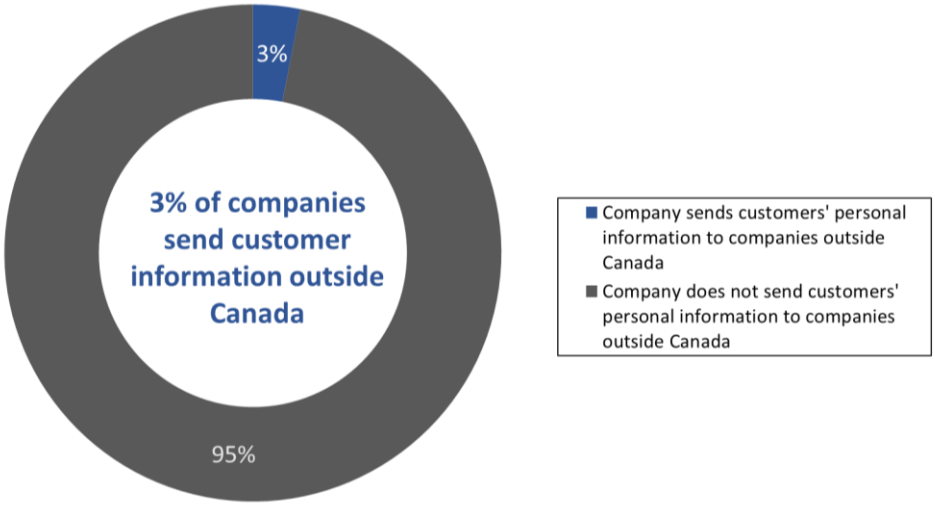
[1] Among companies that use off-site, third-party storage, the vast majority (90%) said their company does not send customers' personal information to companies outside Canada for processing, storage, or other purposes.

compared to those that sell exclusively to consumers (28%). Use of third-party storage services also tended to be higher among companies operating in core industries or sectors of the economy[2], such as professional, scientific and technical services, finance and insurance, information and cultural industries, and arts, entertainment and recreation.

Very few companies send customer information outside Canada

Three percent of surveyed business representatives said their company sends customers' personal information to companies outside Canada for processing, storage, or other purposes. The vast majority (95%) do not.

Figure 3: Cross-border movement of customers' personal information



Q5. Does your company send customers' personal information to companies outside Canada for processing, storage or other purposes? Base: n=800; all respondents. Don't know: 2%

Among companies that send customers' personal information outside Canada (n=26)[3], two-thirds (67%) of the business representatives surveyed said their company informs customers that their personal information may leave Canada. The rest of the companies do not do this, or the respondent did not know. Companies that inform customers (n=13)[2] are most likely to use the corporate privacy policy to inform customers, followed by the Terms of Service agreement and, finally, express consent.

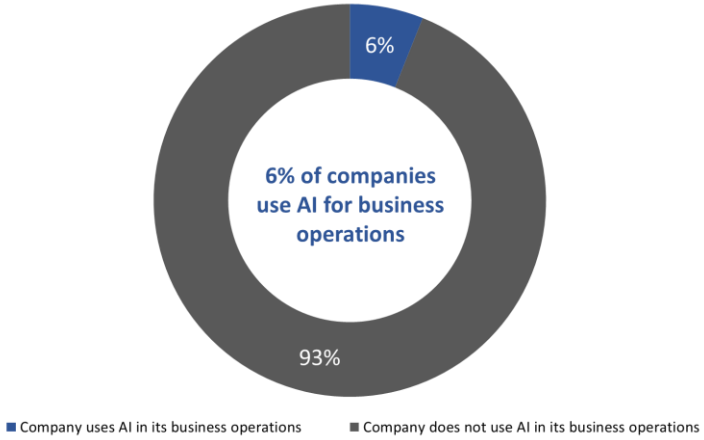
[2] No percentages are provided due to small sample sizes.
[3] Exercise caution when interpreting due to the very small sample sizes, n=26 and n=13.

2. Technology

Limited use of AI for business operations

Six percent of business representatives surveyed reported that their company uses AI for business operations. The vast majority (93%) do not.

Figure 4: Use of AI for business operations

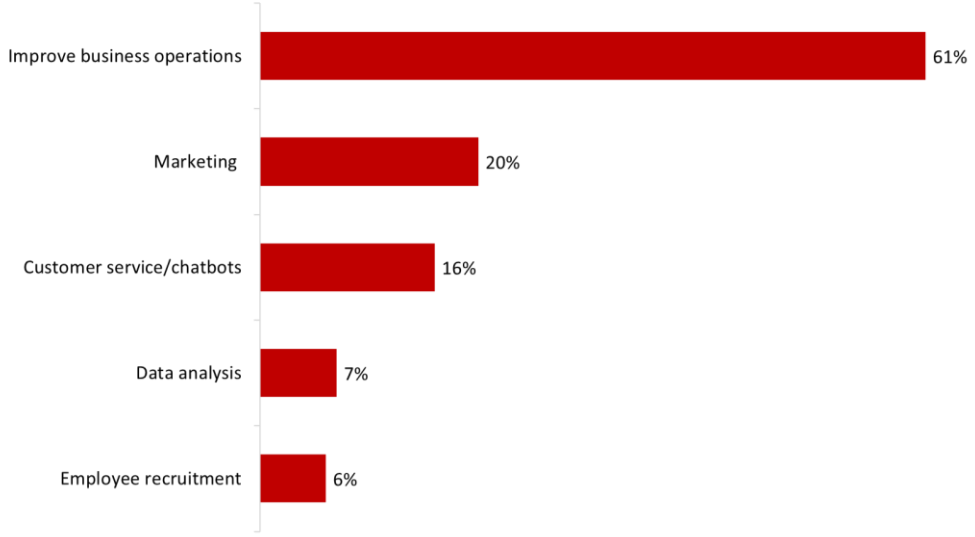


Q8. Does your company use AI for business operations? Base: n=800; all respondents. Don't know: 1%

Improve business operations – top use for AI

Among companies that use AI for business operations (n=39)[4], the majority (61%) are using it to improve business operations.

Figure 5: How AI is used in business operations



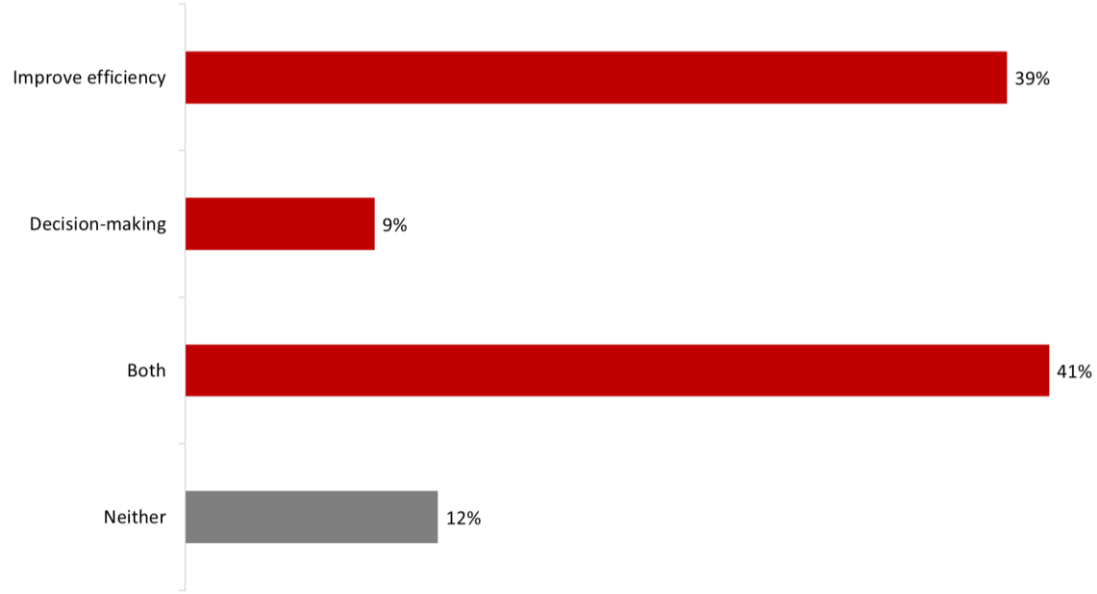
Q9. How is your company using AI in its business operations? Multiple responses accepted Base: n=39; those using AI in their business operations. Don't know: <1%.

[4] Exercise caution interpreting this finding due to the relatively small sample size, n=39.

4 in 10 use AI to improve efficiency and to make decisions

Four in ten (41%) respondents who reported that their company uses AI in its business operations said AI is being used to improve efficiency and for decision-making.[5] Almost as many (39%) said their company is using AI to improve efficiency but not for decision-making. Few companies are currently using AI for decision-making but not to improve efficiency. Just over one in 10 (12%) surveyed business representatives said their company is using AI in business operations for neither of these purposes.

Figure 6: What AI is being used for by companies



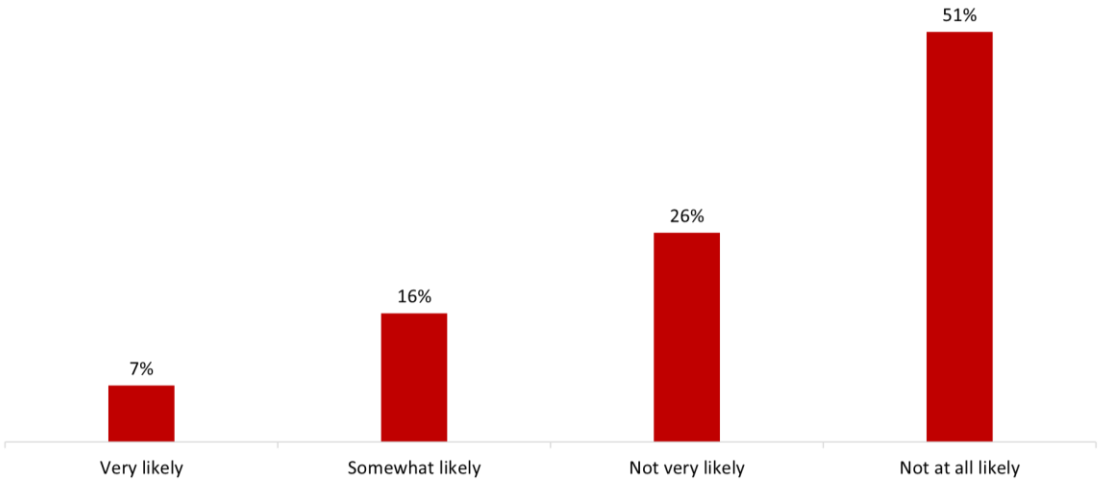
Q10. Is AI being used by your company to improve efficiency, for decision-making, or for both? Base: n=39; those using AI in their business operations. Don't know: <1%

One-quarter of companies not using AI are somewhat or very likely to do so in the next 5 years

Nearly one-quarter of those surveyed who said their company does not currently use AI (n=761) reported that it is somewhat (16%) or very (7%) likely that their company will use AI for business operations in the next five years. In contrast, just over three-quarters of respondents said it is not very (26%) or not at all (51%) likely that their company will use AI in the next five years.

[5] Exercise caution interpreting this finding due to the relatively small sample size, n=39.

Figure 7: Likelihood of using AI for business operations in the next 5 years



Q12. How likely is it that your company will use AI for business operations in the next five years? Base: n=761; those who do not currently use AI for business operations. Don't know: <1%

3. Canada's privacy laws and compliance

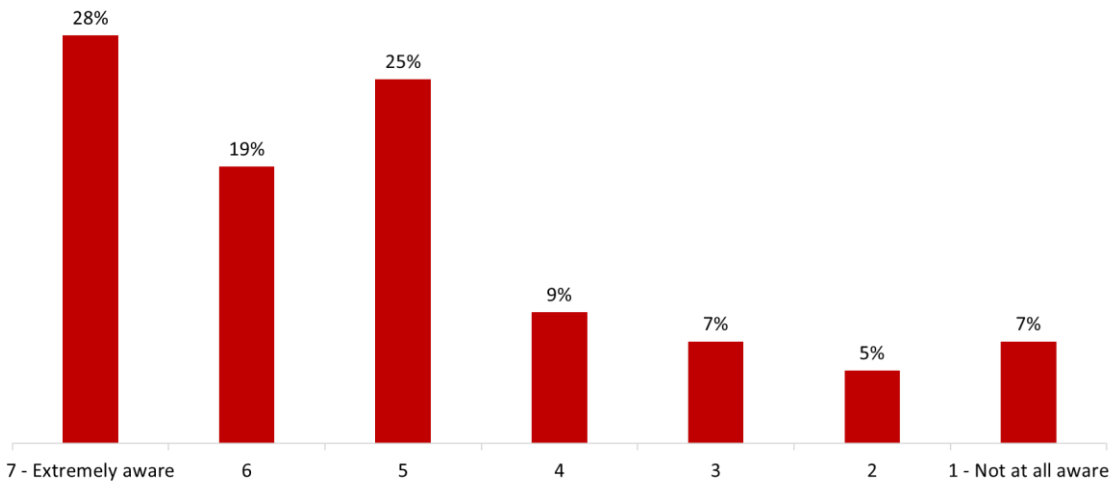
This section examines findings regarding companies' awareness of their responsibilities under privacy laws. Questions in this section were prefaced with the following description of Canada's privacy laws:

> 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

Almost half of business representatives (47%) said their company is highly aware of its responsibilities under Canada's privacy laws (scores of 6 or 7 on the 7-point scale), while 41% rated their company as moderately aware (scores of 3 to 5). Taken together, the majority (88%) of surveyed companies are at least moderately aware of their privacy-related responsibilities. Few (12%) rated their company's awareness as low (scores of 1 or 2).

Figure 8: Companies' awareness of responsibilities under privacy laws



Q13. How would you rate your company's awareness of its responsibilities under Canada's privacy laws? Base: n=800; all respondents. Don't know: 1%.

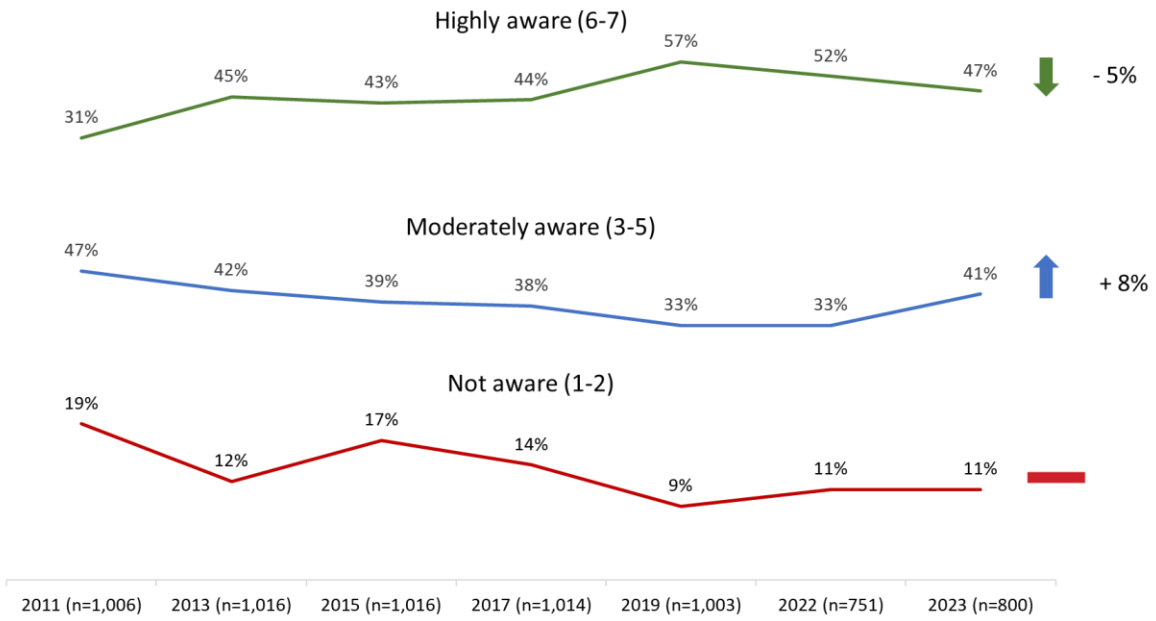
Awareness was higher among companies based in Quebec (65%) compared to those in Atlantic Canada (36%), Ontario (45%) and western Canada (43%) and it increased with company size, from 45% of small businesses to 77% of large businesses.[6] In addition, awareness was higher among companies that have taken steps to ensure it complies with Canada's privacy laws (58% versus 11% of those that have not), collect personal information from minors (69% versus 45% of those that do

[6] Small businesses have 1 to 19 employees, medium-sized businesses have 20 to 99 employees, and large business have 100 or more employees.

not), have a privacy policy (59% versus 31% of those that do not), and are aware of the OPC's resources for businesses (65% versus 35% of those that are not).

The proportion of business representatives who said their company is highly aware of its responsibilities under Canada's privacy laws continues to decline from the high of 57% reported in 2019. This year, 47% (a decline of 5%) felt their company is highly aware of its privacy-related responsibilities compared to 52% in 2022.

Figure 9: Companies' awareness of responsibilities under privacy laws [2011-present]



Net calculations are based on unrounded percentages.
Q13. 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

Three-quarters (76%) of business representatives surveyed 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 baseline of 66% reported in 2017.

Figure 10: Compliance with Canada's privacy laws

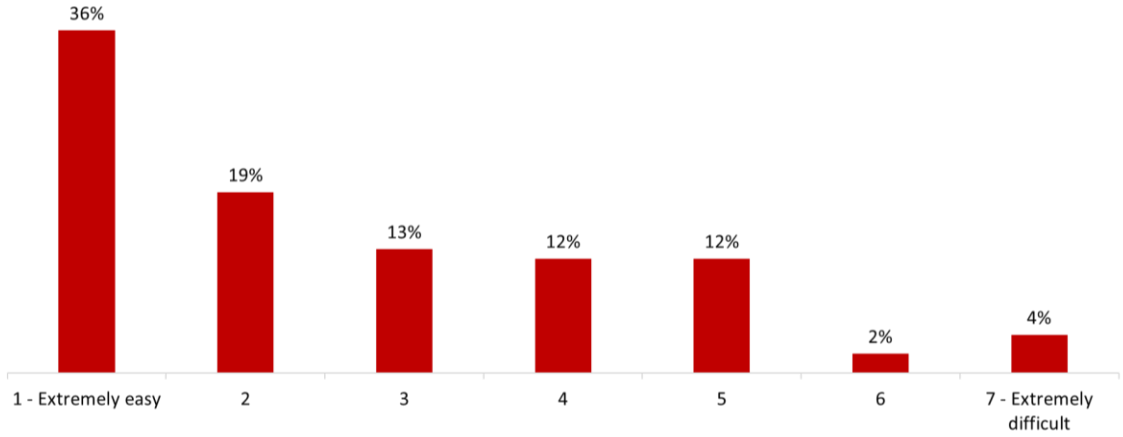
Q14. Has your company taken steps to ensure it complies with Canada's privacy laws? Base: all respondents.

The likelihood of taking steps to ensure compliance increased with the size of the company, from 75% of small businesses to 94% of large businesses. In addition, it was higher among companies that currently use AI in their business operations (99% versus 75% of those that are not), collect personal information from minors (91% versus 75% of those that do not), have a privacy policy (92% versus 55% of those that do not), and are aware of the OPC's resources for businesses (90% versus 67% of those that are not).

Most companies found it at least somewhat easy to ensure compliance

Among companies that have taken steps to comply with Canada's privacy laws (n=623), more than nine in 10 (93%) found it moderately (scores of 3 to 5 on a 7-point scale) or extremely (scores of 1 and 2) easy to bring their personal information handling practices into compliance. Very few business representatives (5%) said their company faced significant difficulties (scores of 6 and 7) ensuring compliance with Canada's privacy laws.

Figure 11: Level of difficulty complying with Canada's privacy laws

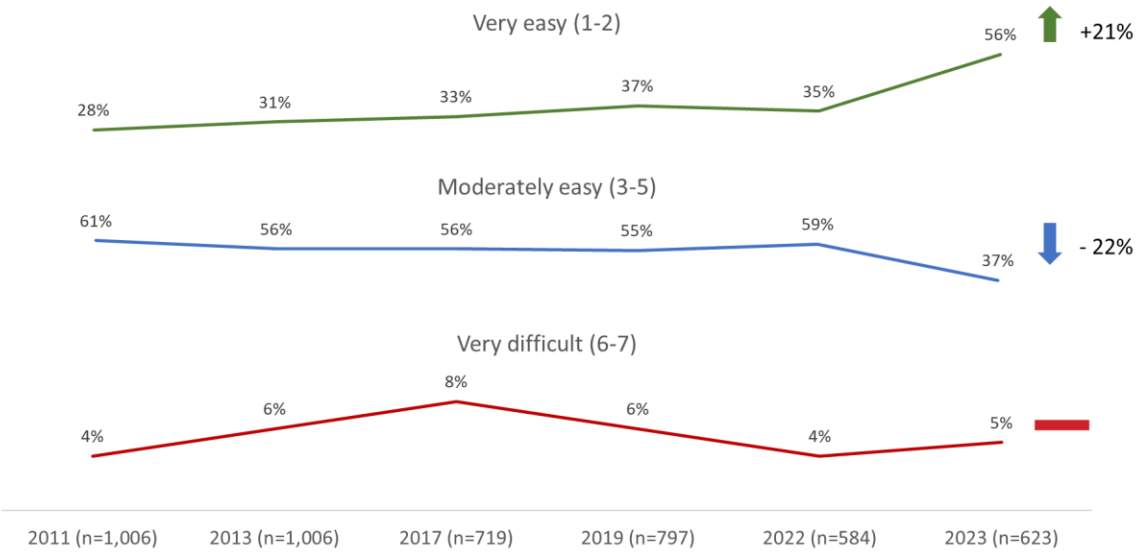


Q15. How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws? Base: n=623; those who have taken steps to comply with Canadian privacy laws. Don't know: 2%.

Small businesses (57%) were more likely to find it easy to comply with Canada's privacy laws as compared to larger businesses (46% of businesses with 20 to 99 employees and 42% of businesses with 100 or more employees).

The proportion of companies that found it very easy to bring personal information handling practices into compliance with Canada's privacy laws has increased significantly this year to a high of 56% (from 35% in 2022 and 37% in 2019).

Figure 12: Compliance with Canada's privacy laws [2011-present]



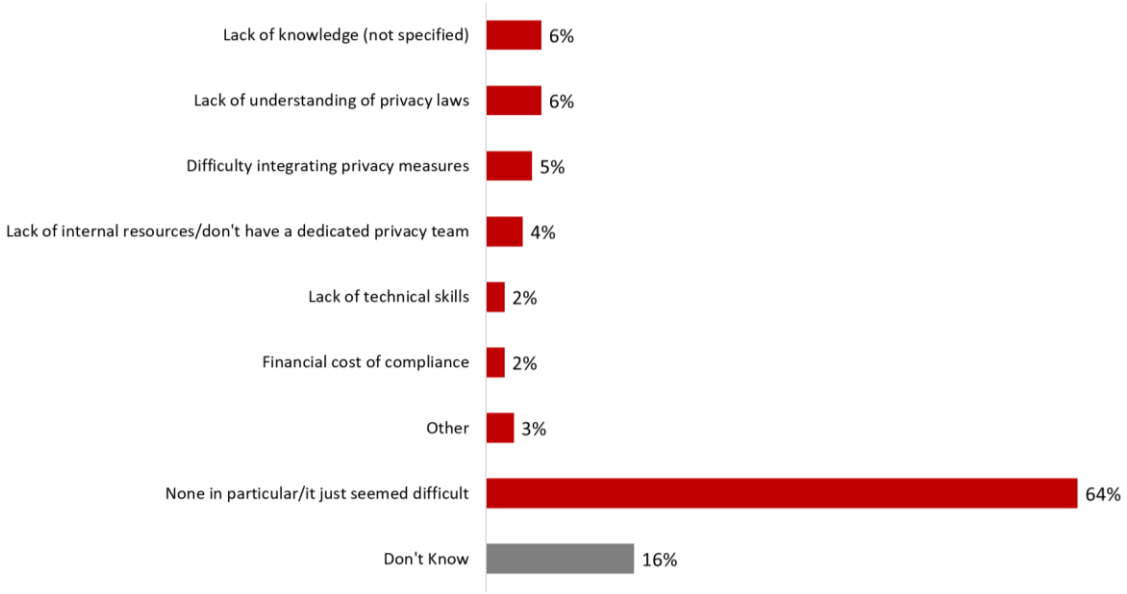
Net calculations are based on unrounded percentages.
Q15. How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws?

Few challenges were identified when it comes to complying with Canada's privacy laws

Nearly two-thirds (64%) of business representatives said their company did not have or does not expect to face any specific challenges when complying with Canada's privacy laws. When asked in an open-ended manner to identify challenges encountered or anticipated, these respondents explained that it just "seemed/seems difficult". An additional 16% said they did not know about any challenges.

Specific challenges included lack of knowledge (6%) or understanding of privacy laws (6%), difficulty integrating privacy measures with existing systems/processes (5%), lack of internal resources or a dedicated privacy team (4%), lack of technical skills (2%), and the financial cost of compliance (2%).

Figure 13: Challenges complying with Canada's privacy laws

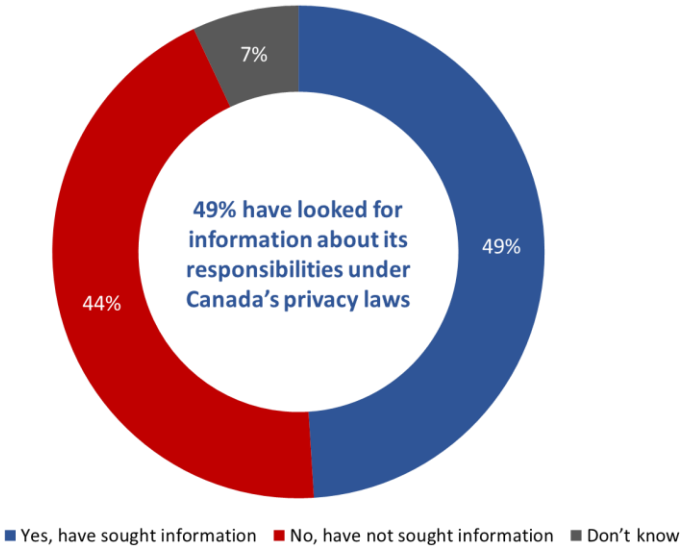


Q16. What challenges, if any, did your company have / do you expect your company will face complying with Canada's privacy laws? Multiple responses accepted. Base: n=800; all respondents.

Half have looked for information about privacy responsibilities

Half (49%) of companies have looked for information about their responsibilities under Canada's privacy laws. Forty-four percent have not (7% of surveyed business representatives did not know whether their company had looked for this type of information).

Figure 14: Sought information about privacy responsibilities



Q17. Has your company ever looked for information about its responsibilities under Canada's privacy laws? Base: n=800; all respondents.

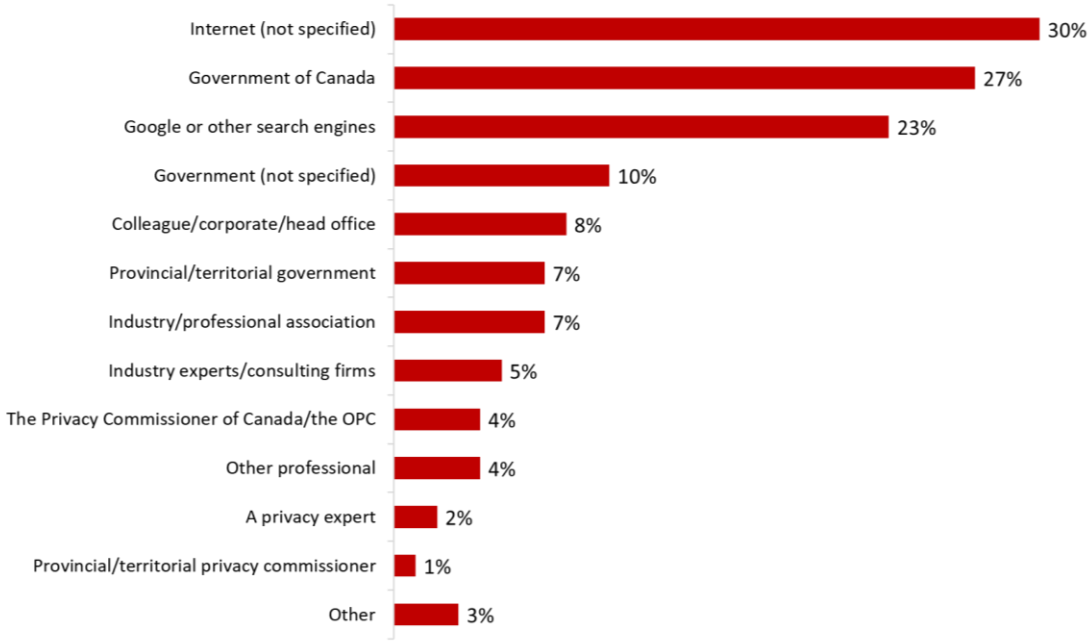
Compared to companies in Atlantic Canada (30%), those in Quebec (53%) and Ontario (52%) were more likely to have looked for information about their responsibilities under Canada's privacy laws. Additionally, the likelihood of looking for information increased with business size, from 47% of small businesses to 72% of large businesses, and with knowledge of privacy-related responsibilities, from 15% of companies unaware of these responsibilities to 63% of those highly aware. Companies that are currently using AI (86% versus 46% of those that are not), have taken steps to comply with privacy laws (60% versus 12% of those that have not), and are aware of the OPC's resources for business (57% versus 43% of those that are not) were more likely to have looked for information about Canada's privacy laws.

Internet followed by the government are the top sources of information

If business representatives needed information about their company's responsibilities under Canada's privacy laws, the top source of information would be the Internet (30%) and the Government of Canada (27%), followed by Google or other online search engines (23%). In addition to the Government of Canada, 10% said they would look to government, but did not specify which jurisdiction, while 7% mentioned their provincial or territorial government, 4% the Office of the Privacy Commissioner of Canada, and 1% their provincial or territorial privacy commissioner.

Beyond the Internet and government, 8% said they would ask a colleague or their corporate or head office for information, 7% their industry or professional association, 5% industry experts or consulting firms, 4% other types of professionals, such as accountants or lawyers, and 2% a privacy expert.

Figure 15: Sources of information about privacy-related responsibilities

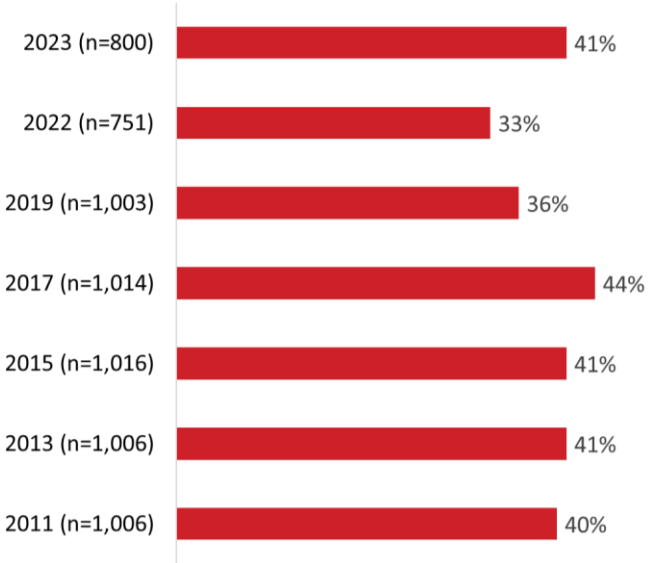


Q18. If you needed information about your company's responsibilities under Canada's privacy laws, where would you look? Multiple responses accepted. Base: n=800; all respondents. Don't know: 4%

4 in 10 aware of OPC's resources

Four in 10 (41%) surveyed business representatives are aware that the OPC has information and tools to help companies comply with their privacy obligations. Awareness of OPC's resources for businesses has increased significantly since 2021, when exactly one-third (33%) of respondents were aware.

Figure 16: Awareness of OPC resources [2011-present]



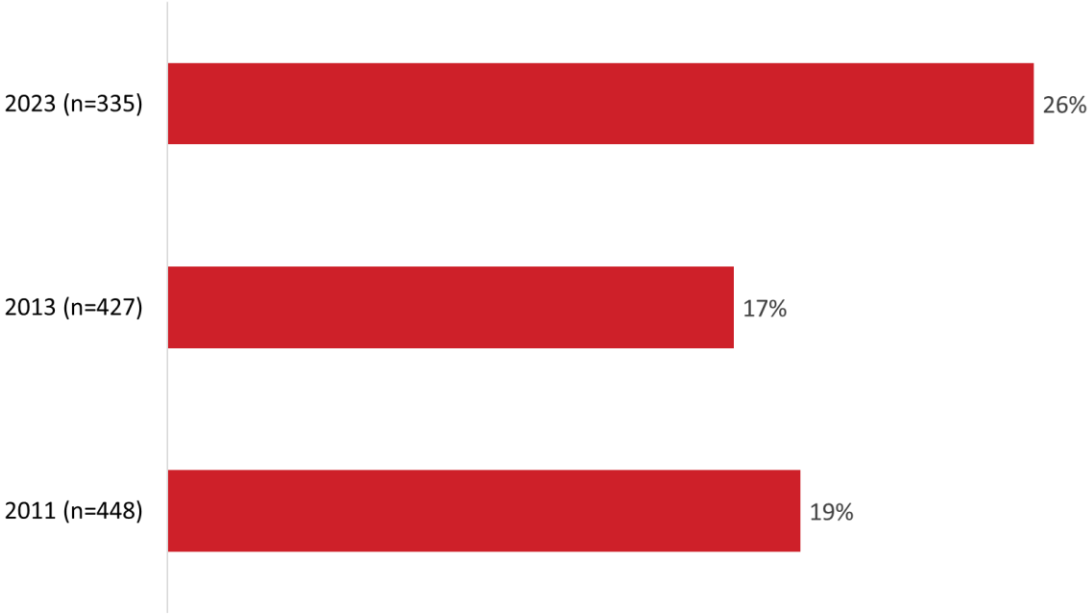
Q19. Are you aware that the Office of the Privacy Commissioner of Canada has information and tools available to companies to help them comply with their privacy obligations? Base: n=800 all respondents.

The likelihood of being aware that the OPC has information and tools available to companies to help them comply with privacy laws in Canada increased with business size, from 40% of small businesses to 59% of large businesses, and with knowledge of privacy-related responsibilities, from 24% of companies unaware of these responsibilities to 56% of those highly aware. Awareness was also higher among companies that have taken steps to comply with privacy-related obligations (48% versus 19% of that have not).

1 in 4 companies have used OPC's resources

One in four (26%) respondents aware of the OPC's resources (n=335) said their company has used the information and tools to help comply with privacy obligations. Compared to a decade ago, self-reported use of the OPC's information and tools has increased significantly, from 17% in 2013 to 26% in 2023.

Figure 17: Use of OPC resources [2011-present]



Q20. Has your company ever used any of these resources? Base: those aware of OPC tools and information.

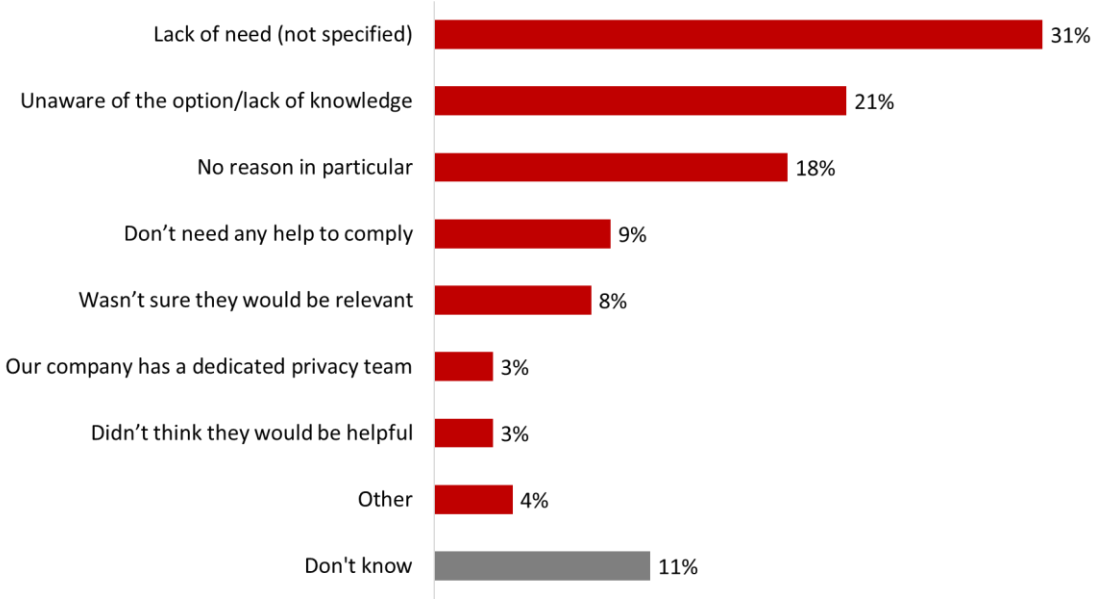
Use of the OPC's resources increased with business size, from 22% of small businesses to 54% of large businesses.

Lack of need is the main reason for not using the OPC's resources

Among those aware of the OPC's resources who have not used them (n=405), the main reason offered was a lack of need. Three in 10 (31%) said lack of need specifically, 9% that they do not need help to comply, and 3% that their company has a dedicated privacy team. Following lack of need, two in 10 (21%) pointed to lack of awareness or knowledge that resources existed, 8% to their perception that the resources would not be relevant, and 3% to their perception that the resources would not be helpful.

Others offered no specific reason for never having used the OPC's resources: 18% said there is no reason in particular and 11% did not know why their company has not used the information and tools.

Figure 18: Reasons for not using the OPC resources



Q21. Is there a specific reason why your company has never used these resources? Multiple responses accepted. Base: n=405, those aware of OPC resources, but have not used any.

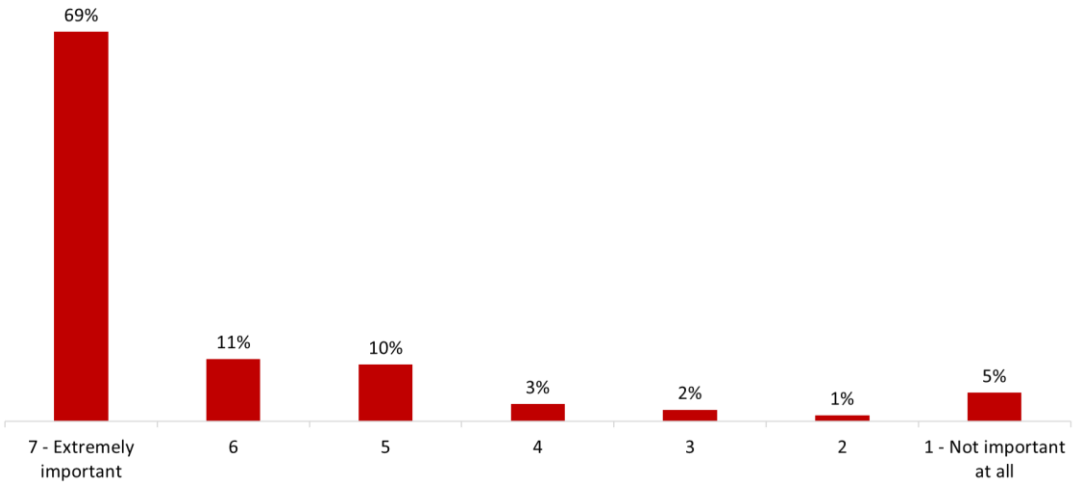
4. Company privacy practices

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

8 in 10 attribute high importance to protecting customers' personal information

The vast majority (94%) of business representatives said their company considers the protection of customers' personal information to be at least moderately important. Specifically, eight in 10 (80%) said their company considers the protection of customers' personal information to be of high importance (scores of 6 and 7 on a 7-point scale), including nearly seven in 10 (69%) who said this is an extremely important corporate objective, and 14% who attribute moderate importance to this objective. At the other end of the scale, 6% of business representatives reported that protecting customers' personal information is not an important corporate objective for their company (scores of 1 and 2).

Figure 19: Importance attributed to protecting customers' personal information

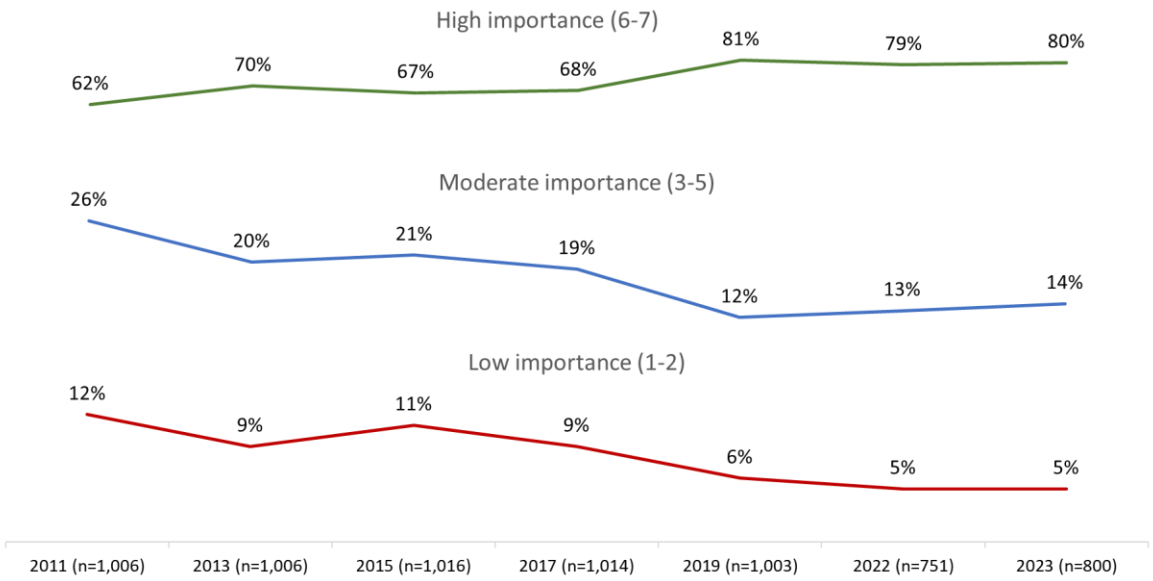


Q22. What importance does your company attribute to protecting your customers' personal information? Base: n=800; all respondents. Don't know: 1%

Medium-sized (91%) and large (92%) companies were more likely than small companies (78%) to place a high level of importance (scores of 6 and 7) on the protection of customers' personal information. In addition, companies that currently use AI (100% versus 78% of those that do not), that have taken steps to comply with Canada's privacy laws (88% versus 50% of those that have not), and that collect information from minors (94% versus 78% of those that do not) also were more likely to view this as something that is highly important.

The proportion of companies that attribute importance to protecting customers' personal information remains high and virtually unchanged since 2019: 81% in 2019, 79% in 2022, and 80% in 2023.

Figure 20: Net importance of protecting customers' personal information [2011-present]



Net calculations are based on unrounded percentages.
Q22. What importance does your company attribute to protecting your customers' personal information?

Half or more have implemented most privacy practices

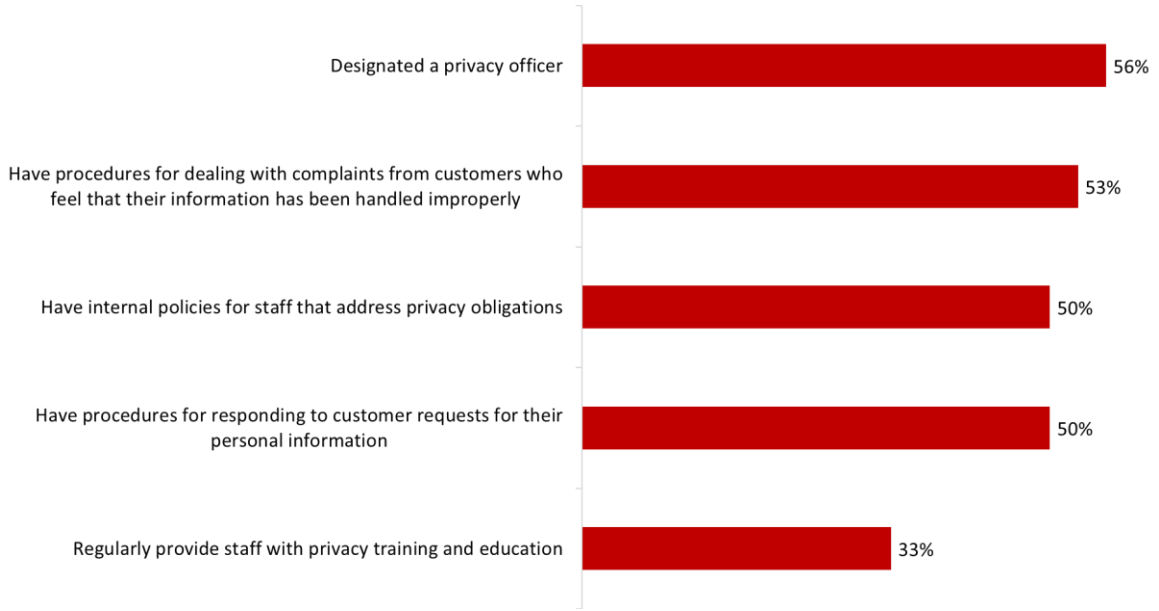
Business representatives were asked whether their company has put in place a series of privacy practices. Half or more of respondents said their company has implemented the following privacy practices: designated a privacy officer (56%); put in place procedures for dealing with customer complaints about the handling of their personal information (53%) and for responding to customer requests for access to their personal information (50%); and developed and documented internal policies for staff that address privacy obligations (50%). Exactly one-third (33%) said their business regularly provides staff with privacy training and education.

A directional trend exists where the likelihood of having implemented many of the practices increased with company size. Regional differences were limited. Companies in western Canada (54%) were more likely than those in Quebec (40%) to have internal policies for staff, and companies in Ontario (59%) were more likely than those in Atlantic Canada (37%) and Quebec (45%) to have procedures in place for dealing with complaints from customers who feel that their information has been handled improperly.

Additionally, companies aware of the OPC's resources to help companies comply with their privacy obligations were more likely than companies not aware to have implemented all of these privacy practices. Companies that collect personal information from minors were more likely than those that do not to have internal policies for staff that address privacy obligations (74% versus 47%), provide regular staff privacy training and education (58% versus 29%), and to have procedures for responding to customer requests for access to their personal information (75% versus 47%) as well

as for dealing with customer complaints about the handling of personal information (72% versus 51%).

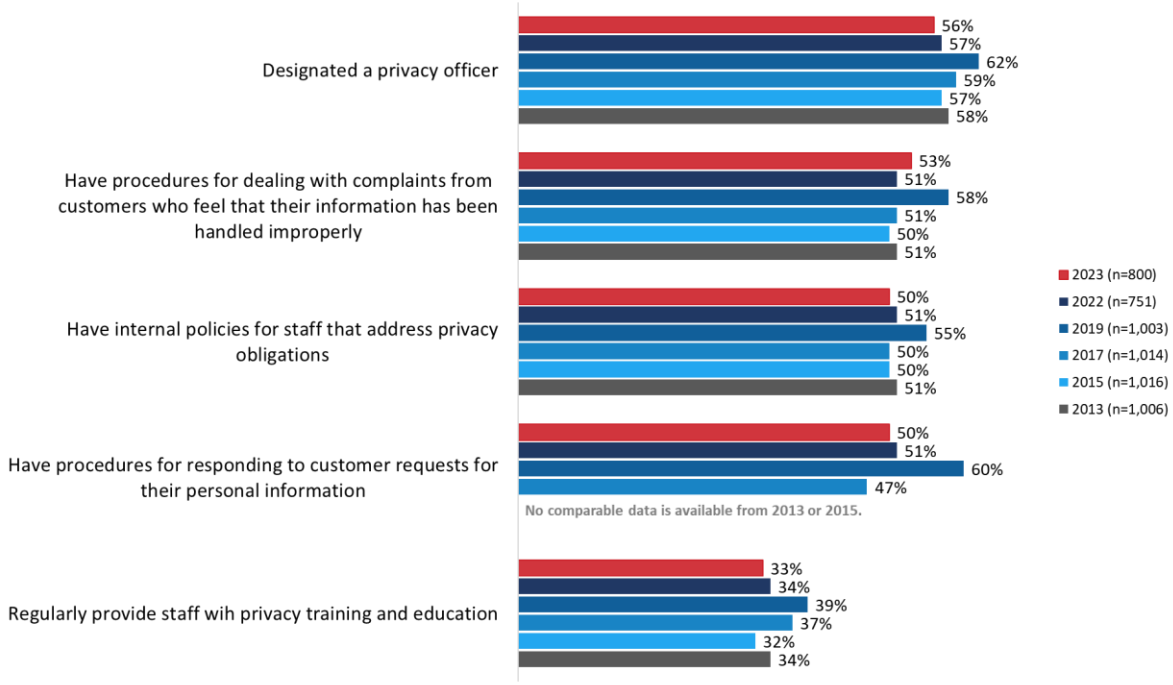
Figure 21: Actions taken to manage company privacy obligations



Q23 to Q27. Base: n=800; all respondents. Don't know: 3% to 4%.

Implementation of these privacy practices is virtually unchanged since 2022, when a decline was reported across all measures. At the time, the decrease in the proportion of companies reporting having implemented these practices was considered within the context of the COVID-19 global pandemic, with some speculation that the pandemic may have affected the survey findings. This year's findings suggest the decline in implementation between 2019 and 2022 may be a trend, rather than an isolated event influence by the pandemic.

Figure 22: Actions taken to manage company privacy obligations [2013-present]



Q23 to Q27.

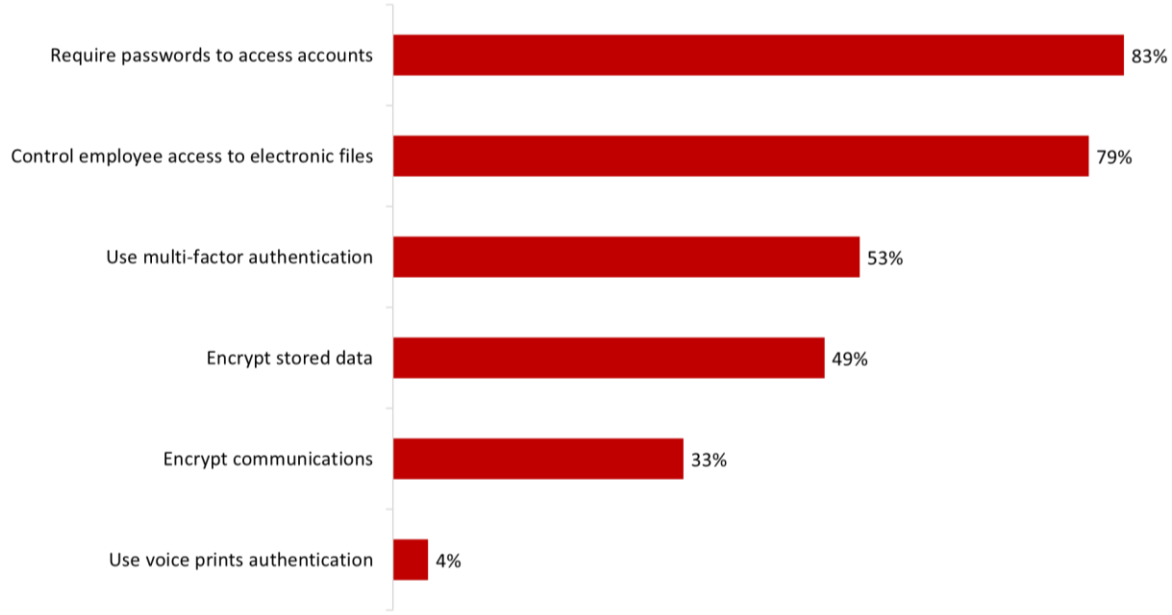
Uneven implementation of actions to safeguard the personal information

When it comes to safeguarding the personal information of customers and employees, approximately eight in 10 business representatives said their company requires passwords to access accounts (83%) and controls employee access to electronic files (79%). Roughly half reported that their company uses multi-factor authentication (53%) and encrypts stored data (49%) to safeguard customer and employee information. Following this, exactly one-third (33%) encrypt communications. Very few (4%) companies use voice prints authentication.

Regional differences were limited to two actions: multi-factor authentication and communications encryption. For both, companies based in Quebec were less likely than those based elsewhere in the country to have implemented each of these security measures. Specifically, 39% of companies in Quebec reportedly use multi-factor authentication compared to 58% each of companies in Ontario and western Canada, and 20% encrypt communications compared to 48% of companies in Ontario.

In addition, differences based on business size were evident for several of these measures, with small companies less likely than larger companies to require passwords (81%), to use multi-factor authentication (52%), and to control employee access to electronic files (77%).

Figure 23: Actions taken to safeguard personal data

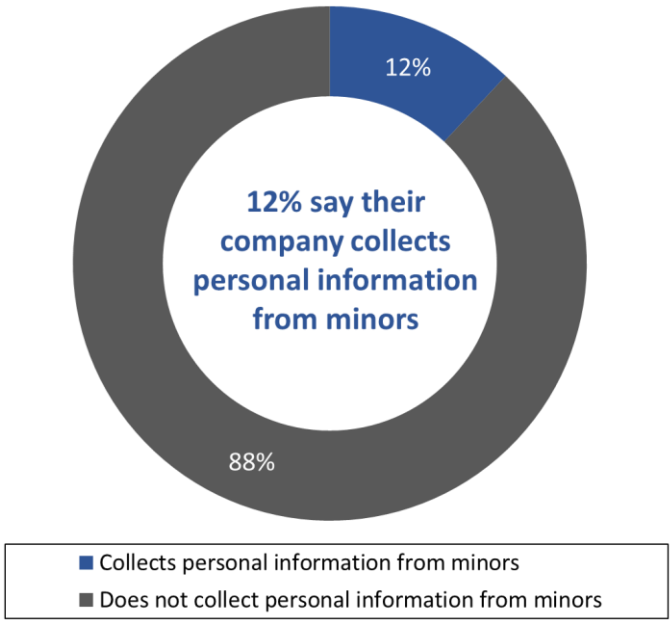


Q28A–F. Does your company take any of the following actions to safeguard personal information? Base: n=800; all respondents. Don't know: 0% to 7%. Does not apply 4% to 6%.

1 in 10 companies collect personal information from minors

Approximately one in 10 (12%) business representatives said their company collects personal information from customers who are under the age of 18. Most companies (88%) do not collection this information from minors.

Figure 24: Collecting personal information from minors



Q29. Does your company collect personal information from customers who are minors, that is under the age of 18? Base: n=800; all respondents. Don't know: <1%.

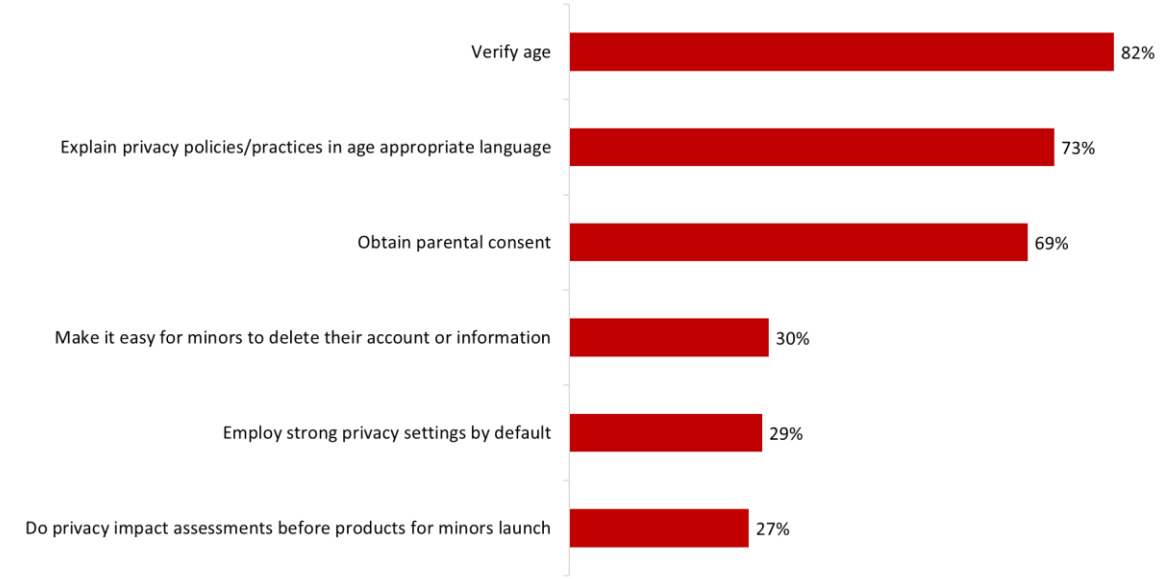
Companies in Atlantic Canada (24%) were more likely to collect personal information from minors compared to companies based elsewhere in the country (10% of companies in Ontario and 9% in western Canada). Similarly, companies that sell **only** to consumers (23%) were much more likely than those that sell to business **and** consumers (12%) to collect personal information from minors. Large companies (20% versus 11% of small companies) and companies that have taken steps to comply with their privacy obligations (14% versus 3% of those that have not) also were more likely to collect information from minors.

Additionally, companies operating in the following industries or sectors of the economy[7] tended to be more likely to collect personal information from minors: education services, social services, and finance and insurance.

Companies implement various practices when collecting personal information from minors

A majority of business representatives who said their company collects personal information from minors (n=67) verify age (82%), explain privacy policies and practices in simple, age-appropriate language (73%), and obtain parental consent (69%) when collecting information from those under the age of 18. Smaller, and similar proportions make it easy for young people to delete their account or the information they have posted (30%), employ strong privacy settings by default, for example, automatically turning off location tracking (29%), and conduct privacy impact assessments before launching products or tools aimed at young people (27%).

Figure 25: Actions taken when collecting personal information from minors



Q30A-F. When collecting information from minors, does your company do any of the following? Base: n=67; those who collect information from minors. Don't know: 0% to 8%. Does not apply: 5% to 46%.

[7] No percentages are provided due to small sample sizes.

5. Privacy policies

This section focuses on the content of company's privacy policies.

Majority of surveyed companies have a privacy policy

Just over half (55%) of the business representatives surveyed said their company has a privacy policy. Over time, the proportion of companies with a privacy policy has declined, from a high of 65% in 2019, to 59% in 2022, to 55% this year. In 2022, the decrease in the proportion of companies reporting a privacy policy was considered within the context of the COVID-19 global pandemic. Specifically, when businesses were preoccupied with the impact of the pandemic on operations, it was reasonable to assume that privacy responsibilities might not be top-of-mind. This year's findings suggest the decline in privacy policies may be a trend, rather than an isolated event influence by the pandemic.

Figure 26: Use of privacy policies [2019-present]

Q31. Does your company have a privacy policy? Base: all respondents.

Companies in Quebec (36%) were less likely than those in Atlantic Canada (65%), Ontario (62%), and western Canada (57%) to have a privacy policy. Additionally, as business size increased so did the likelihood of having a privacy policy. Half (53%) of small businesses have a privacy policy compared to two-thirds (67%) of medium-sized businesses, and nearly nine in 10 (87%) large businesses. Companies that use AI (78%) were more likely than those that do not (54%) to have a privacy policy, as were companies that collect information from minors (82% versus 52% of those that do not), and companies aware that the OPC has resources available to companies to help them comply with their privacy obligations (68% versus 46% of those unaware).

Companies' privacy policies had varying levels of plain language disclosures

Among companies that have a privacy policy (n=472), most explain in plain language the following: the purpose for which the company collects, uses, and discloses customers' personal information (85%); what personal information is being collected (81%); and how the company collects, uses, and discloses this information (80%). In addition, seven in 10 (70%) explain in plain language with which parties the personal information collected will be shared, two-thirds (67%) for how long the company keeps the personal information, and six in 10 (62%) how the company disposes of customers' personal information. Just over half (55%) said their company's policy explains in plain language the risks of harm in the event of a data breach.

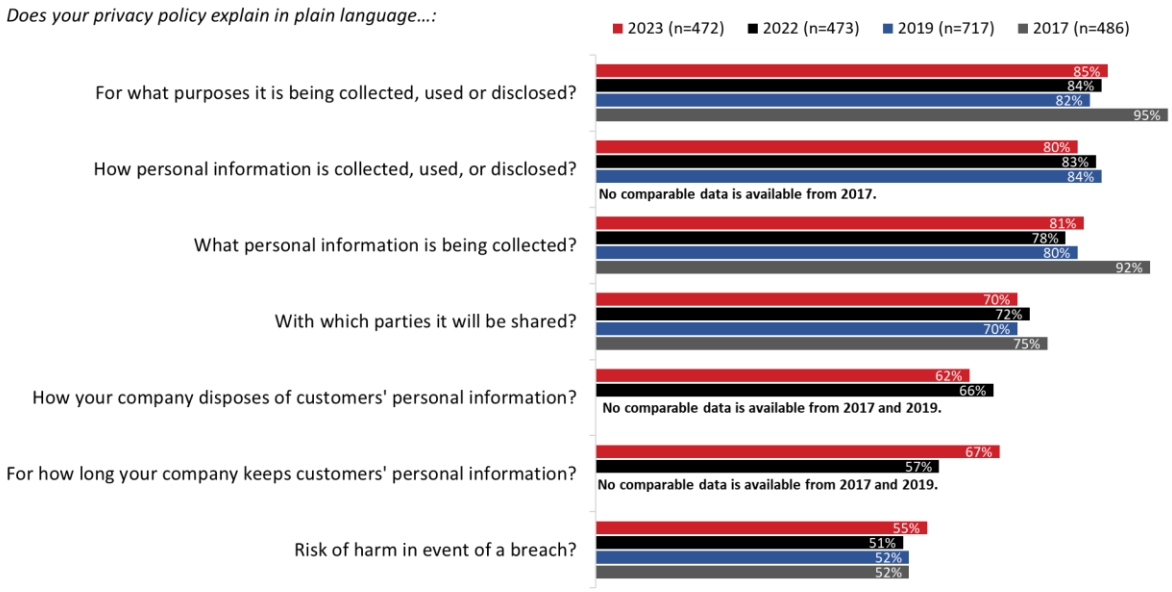
Figure 27: Privacy policy disclosures

Q32A-G. Does your privacy policy explain in plain language…? Base: n=472; companies with privacy policies. Don't know: 3% to 9%; Does not apply: 3% to 6%.

Companies in Quebec were more likely than those based in Ontario or western Canada to include in their privacy policy plain language about how long the company keep customers' personal information (87% versus 63% and 64%, respectively) and about how the company disposes of personal information (85% versus 55% and 60%, respectively).

When looking at whether companies have plain language disclosures in their privacy policies, the 2023 results are generally consistent with previous years. The one noteworthy change over time has been the proportion of companies that disclose, in plain language, for how long customers' personal information is kept. This increased from 57% in 2022 to 67% in 2023. All other year-over-year changes did not exceed 4%.

Figure 28: Privacy policy disclosures [2017-present]



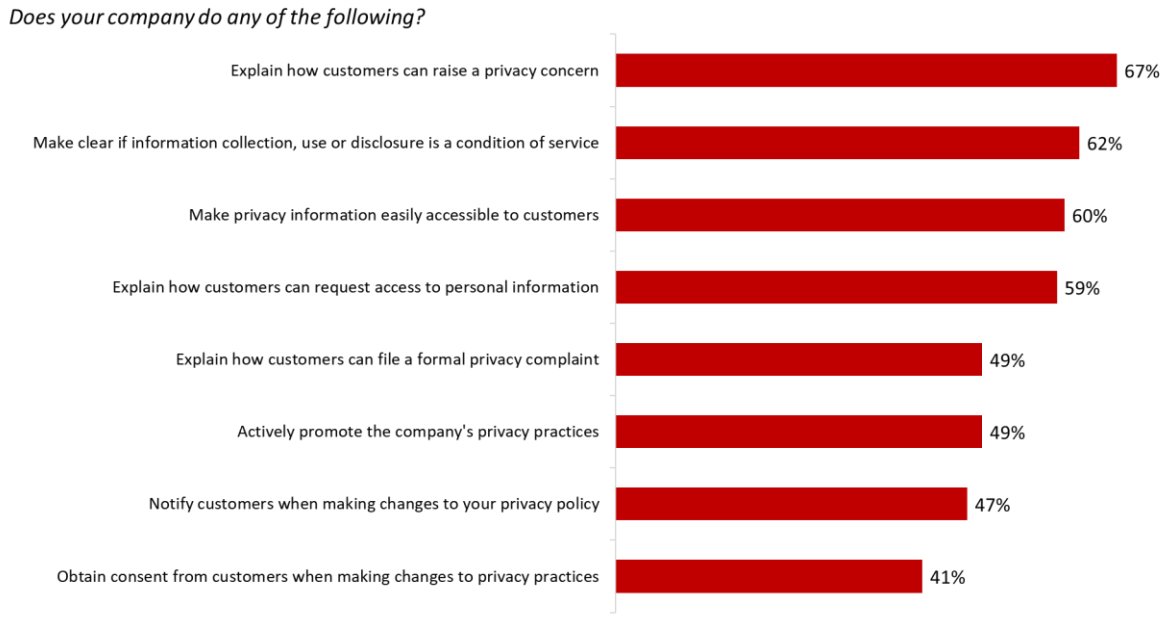
Q32A-G. Does your privacy policy explain in plain language…? Base: n=472; companies with privacy policies.

Proactive communications of privacy practices varies

Business representatives who said their company has a privacy policy (n=472) were asked whether their company communicates with customers about different aspects of its privacy practices. Exactly two-thirds (67%) said their company explains how customers can raise a privacy concern or ask a privacy question. Following this, approximately six in 10 companies make clear whether the collection, use or disclosure of information is a condition of service (62%), make privacy information easily accessible to customers (60%), and explain how customers can request access to their personal information (59%).

Just under half explain how customers can file a formal privacy complaint (49%), actively promote their company's privacy practices (49%), and notify customers when making changes to their privacy policy (47%). Four in 10 (41%) business representatives said their company obtains consent from customers when making changes to their privacy practices.

Figure 29: Communication of company privacy practices

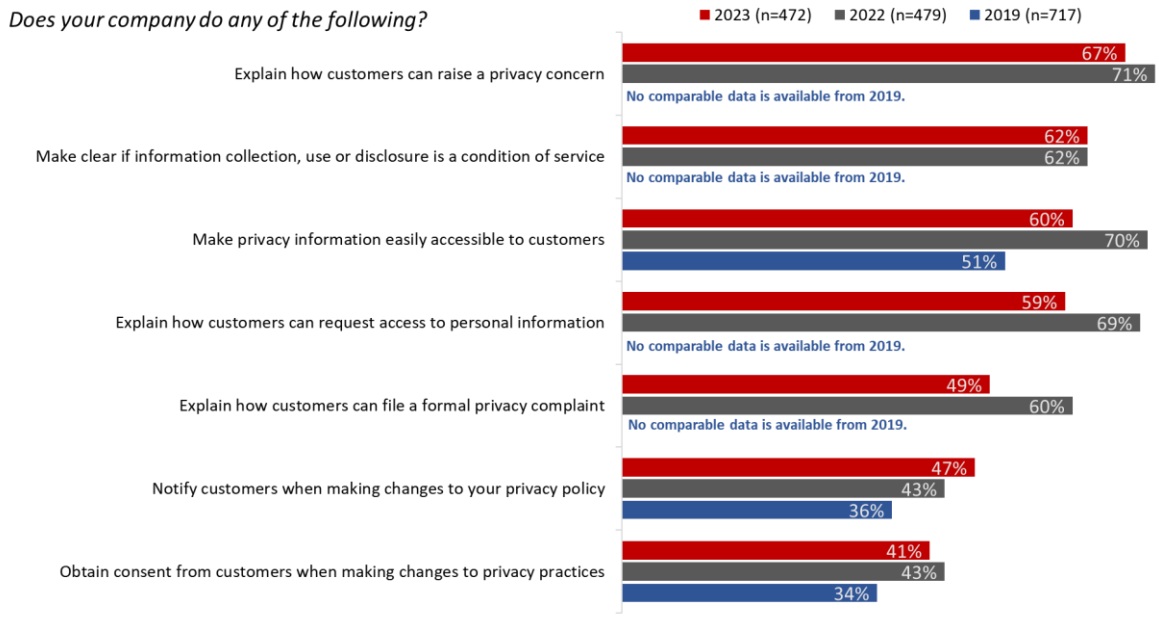


Q33A–H. Does your company do any of the following? Base: n=472; companies with privacy policies. Don't know: 2% to 6%; Does not apply: 1% to 6%.

There were several noteworthy regional differences, and to the extent that a pattern emerged, differences often separated Quebec from the rest of the country. Companies in Atlantic Canada (67%) and Quebec (62%) were more likely than those in Ontario (33%) and western Canada (38%) to obtain consent from customers before making changes to their privacy practices. Companies in Quebec (77%) were more likely than those in western Canada (54%) to make privacy information accessible, and compared to those in Ontario (52%), companies in Quebec (74%) were also more likely to explain how customers can request access to their personal information. In addition, companies in Quebec (85%) were the most likely to explain how customers can file a formal privacy complaint (versus 42% of companies in Atlantic Canada, 41% in Ontario and 47% in western Canada).

Over time transparency vis-à-vis company privacy practices has fluctuated, with the most significant year-over-year changes a decline in the proportion of companies that explain how customers can file a formal privacy complaint (from 60% in 2022 to 49% in 2023), that make privacy information easily accessible (from 70% in 2022 to 60% in 2023), and that explain how customers can request access to personal information (from 69% in 2022 to 59% this year). Other year-over-year changes did not exceed 4%.

Figure 30: Communication of company privacy practices [2019-present]



Q33A–H. Does your company do any of the following? Base: companies with privacy policies.

6. Managing privacy risks

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

More than one-third of companies have policies or procedures to assess privacy risks

More than one-third (37%) of business representatives said their company has policies or procedures in place to assess privacy risks related to their business, including assessing privacy risks associated with the development or use of new products, services, or technologies. Thirty-seven percent represents an increase since 2022, when the proportion of companies reporting use of risk management policies declined to 33% (from 38% in 2019).

Figure 31: Corporate policies and procedures to assess privacy risks [2019-present]

Q34. Does your company have any policies or procedures in place to assess privacy risks related to your business? Base: all respondents.

Companies that sell **only** to consumers (47%) were more likely to have privacy risk policies and procedures in place compared to companies that sell only to businesses (32%) and to consumers **and** businesses (34%). In addition, as business size increased so too did the likelihood of having such policies and procedures in place, from 35% of small businesses, to 45% of medium-sized businesses, to 59% of large businesses. Companies that collect personal information from minors (56%) were more likely than companies that do not (34%) to have risk assessment policies or procedures in place.

Half have a least some concern about a data breach

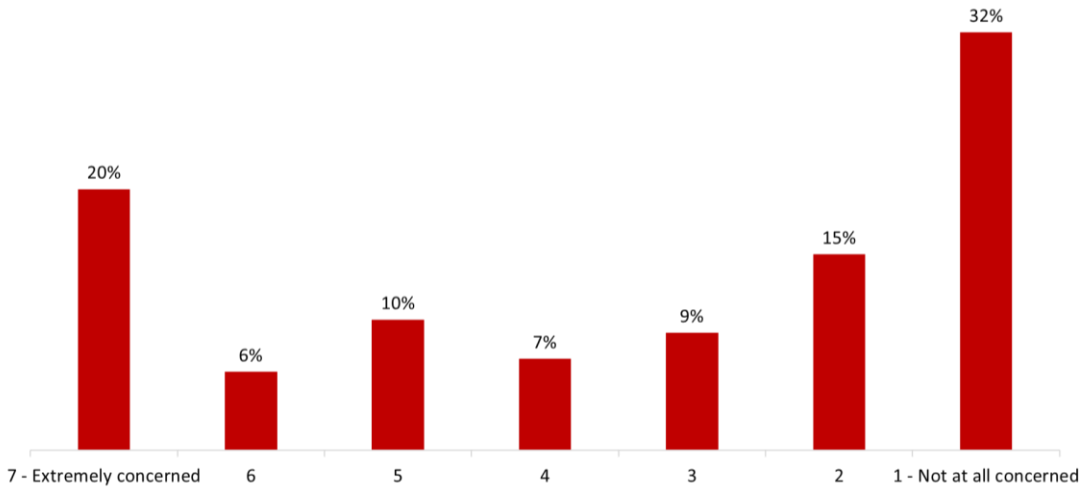
Business representatives were asked to rate their level of concern about a data breach, where the personal information of their customers is compromised. Before being asked this question, interviewers provided the following information:

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

Respondents were split with regards to their level of concern about a data breach involving customers' personal information. Just over half (52%) of surveyed business representatives said

they are least somewhat concerned (scores of 3 to 7 on a 7-point scale), including one-quarter (26%) who are highly concerned (score of 6 and 7). Conversely, almost as many (47%) reported a low level of concern (scores of 1 and 2), including nearly one-third (32%) who are not all concerned about a data breach.

Figure 32: Level of concern about a data breach

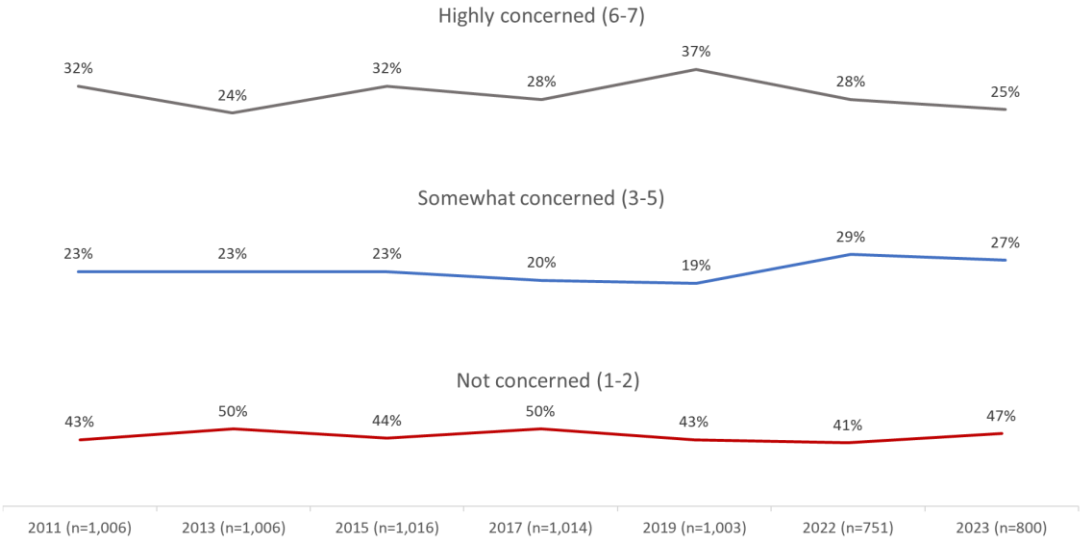


Q35. How concerned are you about a data breach, where the personal information of your customers is compromised?
Base: n=800; all respondents. Don't know: 1%.

Business representatives in Quebec were the most likely to be highly concerned about a data breach: 42% compared to 23% of those who reside in Atlantic Canada and Ontario, and 20% of those in western Canada.

The proportion of business representative highly concerned about a data breach continues to decline since the high of 37% recorded in 2019.

Figure 33: Level of concern about a data breach [2011-present]

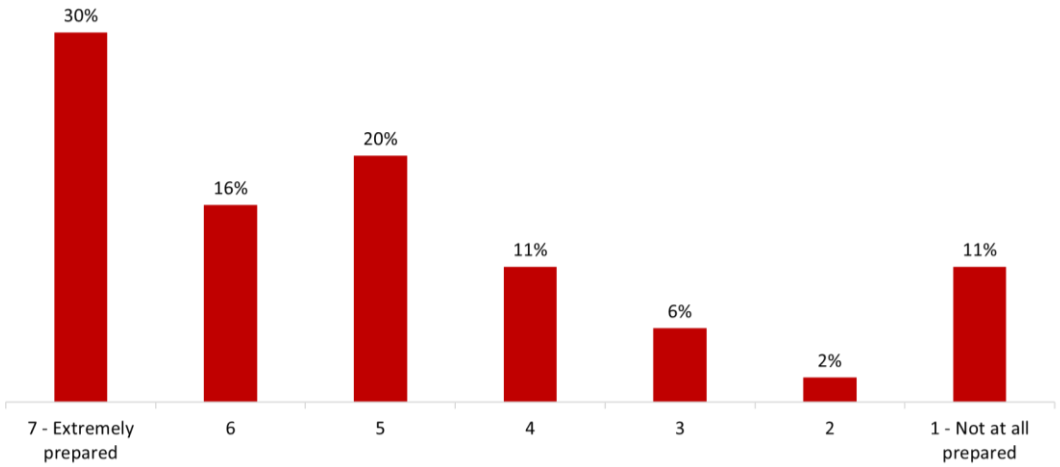


Net calculations are based on unrounded percentages.
Q35. How concerned are you about a data breach, where the personal information of your customers is compromised?

Most companies are at least somewhat prepared to deal with a data breach

More than eight in 10 (84%) survey respondents said their company is at least somewhat prepared to respond to a data breach involving personal information (scores of 3 to 7 on a 7-point scale), including close to half (46%) who said their company is highly prepared (scores of 6 and 7) for such an event. Fourteen percent felt their company is not prepared for a data breach (scores of 1 and 2).

Figure 34: Preparedness to deal with data breaches



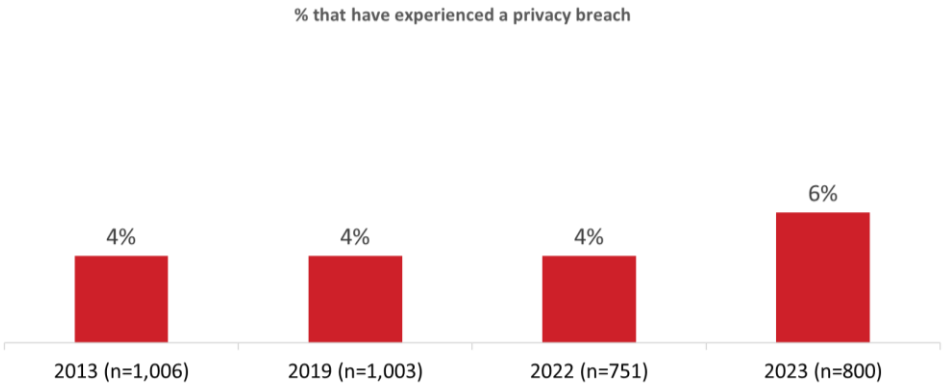
Q36. To what extent is your company prepared to respond to a data breach involving personal information? Base: n=800; all respondents. Don't know: 3%

As company size increased so too did preparedness. Seven in 10 (71%) large businesses would be highly prepared (scores of 6 and 7) to respond to a data breach compared to 48% of medium-sized businesses and 45% of small businesses. In addition, companies using AI (71% versus 44% of those not using AI), those that have taken steps to comply with privacy laws (51% versus 24% that have not), and those aware of the OPC's resources for businesses (55% versus 38% unaware) were more likely to be highly prepared to respond.

Vast majority of companies have not experienced a privacy breach

The vast majority of business representatives (93%) said their company has never experienced a breach where the personal information of their customers was compromised. The incidence of reported privacy breaches has been consistent for the last decade (4% in 2013, 2019 and 2022 and 6% in 2023).

Figure 35: Data breaches [2013-present]

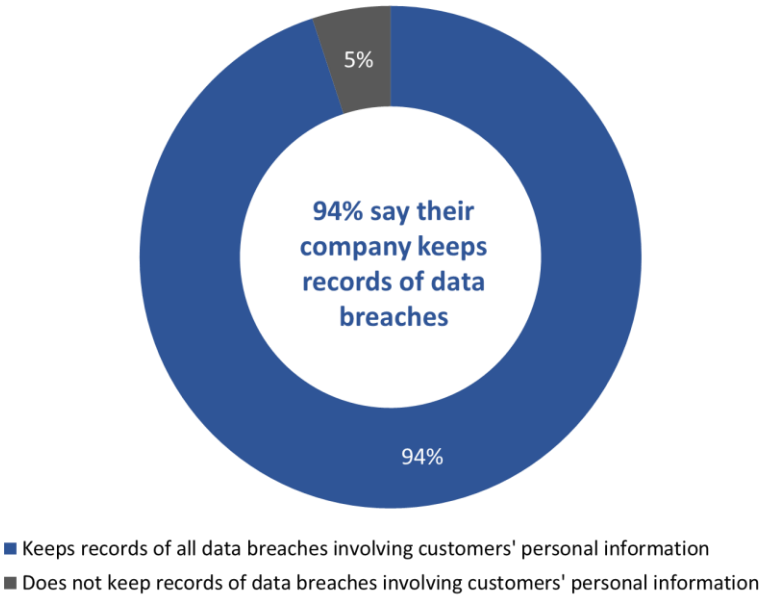


Q37. Has your company ever experienced a breach where the personal information of your customers was compromised? Base: all respondents.

Almost all companies that have experienced a data breach keep records of what was lost

Almost all (94%) companies that have experienced a data breach (n=46)[8] keep records of all data breaches involving customers' personal information.

Figure 36: Record keeping for data breaches



Q38. Does your company ensure that it keeps records of all data breaches involving your customers' personal information? Base: n=46, those who have experienced a data breach. Don't know: <1%.

[8] Exercise caution interpreting this finding due to the relatively small sample size, n=46.

Appendix

Corporate profile of responding companies

The following tables present the characteristics of Canadian businesses included in the survey sample (using weighted data), as well as business representatives.

Customer type	Percent
Sells directly to consumers	27%
Sells directly to businesses	29%
Sells directly to consumers and businesses	44%

Region	Percent
Atlantic Canada	7%
Quebec	19%
Ontario	38%
Prairies	7%
Alberta	15%
British Columbia	14%

Number of employees	Percent
1 employee (self-employed)	14%
2-4 employees	23%
5-9 employees	24%
10-19 employees	28%
20-99 employees	11%
100+ employees	1%

Industry/sector	Percent
Construction	12%
Professional, Scientific and Technical Services	12%
Retail Trade	11%
Other Services (except Public Administration)	9%
Accommodation and Food Services	7%
Health Care and Social Assistance	6%
Agriculture, Forestry, Fishing and Hunting	5%
Wholesale Trade	5%
Transportation and Warehousing	5%
Finance and Insurance	5%
Information and Cultural Industries	4%
Manufacturing	4%
Educational Services	4%
Arts, Entertainment and Recreation	2%

Industry/sector (cont'd.)	Percent
Administrative and Support, Waste Management and Remediation Services	2%
Real Estate and Rental and Leasing	2%
Other	4%

Respondent position	Percent
Owner, President, or CEO	44%
General manager/other manager	27%
Administration	9%
Director	4%
Accountant/bookkeeper	4%
Another title	11%

Survey questionnaire

Introduction

1st POINT OF CONTACT/GATEKEEPER:

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? 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 ASKED BY GATEKEEPER:

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.

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

RESPONDENT:

Hello/Bonjour, my name is [Interviewer's name]. 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.

The survey takes about 15 minutes and is voluntary. Your responses will be kept confidential and anonymous, and the information you provide will be administered according to the requirements of the Privacy Act, the Access to Information Act, and any other pertinent legislation. The survey is registered with the Canadian Research Insights Council's survey validation system.

May I continue?

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

INTERVIEWER NOTE: IF A RESPONDENT ASKS ABOUT THE LEGITIMACY OF THIS SURVEY, SAY: This survey is registered with the Canadian Research Insights Council's survey validation system. The registration number is: 20231120-PH062. If further validation is needed, offer to email them the background letter from the OPC.

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. [DO NOT READ] Other, please specify: [THANK AND TERMINATE]
05. [DO NOT READ] Not for profit [THANK AND TERMINATE]
99. [DO NOT READ] Don't know/refusal [THANK AND TERMINATE]

INTERVIEWER NOTES:
*IF ASKED ABOUT RESPONSE OPTION (1) "CONSUMERS", SAY: This refers to an individual not a business or organization.
**IF ASKED ABOUT "ORGANIZATIONS", SAY: This includes selling to governments.

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]

Section 1. Customers' Personal Information

I'd like to begin by asking about the personal information your company collects about customers. By personal information, I mean 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,

3. What does your company 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 data analytics
05. to train an artificial intelligence, or AI*, system
06. for some other purpose. If so, please specify:
07. [DO NOT READ] Don't know

INTERVIEWER NOTE:

*IF ASKED ABOUT "AI", SAY: AI is generally understood as machine learning, in the sense of creating an algorithm or model to simulate tasks normally requiring human intelligence. When we say "train an AI system" we're referring to the process of using data to develop such an algorithm or model.

4. How does your company store the personal information of 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 employee's or employer's home office on paper
05. Stored at an employee's or employer's home office electronically
06. [VOLUNTEERED] Company does not store personal information about customers
07. [DO NOT READ] Don't know

5. Does your company send customers' personal information to companies outside Canada for processing, storage or other purposes? [READ LIST]

01. Yes
02. No
03. [DO NOT READ] Don't know

6. [IF Q5=01] Do you inform customers that their personal information may leave Canada? [READ LIST]

01. Yes
02. No
03. [DO NOT READ] Company only provides this information if asked
04. [DO NOT READ] Don't know

7. [IF Q6=01] How does your company inform customers? Is this done through… [READ LIST; ACCEPT ALL THAT APPLY]

01. The Terms of Service agreement
02. The company's Privacy Policy
03. Express consent, or
04. Some other way. [SPECIFY]
05. [DO NOT READ] Don't know

Section 2: Technology

8. Does your company use AI for business operations? [READ LIST]

01. Yes
02. No
03. [DO NOT READ] Don't know

9. [IF Q8=01] How is your company using AI in its business operations? [DO NOT READ LIST; ACCEPT MULTIPLE RESPONSES]

01. Customer service/chatbots
02. Marketing (tailored advertising, personalized services, etc.)
03. Forecast trends/customers behaviour/demand
04. Fraud detection
05. Video/image analysis
06. Employee recruitment
07. Human resources-related applications
08. Quality control
09. Supply chain optimization
10. Data analysis
11. Other [SPECIFY]
99. Don't know

10. [IF Q8=01] Is AI being used by your company to improve efficiency, for decision-making, or for both?

01. Improve efficiency
02. Decision-making
03. Both
04. [VOLUNTEERED] Neither
99. [VOLUNTEERED] Don't know

INTERVIEWER NOTE:

*IF ASKED ABOUT "AI FOR DECISION-MAKING", SAY: Examples of this would be using AI in the process of hiring an employee or to decide whether to approve a loan.

11. [IF Q10=02,03] When your company uses AI for decision-making does a human employee review the decision before any action is taken by your company? [READ LIST]

01. Yes
02. No
03. [DO NOT READ] Don't know

INTERVIEWER NOTE:

*IF ASKED ABOUT "AI FOR DECISION-MAKING", SAY: Examples of this would be using AI in the process of hiring an employee or to decide whether to approve a loan.

12. [IF Q8=02, 03] How likely is it that your company will use AI for business operations in the next five years? Is it very likely, somewhat likely, not very likely, or not at all likely?

Section 3: 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.

13. 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.

14. Has your company taken steps to ensure that it complies with Canada's privacy laws? [READ LIST]

01. Yes
02. No
99. [DO NOT READ] Don't know

15. [IF Q14=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.

16. What challenges, if any, [IF Q14=01: did your company have / IF Q14=02,99: do you expect your company will face] complying with Canada's privacy laws? [DO NOT READ LIST; ACCEPT MULTIPLE RESPONSES]

01. Lack of internal resources/company doesn't have a dedicated privacy team
02. Lack of knowledge (not specified)
03. Lack of understanding of privacy laws
04. Financial cost of compliance
05. Lack of technical skills
06. Difficulty integrating privacy measures with existing systems/processes
07. No reason in particular/it just seemed difficult
08. Other (specify)
99. Don't know

17. Has your company ever looked for information about its responsibilities under Canada's privacy laws? [READ LIST]

01. Yes
02. No
99. [DO NOT READ] Don't know

18. If you needed information about your company's responsibilities under Canada's privacy laws, where would you look? [DO NOT READ LIST; ACCEPT MULTIPLE RESPONSES]

01. Internet (not specified)
02. Google or other search engines
03. Government (not specified)
04. Government of Canada
05. Provincial/territorial government
06. The Privacy Commissioner of Canada/the Office of the Privacy Commissioner of Canada
07. Provincial/territorial privacy commissioner
08. Industry/professional association
09. Industry experts/consulting firms
10. Consulted a privacy expert
11. Other (specify)
99. Don't know

19. 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? [READ LIST]

01. Yes
02. No
03. [DO NOT READ] Not aware of the OPC
99. [DO NOT READ] Don't know

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

20. [IF Q19=01] Has your company ever used any of these resources? [READ LIST]

01. Yes
02. No
99. [DO NOT READ] Don't know

21. [IF Q19=02] Is there a specific reason why your company has never used these resources? [DO NOT READ LIST; ACCEPT MULTIPLE RESPONSES]

01. Lack of need (no specified)
02. Wasn't sure they would be relevant to our company/our situation
03. Our company has a dedicated privacy team
04. Lack of trust in the OPC's resources
05. Didn't think they would be helpful
06. Don't need any help to comply
07. No reason in particular
08. Other (specify)
99. Don't know

Section 4: Company Privacy Practices

22. 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.

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

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

01. Yes
02. No
99. [DO NOT READ] Don't know

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

01. Yes

02. No
99. [DO NOT READ] Don't know

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

01. Yes
02. No
99. [DO NOT READ] Don't know

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

01. Yes
02. No
99. [DO NOT READ] Don't know

27. 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
99. [DO NOT READ] Don't know

28. Does your company take any of the following actions to safeguard the personal information of customers and employees? Please answer yes or no. [READ ITEMS; ROTATE ITEMS]

a. Require passwords to access accounts
b. Use multi-factor authentication
c. Use voice prints authentication
d. Encrypt communications
e. Encrypt stored data
f. Control employee access to electronic files

RESPONSE OPTIONS:

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

29. Does your company collect personal information from customers who are minors, that is under the age of 18? [READ LIST]

01. Yes
02. No
03. [DO NOT READ] Don't know

30. [IF Q29=01] When collecting information from minors, does your company do any of the following? Please answer yes or no. [READ ITEMS; ROTATE ITEMS]

a. Verify age

b. Obtain parental consent
c. Explain privacy policies and practices in simple, age appropriate language
d. Conduct privacy impact assessments before launching products or tools aimed at young people
e. Employ strong privacy settings by default, for example, automatically turning off location tracking
f. Make it easy for young people to delete their account or information they've posted

RESPONSE OPTIONS:

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

Section 5: Privacy Policies

31. Does your company have a privacy policy? [READ LIST]

01. Yes
02. No
99. [DO NOT READ] Don't know

32. [IF Q31=01] Does your privacy policy explain in plain language...? [READ LIST; ROTATE ITEMS]

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. [DO NOT READ] Does not apply
99. [DO NOT READ] Don't know

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

33. [IF Q31=01] Does your company do any of the following? [READ LIST; ROTATE ITEMS]

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?
h. Actively promote your company's privacy practices?

RESPONSE OPTIONS:

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

Section 6: Risk Assessment and Breaches

34. 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. [READ LIST]

01. Yes
02. No
98. [DO NOT READ] Does not apply
99. [DO NOT READ] 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.

35. 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.

36. 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.

37. Has your company ever experienced a breach where the personal information of your customers was compromised? [READ LIST]

01. Yes
02. No
99. [DO NOT READ] Don't know

38. [IF Q37=01] Does your company ensure that it keeps records of all data breaches involving your customers' personal information?

01. Yes
02. No
99. [DO NOT READ] Don't know

Section 7: Corporate Profile

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

39. 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:
99. Don't know/no response

40. 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
99. Don't know/no response

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