Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

2025-2026 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: CW2230204
Award Date: 2025-11-24
Contract Value: $77,744.41 (including HST)
Delivery Date: 2026-03-25

Registration Number: POR 059-25

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

Ce rapport est aussi disponible en français.

Canada

2025-2026 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 2026

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 from January 19 to February 25, 2026.

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

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

Catalogue Number: IP54-96/2026E-PDF

International Standard Book Number (ISBN): ISBN 978-0-660-99751-3

Related publications (POR registration number): ROP 059-25
Catalogue number (Final report, French): IP54-96/2026F-PDF
ISBN: ISBN 978-0-660-99752-0

Aussi offert en français sous le titre : « Sondage de 2025-2026 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 year's research were to collect data on the type of privacy policies and practices businesses have in place; businesses' compliance with the law; and businesses' awareness and approaches to privacy protection. The findings will be used by the OPC to provide guidance to both individuals and organizations on privacy issues, and to enhance its outreach efforts with 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 operating in sectors with a higher likelihood of collecting, using, storing, and/or disclosing customers' personal information. To be eligible, companies needed to sell or offer services or products directly to individual consumers. The following sectors, as classified by the North American Industry Classification System (NAICS), were included:

- 44-45 – Retail trade
- 48-49 – Transportation and warehousing
- 51 – Information and cultural industries
- 52 – Finance and insurance
- 53 – Real estate and rental and leasing
- 54 – Professional, scientific, and technical services
- 61 – Educational services
- 62 – Health care and social assistance
- 71 – Arts, entertainment, and recreation
- 72 – Accommodation and food services
- 81 – Other services (except public administration).

Respondents were senior decision makers with responsibility and knowledge of their company's privacy and security practices. The fieldwork took place January 19 to February 25, 2026. The survey results were weighted to the sample frame by business size, region and sector to ensure they reflect the distribution of businesses in Canada operating in the targeted sectors. Based on a sample of 800 companies, the results can be considered accurate to within ±3.5%, 19 times out of 20.

Key Findings

Canadian businesses continue to use customer information primarily to provide services and rely on electronic and third-party storage methods. Fewer than one in five use AI in their business operations.

- Most business representatives (86%) said their company uses customer information to

provide service to customers. Very few (2%) companies use this information to train an AI system.

- Nearly two-thirds of companies (63%) store the customer information they collect on-site electronically, while half (50%) use off-site storage with a third party, such as a cloud service.
- Sixteen percent of Canadian businesses reported using AI in their operations. Among businesses using AI, the most common use was research and document drafting (45%), followed by marketing (24%), text or data analysis (18%), and customer service or chatbots (15%).

Canadian businesses use a variety of different security measures to protect customers' personal information.

- Business representatives reported that their company takes a range of actions to safeguard customers' personal information. The most common measures include using end-point protection tools (90%), requiring passwords to access accounts (87%), and controlling employee access to electronic files (86%). Many businesses also use multi-factor authentication (65%), while just over half use encryption (55%) and intrusion detection systems (52%).
- Among companies that collect personal information from young people, most verify age (85%) and obtain parental consent if the young person is under 13 (84%). In addition, 68% explain their privacy policies and practices in simple, age-appropriate language. Fewer companies use strong privacy settings by default, such as automatically turning off location tracking (36%) or make it easy for young people to delete their account or information they have posted (34%).

Most Canadian businesses are highly aware of their responsibilities under Canada's privacy laws and report having taken steps to comply.

- The vast majority of business representatives (93%) said their company is at least moderately aware of its privacy-related responsibilities, including 72% that are highly aware.
- Nine in 10 businesses (91%) have taken steps to ensure their company complies with Canada's privacy laws, and nearly six in 10 (58%) of these companies found it easy to comply.

Many businesses are aware of the OPC's resources and pointed to practical compliance tools as the most helpful type of supports.

- Half of business representatives (51%) reported being aware that the OPC has information and tools available to companies to help them comply with their privacy obligations. Among those aware of the OPC's resources, 40% said their company has used these resources.
- Step-by-step compliance guides (65%), online training modules for staff (64%), and templates (63%) were most frequently identified as helpful tools, selected nearly two-thirds of the time they were presented to respondents. Self-assessment tools (42%), breach reporting guidance (34%), and guidance on AI and emerging technologies (25%) were selected less frequently.

Majority of Canadian businesses report having formal privacy practices in place to protect personal information collected from their customers.

- Approximately three-quarters of business representatives said their company has procedures in place to handle complaints from customers who believe their personal information has been handled improperly (77%) and to respond to customer requests for access to their personal information (75%). A similar proportion reported having developed and documented internal policies for staff that address their privacy obligations under the law (74%), while seven in 10 said their company has designated an individual responsible for privacy issues and the personal information their company holds (72%). A smaller proportion, though still a majority at 62%, reported that their company regularly provides staff with privacy training and education.

Most businesses report having a privacy policy and say their policy explains key information-handling practices in plain language.

- Eight in 10 (84%) business representatives said their company has a privacy policy.
- Most business representatives whose company has a privacy policy (n=665) reported that it explains in plain language key elements of their information-handling practices. Nearly nine in 10 (87%) said their policy outlines the purposes for which personal information is collected, used or disclosed. Similarly, large majorities indicated that their policy explains how personal information is collected, used or disclosed (85%), as well as what personal information is collected (84%). Approximately three-quarters reported that their company's privacy policy explains with whom information may be shared (76%), how long personal information is retained (75%), and how it is disposed of (73%). Seven in 10 (70%) said their policy also describes the risk of harm in the event of a breach.
- Among companies that have a privacy policy, many communicate key privacy practices to customers: 75% said their company explains how customers can raise a privacy concern or ask a privacy-related question, 71% make clear when the collection, use or disclosure of personal information is a condition of service and make privacy information easily accessible to customers, 69% explain how customers can request access to their personal information, and 65% explain how customers can file a formal privacy complaint.

The vast majority of businesses are a least moderately prepared to respond to a data breach, and close to two-thirds of respondents consider their company highly prepared.

- Nine in 10 business representatives (90%) said their company is at least moderately prepared to respond to a data breach involving personal information, including 64% that are highly prepared.
- At the same time, one in 10 businesses (10%) have, at some point, experienced a breach where the personal information of their customers was compromised.

Contract Value

The contract value was $77,744.41 (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 in the Policy on Communications and Federal Identity and the and the Directive on the Management of Communications and Federal Identity, Appendix B: Mandatory Procedures for 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 Agent of Parliament whose mission is to protect and promote privacy rights. The Commissioner investigates complaints and publicizes investigative findings, provides privacy and data protection advice to Parliamentarians, federal government institutions, businesses and individuals, conducts research into privacy issues and works with other regulators in Canada and abroad to improve privacy protections.

The OPC oversees compliance with the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, Canada's federal private-sector privacy law, 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 important that the OPC understands businesses' awareness and approaches to privacy protection.

The purpose of this research was 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 results will 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 operating in sectors with a higher likelihood of collecting, using, storing and/or disclosing customers' personal information. Sectors with limited or no direct handling of customer data were excluded to improve the relevance of the results. This approach ensures the findings more accurately reflect privacy practices among businesses for which personal information management is a core operational consideration.

The OPC has been surveying Canadian businesses since 2011, generating findings that are representative of businesses across Canada and that support its outreach efforts. This year, the target population for the survey was refined to better meet communication and outreach objectives by limiting participation to companies that sell or offer services or

products directly to individual consumers and collect customers' personal information. Respondents were senior decision makers with responsibility and knowledge of their company's privacy and security practices.

These following sectors, as classified by the North American Industry Classification System (NAICS), were included:

- 44-45 – Retail trade
- 48-49 – Transportation and warehousing
- 51 – Information and cultural industries
- 52 – Finance and insurance
- 53 – Real estate and rental and leasing
- 54 – Professional, scientific, and technical services
- 61 – Educational services
- 62 – Health care and social assistance
- 71 – Arts, entertainment, and recreation
- 72 – Accommodation and food services
- 81 – Other services (except public administration).

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). The survey was pre-tested between January 6 and 9, 2026, using Computer Assisted Telephone Interviewing (CATI). Based on the pre-test, revisions were made to reduce the questionnaire length, including removing a small number of questions and implementing split samples. Fieldwork resumed on January 19 and was completed on February 25, 2026.

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	**11,092**
Out-of-scope – Invalid	**933**
Unresolved (U)	**4,471**
No answer/Answering machine	4,471
In-scope - Non-responding (IS)	**2,187**
Language barrier	55
Incapable of completing (ill/deceased)	24
Callback (respondent not available)	2,108
Refusal	2,189
Termination	95
In-scope - Responding units (R)	**1,217**
Completed interview	800
Not eligible (does not sell to customers)	178
Not eligible (does not collect personal information)	204

Not eligible (does not know how many employees)	35
Response rate	**12%**

The survey results were weighted to the sample frame by business size, region and sector to ensure they reflect the distribution of businesses in Canada operating in the targeted sectors. Based on a sample of 800 companies, the results can be considered accurate to within ±3.5%, 19 times out of 20.

Notes to readers

- Results are compared to similar surveys conducted in 2011-2012, 2013-2014, 2015-2016, 2017-2018, 2019-2020, 2021-2022, and 2023-2024. Historical data is provided for measures when available. When comparing results over time, it is important to consider the change to the target population this year, which may influence observed differences from previous years.
- 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 presents findings on how Canadian businesses use, store, and handle the personal information they collect from customers.

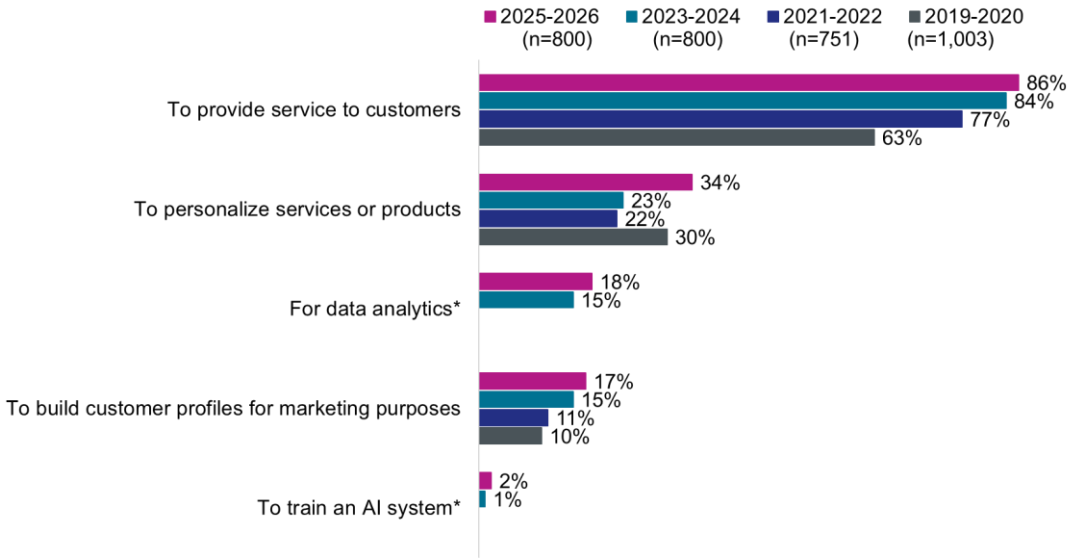
Most Canadian businesses use customer information primarily to provide services

Most representatives of the businesses surveyed (86%) reported that their company uses customer information to provide service to customers. Results are virtually unchanged from 2023, but reflect a sustained increase since 2019 (63%), with levels rising to 84% in 2023 and holding steady at 86% this year.

About one-third of respondents (34%) said their company uses customer information to personalize services or products, up from 23% in 2023 and 22% in 2021, and slightly higher than in 2019 (30%). Smaller proportions reported using customer information for data analytics (18%) and to build customer profiles for marketing purposes (17%). Business use of customer profiles has been gradually increasing since 2019.

Very few (2%) business representatives said their company uses customer information to train an artificial intelligence (AI) system.

Figure 1: Use of customer information collected by companies



*New categories this year.
Q4. What does your company do with the personal information that it collects about customers? Is it used...? Multiple responses accepted. Base=all respondents. "Don't know" 2025: 6%.

Regionally, companies in Quebec are more likely to use personal information collected about customers to provide them with services (92%, compared to 78% of companies in Atlantic Canada and 83% of those in Ontario). Higher rates are also observed among companies that collect information from minors (92%) and those that use AI in their business operations (93%).

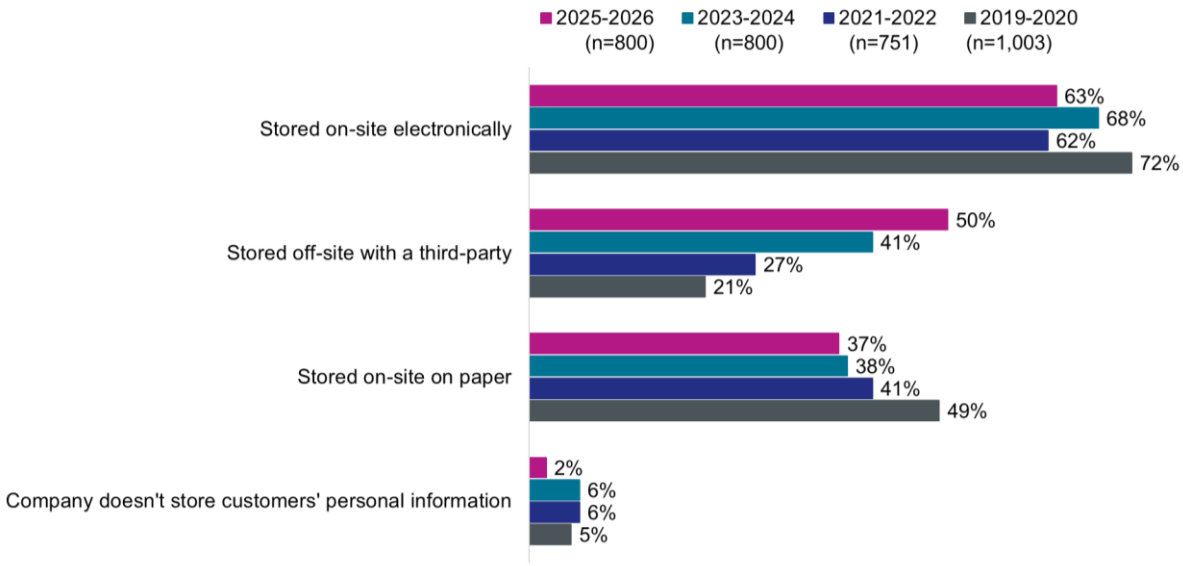
Electronic and cloud storage are the primary methods used by businesses

Nearly two-thirds of business representatives (63%) said their company stores customer information on-site electronically, a slight decline from 2023 (68%), and consistent with 2021 levels (62%).

Half of surveyed businesses (50%) store customer information off-site with a third party, such as a cloud service, continuing a steady increase from 21% in 2019 to 27% in 2021 and 41% in 2023. In contrast, more than one-third (37%) store customer information on-site on paper, continuing a downward trend from 49% in 2019 to 41% in 2021 and 38% in 2023.

Very few business representatives (2%) said their company does not store personal information about customers.

Figure 2: Methods used by companies to store personal information



Q5. How does your company store the personal information of customers? Multiple responses accepted. Base=all respondents. “Don’t know” 2025: 4%.

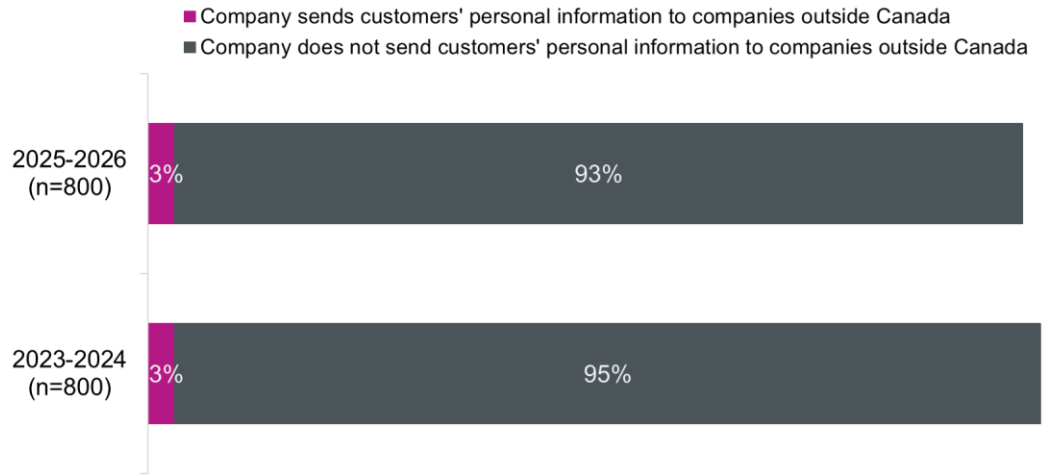
Businesses in Quebec are more likely to store personal information off-site with a third-party (57%, compared to 39% of companies in Atlantic Canada and 44% in western Canada) or store it on-site electronically (69%, compared to 58% of companies in Ontario).

Differences are also observed by company size. Small businesses (1-19 employees) are more likely than medium (20-99 employees) and large (100+ employees) businesses to store personal information on-site in paper form (42%, compared to 31% and 32%, respectively). This is especially true among businesses with fewer than five employees, with 53% reporting on-site paper storage.

Very few companies send customer information outside Canada

Very few business representatives (3%) reported that their company sends customers' personal information to companies outside Canada for processing, storage or other purposes. This is virtually unchanged from 2023.

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



Q6. Does your company send customers' personal information to companies outside Canada for processing, storage or other purposes? Base=all respondents. "Don't know" 2025: 4%.

Most companies[1] that send customers' personal information outside Canada inform their customers that their personal information may be transferred outside Canada.

[1] Due to the very small sample size (n=20), percentages are not reported.

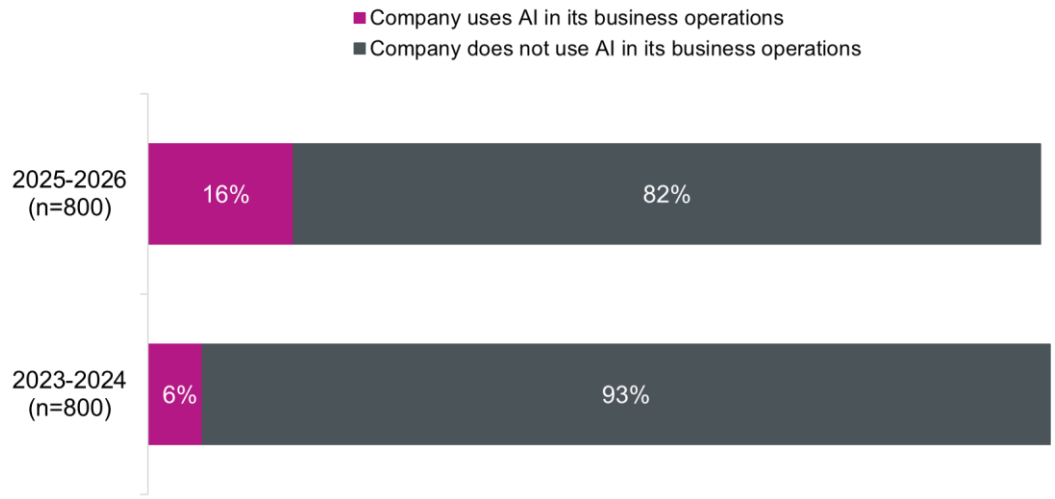
2. Use of AI in business operations

This section examines the use of AI by surveyed companies.

Growing use of AI among Canadian businesses

The proportion of business representatives reporting that their company uses AI for business operations increased from 6% in 2023 to 16% in 2025, though overall levels of use remain low.

Figure 4: Use of AI for business operations



Q8. Does your company use AI for business operations? Base=all respondents. “Don’t know” 2025: 2%.

Use of AI for business operations is higher in Ontario (17%) and western Canada (21%) than elsewhere in the country. Similarly, it is highest among businesses with 100+ employees (29%).

Research and document drafting is the most common use of AI among businesses

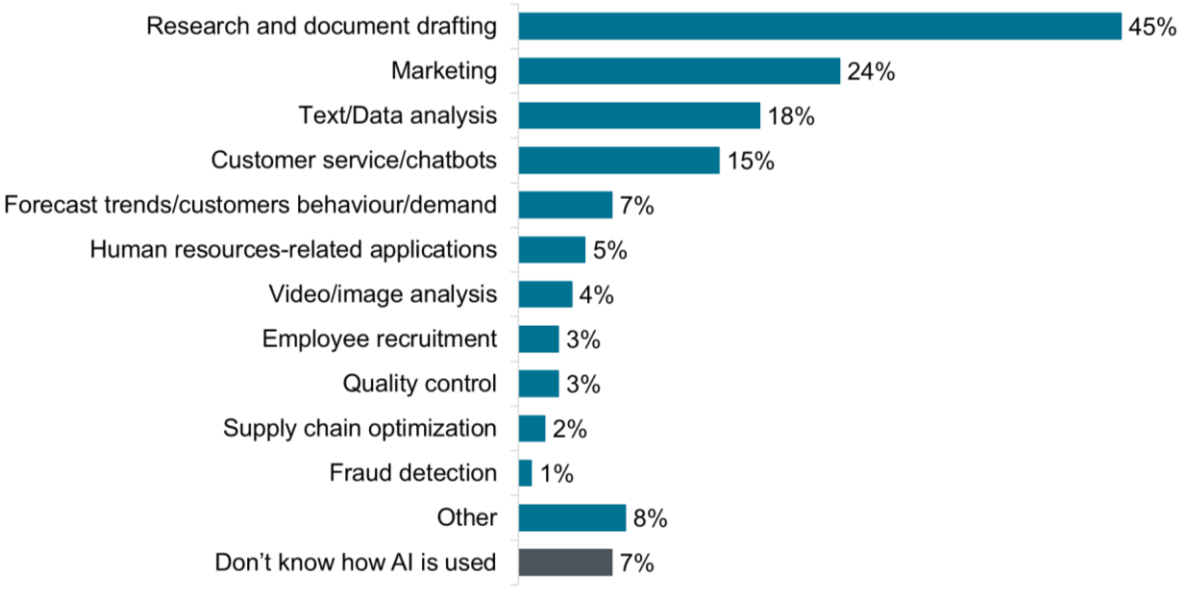
Among Canadian businesses that use AI in their operations (n=113), the most common application is research and document drafting, which was reported by close to half (45%) the survey respondents.

About one-quarter (24%) use AI for marketing, while smaller proportions use it for text or data analysis (18%) and customer service or chatbots (15%).

Fewer businesses reported using AI for other types of business operations. Seven percent use it for forecasting trends or customer behaviour, 5% for human resources-related applications, 4% for video or image analysis, 3% for employee recruitment or quality control, 2% for supply chain optimization, or 1% for fraud detection.

Eight percent reported other uses of AI, while 7% did not know how AI is used in their business operations.

Figure 5: Areas in which companies are using AI



Q9. How is your company using AI in its business operations? Multiple responses accepted
Base: n=113; those using AI in their business operations.

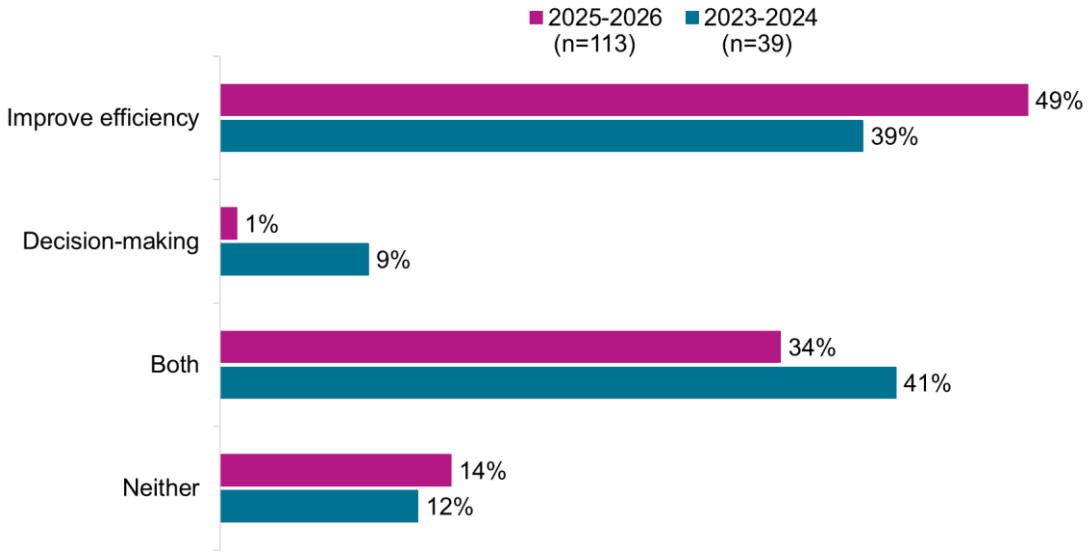
Nearly half of businesses use AI to improve efficiency and to make decisions

Among Canadian businesses that use AI in their operations (n=113), nearly half (49%) reported using it primarily to improve efficiency, compared to 39% in 2023. This difference is not statistically significant and based on a small number of respondents (n=39).

In addition, approximately one-third of respondents (34%) said their company uses AI for both improving efficiency and supporting decision-making, while almost none of the businesses surveyed (1%) use AI exclusively for decision-making.

Fourteen percent of Canadian businesses that use AI do not use it for either operational efficiency or decision-making.

Figure 6: How companies are using AI



Q10. Is AI being used by your company to improve efficiency, for decision-making, or for both? Base=those using AI in their business operations. “Don’t know” 2025: 2%.

Near-unanimous human oversight of AI-driven decisions

Nearly all (97%) surveyed businesses that use AI for both efficiency and decision-making (n=42) reported that a human employee reviews AI-driven decisions before any action is taken by their company. The remainder (3%) did not know whether this human oversight occurs.

Figure 7: Human oversight in AI-driven decision-making

Q11. When your company uses AI for decision-making, does a human employee review the decision before any action is taken by your company? Base: n=42; those using AI in their business operations for both improving efficiency and decision making.

3. Canada's privacy laws and compliance

This section presents findings on companies' awareness of and compliance with their responsibilities under Canada's privacy laws. Before answering these questions, respondents were provided with the following description of Canada's privacy laws.

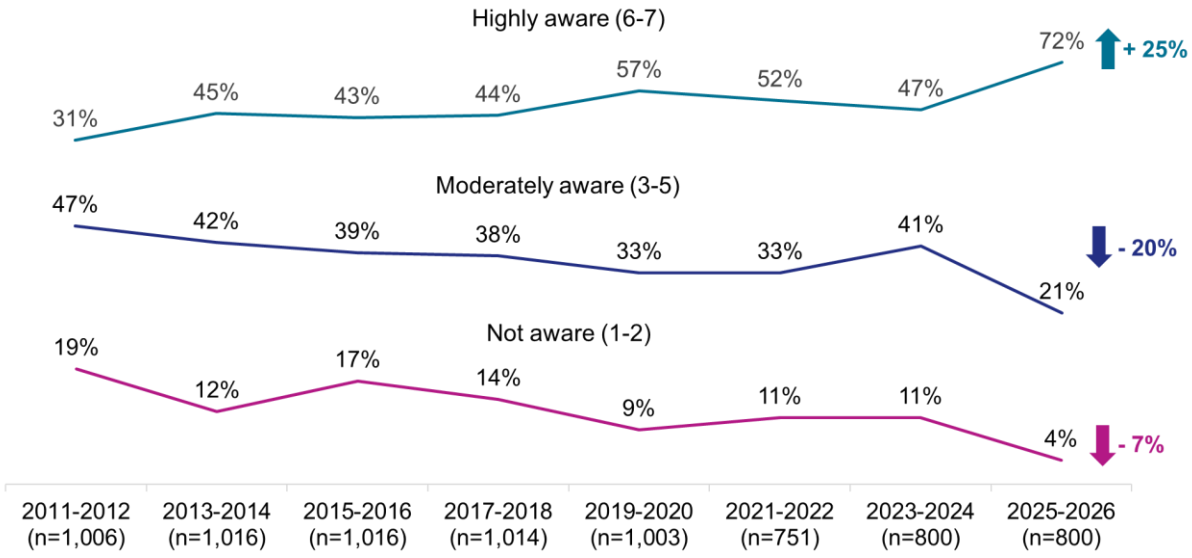
> The federal government's privacy law, the *Personal Information Protection and Electronic Documents Act* or *PIPEDA,* sets out rules that govern how businesses engaged in commercial activities should protect personal information. In Alberta, BC and Quebec, the private sector is governed by provincial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

Most businesses have a high level of awareness of their responsibilities under Canada's privacy laws

Seven in 10 business representatives (72%) 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 21% rated their company as moderately aware (scores of 3 to 5). Taken together, the vast majority (93%) of surveyed companies are at least moderately aware of their privacy-related responsibilities. Few (4%) rated their company's awareness as low (scores of 1 or 2).

Self-reported awareness of responsibilities under Canada's privacy laws is higher this year. Some or all of is increase may be attributable to the change in the target population this year rather than a true increase over time.

Figure 8: Companies' awareness of responsibilities under privacy laws



Net calculations are based on unrounded percentages.
Q12. How would you rate your company's awareness of its responsibilities under Canada's privacy laws? Base=all respondents. "Don't know" 2025: 3%.

Awareness varies by company size and sector. It is higher among large companies (100+ employees) than among small companies (1-19 employees) (79% versus 67%), and it is

higher among companies that are operating in the healthcare and social assistance sector (85%) compared to accommodation and food services (63%), other services (67%), and retail (70%).

9 in 10 businesses have taken steps to comply with Canada's privacy laws

Nine in 10 Canadian businesses (91%) said their company has taken steps to ensure it complies with Canada's privacy laws. Reported compliance has increased compared with recent waves (76% in 2023 and 74% in 2021) and remains well above the baseline of 66% reported in 2017. Some or all of the increase may reflect the change in the target population rather than reflecting a true change over time.

Figure 9: Percentage of companies taking steps to comply with Canada's privacy laws

Q13. Has your company taken steps to ensure it complies with Canada's privacy laws? Base=all respondents. "Don't know" 2025: 4%.

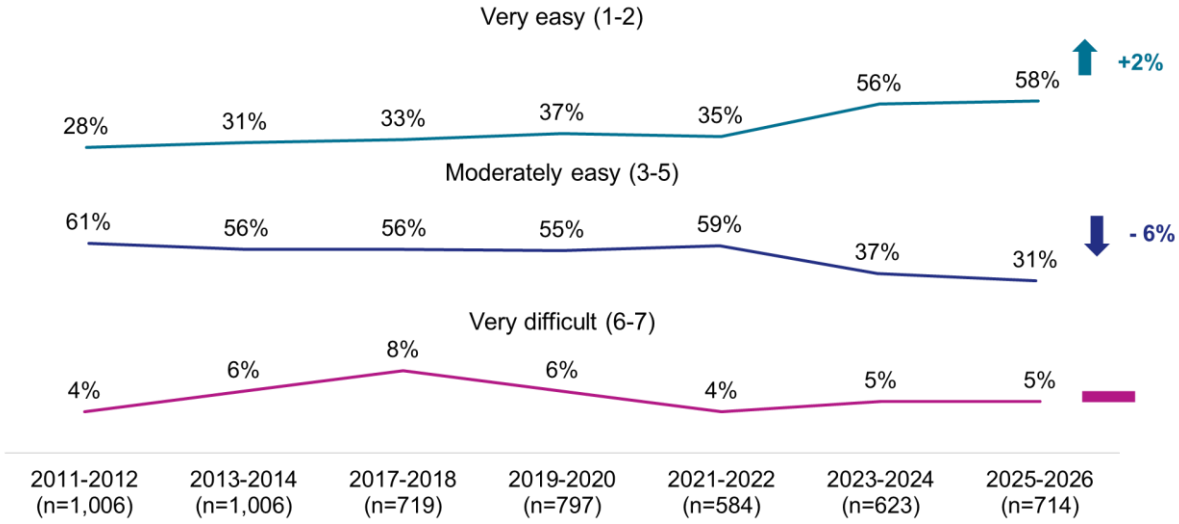
The likelihood of having taken steps to ensure compliance increases with company size and engagement with privacy practices. Large companies (94%) are more likely than small companies (88%) to report taking such steps. Higher rates are also observed among companies with a privacy policy (94%) and those that have used the OPC's compliance information and tools (100%).

Vast majority of companies found it at least somewhat easy to ensure compliance

Among companies that have taken steps to comply with Canada's privacy laws (n=714), 89% reported that doing so has been at least moderately easy. Over half (58%) said compliance has been very easy (scores of 1 and 2 on the 7-point scale), while 31% rated it as moderately easy (scores of 5 to 7). Just 5% of respondents said it was very difficult for their company to comply with Canada's privacy laws.

The proportion of businesses that found it very easy to bring personal information handling practices into compliance with Canada's privacy laws is stable at 58%, after having increased significantly between 2021 (35%) and 2023 (56%). Comparisons with previous years should take into account the change in the target population in 2025.

Figure 10: Ease of complying with Canada's privacy laws



Net calculations are based on unrounded percentages.
Q14. How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws? Base=those who have taken steps to comply with Canadian privacy laws. "Don't know" 2025: 6%.

Fewer businesses in Quebec report that compliance with Canada's privacy laws is very easy (43%).

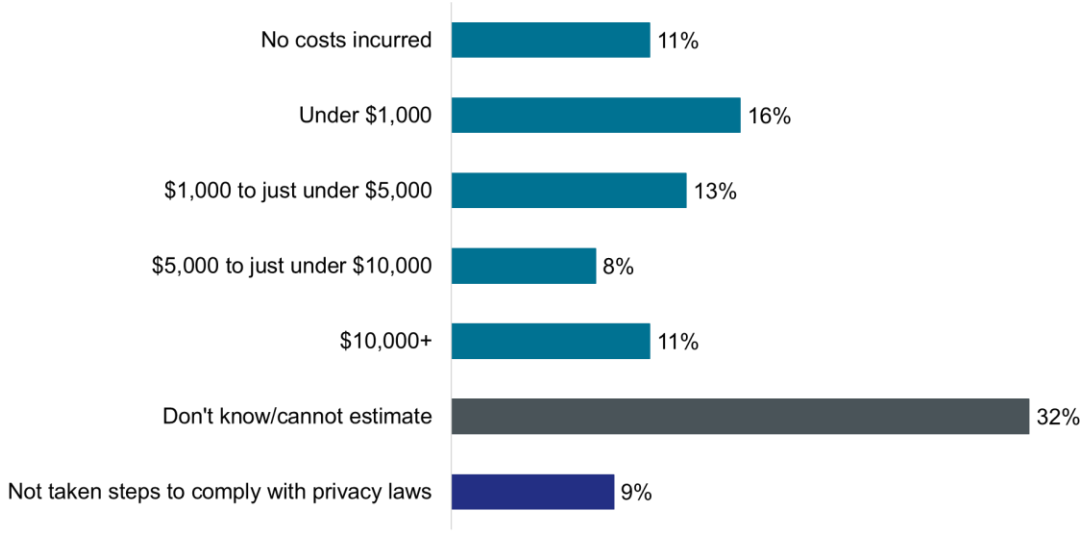
Compliance costs with Canada's privacy laws vary widely among businesses

Canadian businesses reported a range of costs associated with complying with Canada's privacy laws over the past 12 months. The most commonly reported cost was under $1,000 (16%), followed by $1,000 to just under $5,000 (13%). In total, four in 10 businesses reported costs of under $5,000 (29%) or no costs at all (11%). At the same time, two in 10 businesses reported costs of $5,000 or more, including 8% reporting between $5,000 and just under $10,000 and 11% reporting $10,000 or more.

Notably, 9% of businesses indicated they had not taken steps to comply with Canada's privacy laws, and nearly one-third (32%) were unable to estimate the financial cost of compliance.

Respondents were told to include all categories of costs, such as staff time and training, IT, and legal fees, in their estimate. Costs incurred ranged from under $1,000 to $200,000 or more in the last 12 months.

Figure 11: Cost of complying with Canada's privacy laws



Q15. In the past 12 months, which of the following best describes your company's approximate financial cost of complying with Canada's privacy laws. Please include all categories of costs, such as staff time and training, IT, and legal fees. Base: n=800; all respondents.

Small businesses (1-19 employees) are more likely than medium-sized and large businesses to report no costs (14% versus 9% and 6%, respectively) or costs of under $1,000 (19% versus 16% and 11%).

4. Awareness and use of the OPC's resources

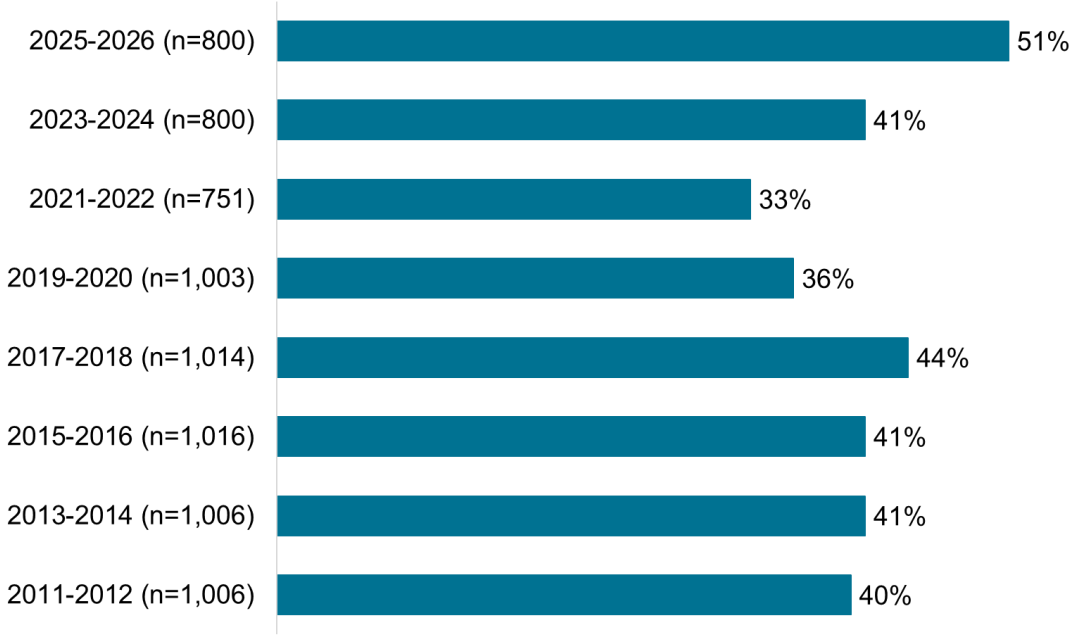
This section presents findings on companies' awareness and use of the OPC's information and tools designed to help companies comply with their privacy obligations.

Half of businesses report awareness of the OPC's privacy compliance resources

Awareness of the OPC's resources has increased in recent years. In 2025, half of business representatives (51%) reported being aware that the OPC has information and tools available to companies to help them comply with their privacy obligations.

This represents an increase compared with 2023 (41%) and 2021 (33%), with awareness at its highest since tracking began. This increase may reflect, in part or in whole, the change in the target population rather than a true increase in awareness of OPC resources over time.

Figure 12: Percentage of companies aware of OPC's resources



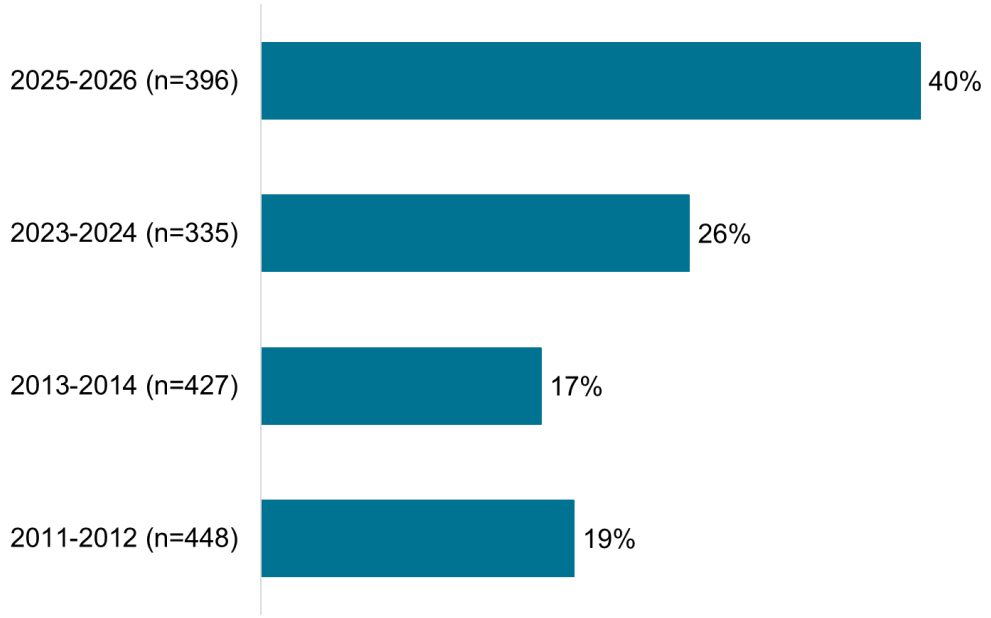
Q16. Are you aware that the Office of the Privacy Commissioner of Canada, or the OPC, has information and tools available to companies to help them comply with their privacy obligations? Base=all respondents. "Don't know" 2025: 1%.

Awareness of the OPC's tools and information is higher among large (100+ employees) and medium-sized (20-99 employees) businesses (57% and 56%, respectively) than among small businesses (1-19 employees) (45%). As well, companies that have taken steps to comply with Canada's privacy laws (54%) and those with a privacy policy (55%) are also more likely to be aware of the OPC's resources.

4 in 10 businesses aware of the OPC's resources report using them

Use of the OPC's information and tools has increased over time among businesses that are aware of them (n=396). In 2025, four in 10 businesses (40%, up from 26% in 2023) reported having used OPC resources. The increase may reflect, in part or in whole, the change in the target population rather than a true increase in the use of OPC resources over time.

Figure 13: Percentage of companies that have used OPC's resources



Q17. Has your company ever used any of these resources? Base=companies aware of OPC's resources. "Don't know" 2025: 19%.

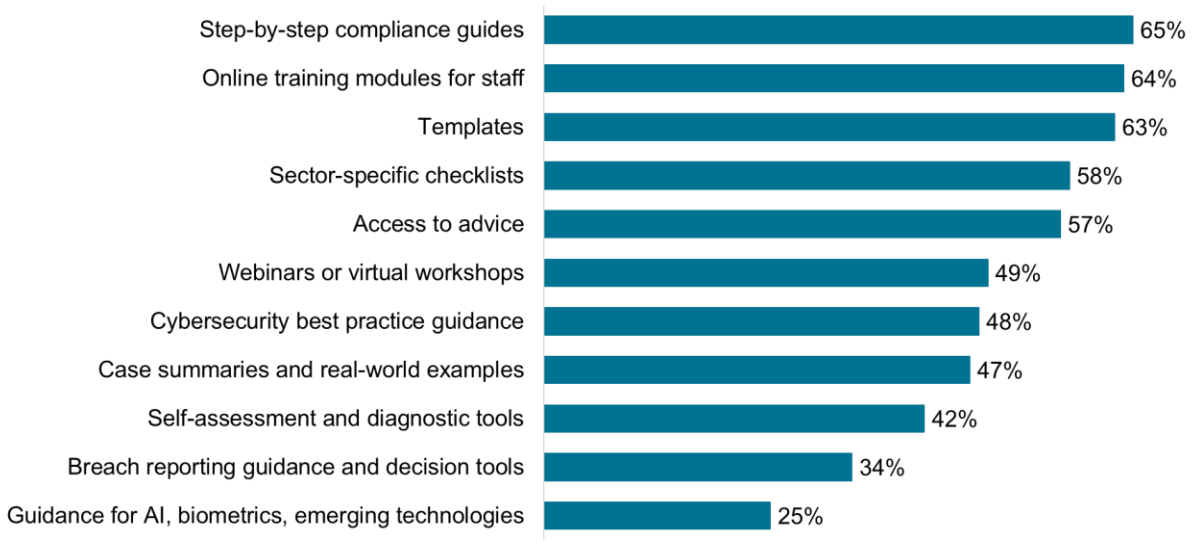
Canadian businesses most often identify practical compliance tools as the most helpful resources

Respondents were presented pairs of potential resources and asked to select which would be most helpful. Results reflect the proportion of times each item was selected when presented. Each respondent was presented two pairs of potential resources.

Companies most often chose practical compliance tools. Step-by-step compliance guides (65%), online training modules for staff (64%), and templates (63%) were most frequently identified as helpful, selected nearly two-thirds of the times they were presented to respondents.

Many also selected sector-specific checklists (58%) and access to advice (57%), while nearly half chose webinars or virtual workshops (49%), cybersecurity best-practice guidance (48%), and case summaries or real-world examples (47%). Self-assessment tools (42%), breach reporting guidance (34%), and guidance on AI and emerging technologies (25%) were selected less frequently than the other tools.

Figure 14: Information and tools viewed as most helpful by companies



Q18. As the person at your company most familiar with the handling of customers' personal information, which of the following information and tools would you find most helpful? [Selection rate (# of times selected ÷ # of times shown)] Base: n=800; all respondents.

5. Company privacy practices

This section presents findings on the procedures and policies companies have in place to protect personal information collected from their customers.

Majority of businesses have designated a privacy officer

Seven in 10 Canadian businesses (72%, up from 56% in 2023) reported having designated someone in their company to be responsible for privacy issues and the personal information the company holds. This increase may reflect, in part or in whole, the change in the target population rather than a true increase in the designation of privacy officers over time.

Figure 15: Percentage of companies with a privacy officer

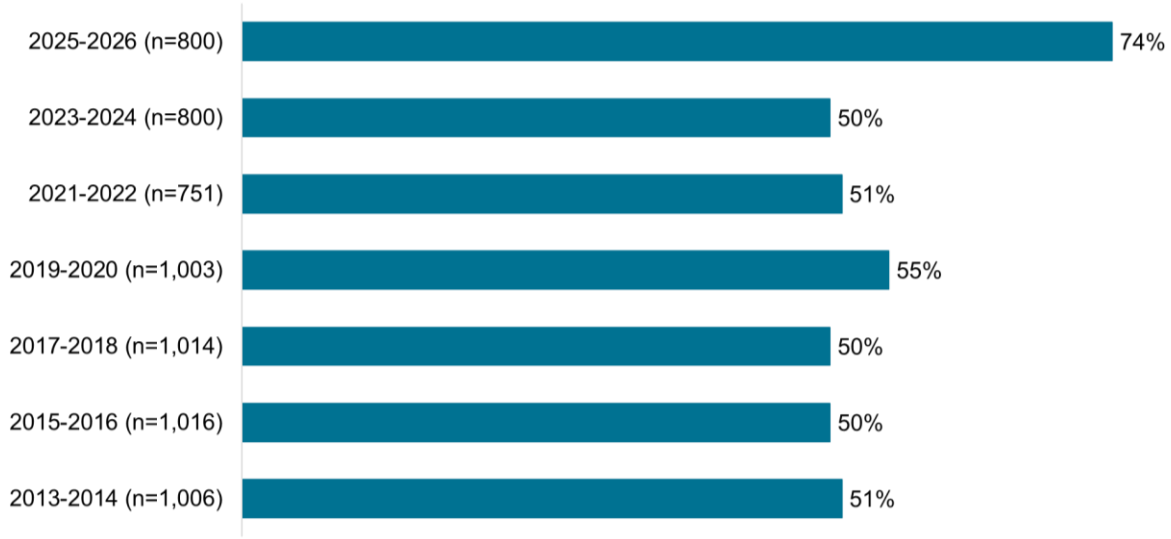
Q19. Have you designated someone in your company to be responsible for privacy issues and personal information that your company holds? Base=all respondents. “Don’t know” 2025: 4%.

The likelihood of designating a privacy officer was higher among companies that have used the OPC’s tools and information (88% compared to 74% of companies that have not used these resources).

Most Canadian businesses have documented privacy policies

Nearly three-quarters (74%, up from 50% in 2023) of business representatives reported that their company has developed and documented internal policies for staff that address their privacy obligations under the law. Comparisons over time should take into account the change to the target population in 2025, which may influence observed differences from previous years.

Figure 16: Percentage of companies with staff policies that address privacy obligations



Q20. Has your company developed and documented internal policies for staff that address your privacy obligations under the law? Base=all respondents. Don't know: 4%.

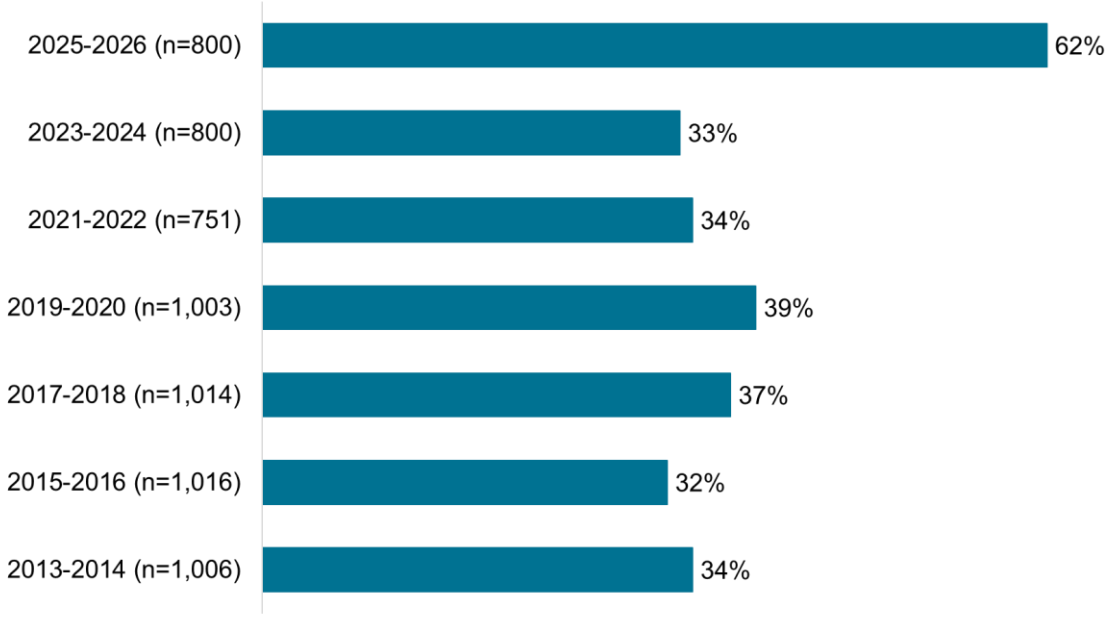
The likelihood of developing and documenting internal policies for staff that address privacy obligations increases with business size, from 64% of small businesses (1-19 employees) to 87% of large businesses (100+ employees).

Regionally, companies in Quebec (66%) are less likely than those in Ontario and western Canada (both 77%) to have such policies in place. Adoption is also higher among companies that have used the OPC's privacy tools (93%).

Six in 10 Canadian businesses provide regular staff privacy training and education

Six in 10 business representatives (62%) reported that their company regularly provides staff with privacy training and education. In previous survey waves, the proportion was considerably lower and relatively stable. Some or all of the increase may be attributable to the change in the target population, rather than a true shift over time.

Figure 17: Percentage of companies providing privacy training and education for staff



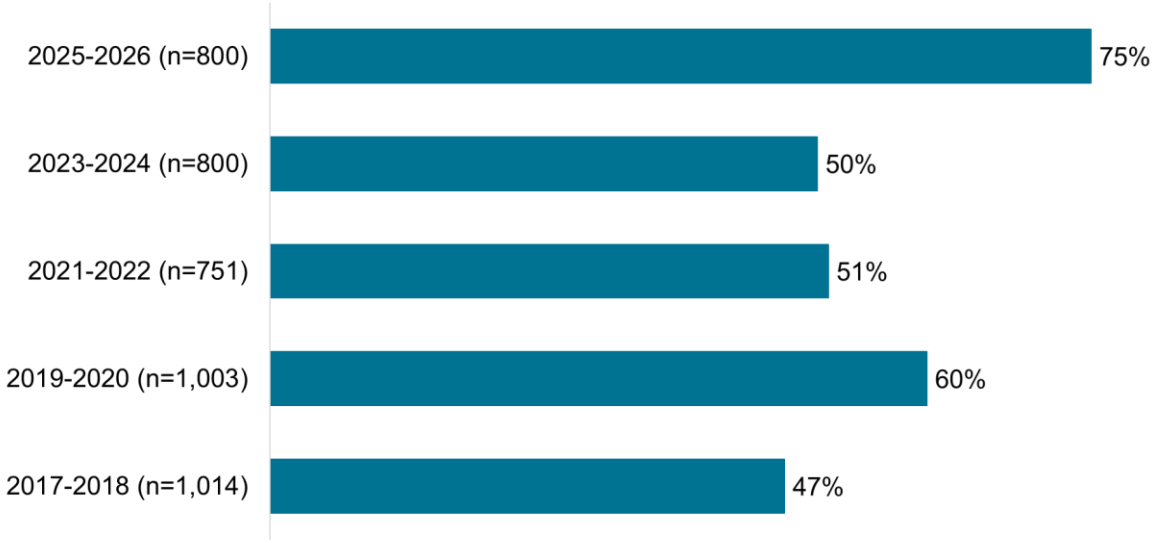
Q21. Does your organization regularly provide staff with privacy training and education? Base=all respondents. “Don’t know” 2025: 1%.

The likelihood of providing regular privacy training and education for staff increases with business size, from 55% of small businesses to 76% of large businesses. Regionally, companies in Quebec (48%) are less likely than those in Ontario (70%) and western Canada (62%) to provide such training and education. Implementation is also higher among companies that have used the OPC’s privacy tools (84%).

Most businesses have procedures for personal information access requests

Three-quarters (75%, compared to 50% in 2023) of business representatives reported that their company has procedures in place to respond to customer requests for access to their personal information. Differences over time may reflect the change in the target population this year rather than true shifts over time.

Figure 18: Percentage of companies with procedures for customer information requests



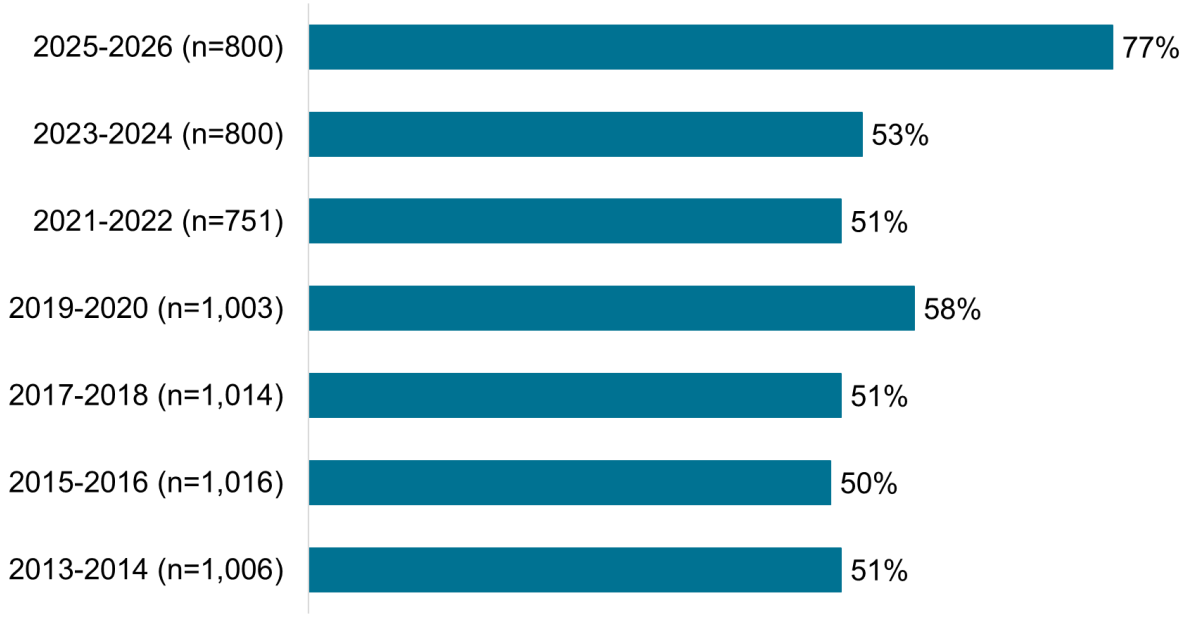
Q22. Does your company have procedures in place for responding to customer requests for access to their personal information? Base=all respondents. “Don’t know” 2025: 4%.

Businesses in Quebec (63%) are less likely than businesses in Ontario and western Canada (79% each) to have procedures for responding to customer requests for personal information. When it comes to business size, these procedures are more common among large businesses (100+ employees) than among small businesses (1-19 employees) (81% versus 72%).

Nearly 8 in 10 businesses report procedures for handling privacy complaints

Just under eight in 10 businesses (77%) have procedures in place to handle complaints from customers who believe their personal information has been handled improperly. In earlier survey waves, roughly half of the business representatives surveyed reported that their company had such procedures. Differences over time may reflect the change in the target population this year rather than true shifts over time.

Figure 19: Percentage of companies with procedures for privacy complaints



Q23. Does your company have procedures in place for dealing with complaints from customers who feel that their information has been handled improperly? Base=all respondents. “Don’t know” 2025: 3%.

Businesses in Quebec (67%) are less likely than those in Ontario and western Canada (both 80%) to have procedures for privacy complaints. In addition, these procedures are more common among larger businesses (83% of companies with 20-99 employees and 85% of companies with 100+ employees) than among small businesses with 1-19 employees (68%). Implementation of such procedures is also higher among companies that have used the OPC’s privacy tools (96%).

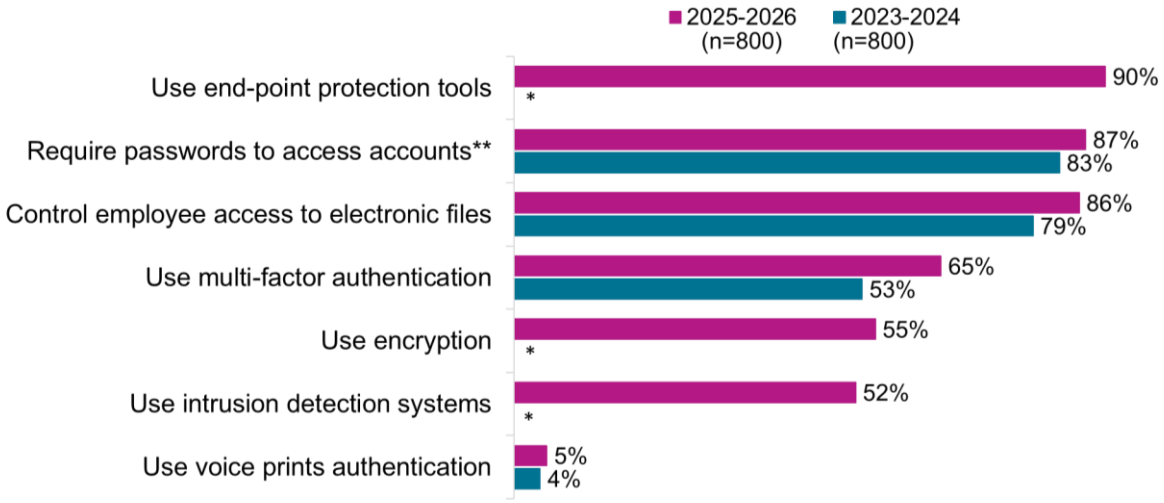
Use of basic security measures is widespread, but adoption of more advanced protections varies

Business representatives reported that their company takes a range of actions to safeguard customers’ personal information. The most common measures include using end-point protection tools (90%), requiring passwords to access accounts (87%), and controlling employee access to electronic files (86%).

Many businesses also reportedly use multi-factor authentication (65%), while just over half use encryption (55%) and intrusion detection systems (52%). A very small proportion use voice print authentication (5%).

The use of several measures has increased since 2023. More companies require passwords to access accounts (87%, compared to 83% in 2023), control employee access to electronic files (86% versus 79%), and use multi-factor authentication (65% versus 53%). Comparisons to 2023 should take into account the change to the target population in 2025.

Figure 20: Actions taken to safeguard personal data



*Not a response option in 2023.
Q24. Does your company take any of the following actions to safeguard the personal information of customers? [Multiple responses accepted] Base=all respondents. Split sample of respondents in 2025 (n=458-472), unless indicated with two asterisks [**].

Regionally, companies in Ontario and western Canada are more likely to use encryption (64% and 63%, respectively) and multi-factor authentication (76% and 72%, respectively) to safeguard the personal information of customers.

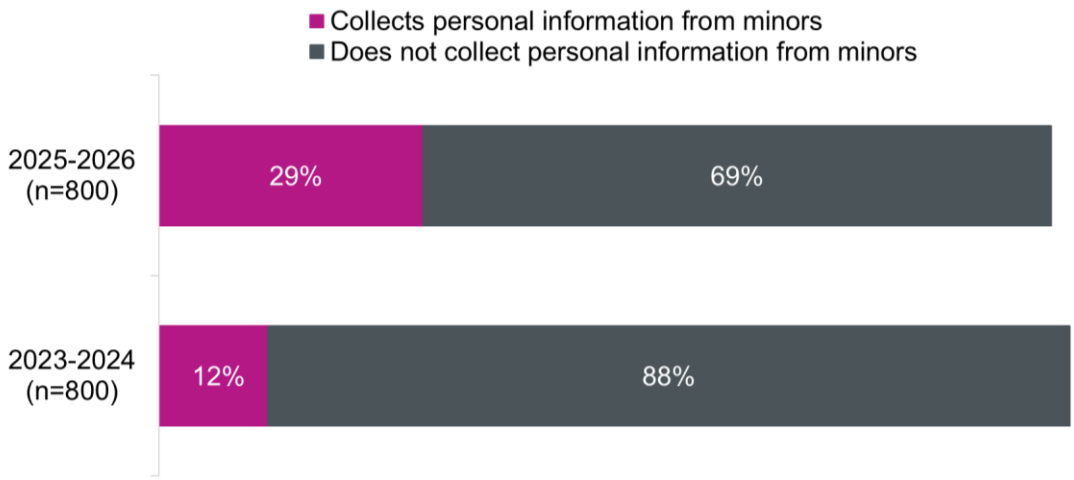
6. Collection of personal information from minors

This section presents findings on the procedures and policies companies have in place to protect the personal information collected from customers under the age of 18.

3 in 10 businesses collect personal information from minors

Three in 10 business representatives (29%) reported that their company collects personal information from customers who are minors (under the age of 18). In 2023, fewer companies (12%) were reportedly collecting personal information from customers under the age of 18. This difference may reflect the change in the target population this year rather than a true shift over time.

Figure 21: Percentage of companies collecting personal information from minors



Q25. Does your company collect personal information from customers who are minors, that is under the age of 18? Base=all respondents. “Don’t know” 2025: 2%.

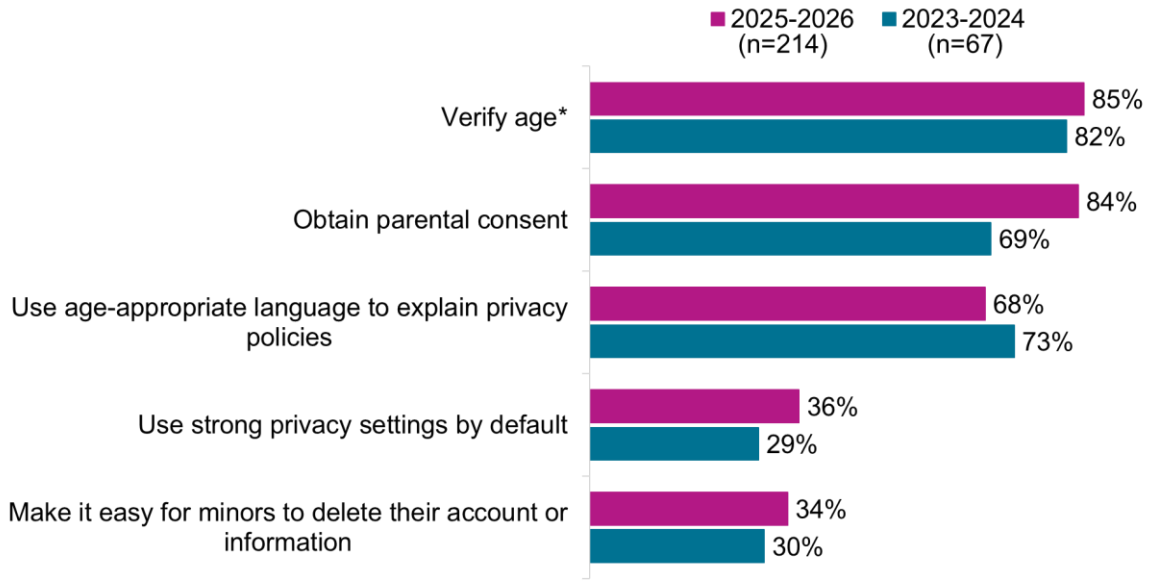
Companies in Quebec (35%) and Ontario (30%) are more likely to collect information from minors compared to companies operating in western Canada (22%).

Most companies verify age and obtain parental consent, but fewer implement stronger protections for young people

Among companies that collect personal information from young people (n=214), most verify age (85%) and obtain parental consent if the young person is under 13 (84%). In addition, approximately two-thirds (68%) explain their privacy policies and practices in simple, age-appropriate language. Fewer companies use strong privacy settings by default, such as automatically turning off location tracking (36%) or make it easy for young people to delete their account or information they have posted (34%).

Compared to 2023, considerably more companies are obtaining parental consent when collecting information from young people (84% in 2025 versus 69% in 2023). This may be attributable, at least in part, to the change in the target population this year. Other differences are not statistically significant due to the small sample sizes.

Figure 22: Actions taken when collecting information from minors



Q26. When collecting information from young people, does your company do any of the following? Please answer yes or no. Base: Companies that collect information from minors. In 2025, split sample (n=122-126), unless indicated with an asterisk [*].

Companies in Quebec (94%) are more likely to verify age compared to companies operating in Ontario (82%) and western Canada (79%).

7. Privacy policies

This section presents findings on privacy policies and how companies communicate their privacy practices.

A strong majority of Canadian businesses have a privacy policy

Eight in 10 (84%) business representatives said their company has a privacy policy. This represents an increase compared with previous waves of the survey. Differences over time may reflect the change in the target population this year rather than true shifts over time.

Figure 23: Percentage of companies that have a privacy policy

Q27. Does your company have a privacy policy? Base=all respondents. “Don’t know” 2025: 3%.

Companies in Quebec (88%) and Ontario (86%) are more likely to have a privacy policy compared to those in western Canada (78%). Use of a privacy policy also increases with business size, from 78% of small businesses (1-19 employees) to 92% of large businesses (100+ employees). Privacy policies are also more common among companies that have used the OPC’s privacy tools (97%).

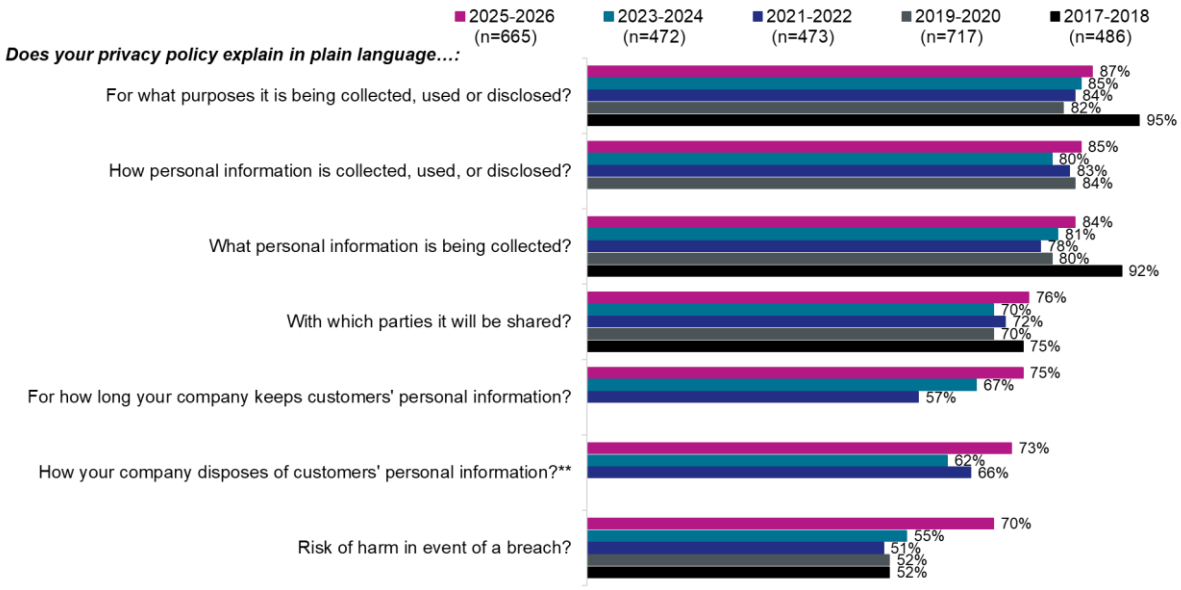
Most privacy policies explain key information-handling practices in plain language

Most business representatives whose company has a privacy policy (n=665) reported that it explains in plain language key elements of their information-handling practices. Nearly nine in 10 (87%) said their policy outlines the purposes for which personal information is collected, used or disclosed. Similarly, large majorities indicated that their policy explains how personal information is collected, used or disclosed (85%), as well as what personal information is collected (84%).

Approximately three-quarters of business representatives reported their company’s privacy policy explains with whom information may be shared (76%), how long personal information is retained (75%), and how it is disposed of (73%). Seven in 10 (70%) said their policy also describes the risk of harm in the event of a breach.

Compared with earlier waves, results point to modest gains across several measures. The share explaining data retention periods increased from 67% in 2023 to 75% in 2025, while explanations of data disposal practices increased from 62% to 73%. Disclosure of the risk of harm in the event of a breach also improved, increasing from 55% in 2023 to 70% in 2025. Differences over time may reflect the change in the target population this year rather than true shifts over time.

Figure 24: Privacy policy disclosures



*Not measured in previous years.
Q28. Does your privacy policy explain in plain language...? Base=companies that have a privacy policy. In 2025, statements were asked of split samples (n=337) unless indicated with a double asterisk [**].

Customer-facing privacy communication is fairly widespread, though some practices are less common

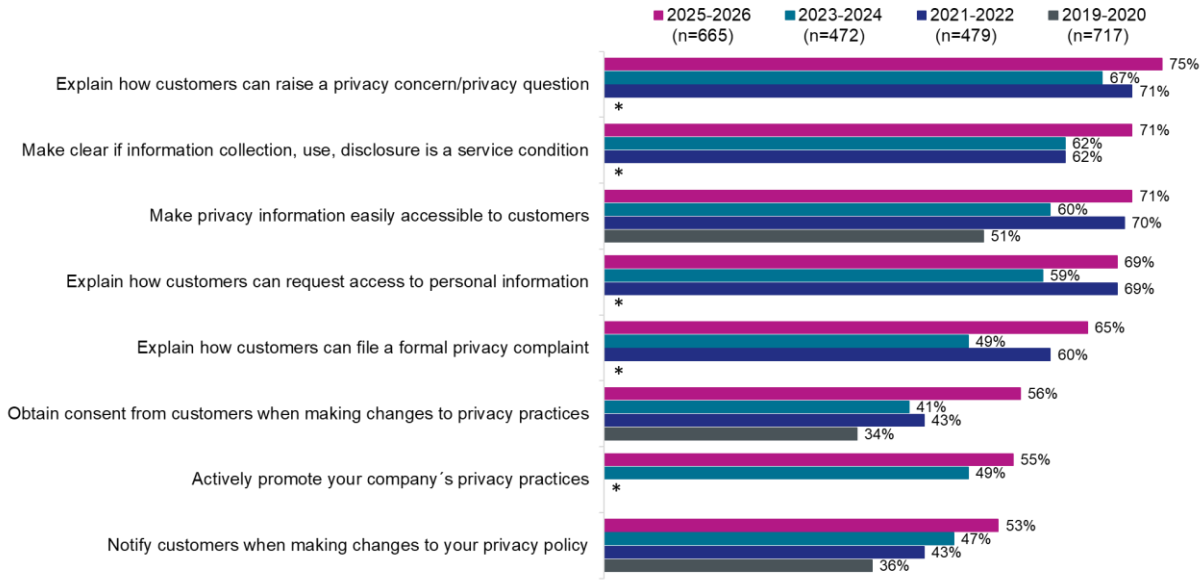
Among companies that have a privacy policy (n=665), many communicate key privacy practices to customers. Three-quarters (75%) of business representatives said their company explains how customers can raise a privacy concern or ask a privacy-related question. In addition, seven in 10 make clear when the collection, use or disclosure of personal information is a condition of service (71%), make privacy information easily accessible to customers (71%), and explain how customers can request access to their personal information (69%). Two-thirds (65%) of companies explain how customers can file a formal privacy complaint.

About half of companies report additional communication practices, including obtaining consent from customers when making changes to privacy practices (56%), actively promoting their company's privacy practices (55%), and notifying customers when changes are made to the privacy policy (53%).

The proportion of companies that communicate elements of their privacy practices has increased since 2023. Comparisons over time should take into account the change to the

target population this year, as differences may reflect this change, at least in part, rather than true shifts over time.

Figure 25: Communication of company privacy practices



*Not measured in previous years.
Q29. Does your company do any of the following? Base: Companies that have a privacy policy. In 2025, all statements asked of split samples (n=337).

Companies in Quebec (56%) are less likely than those operating in Ontario (78%) and western Canada (73%) to make clear whether the collection, use, or disclosure of personal information is a condition of service.

8. Data breaches

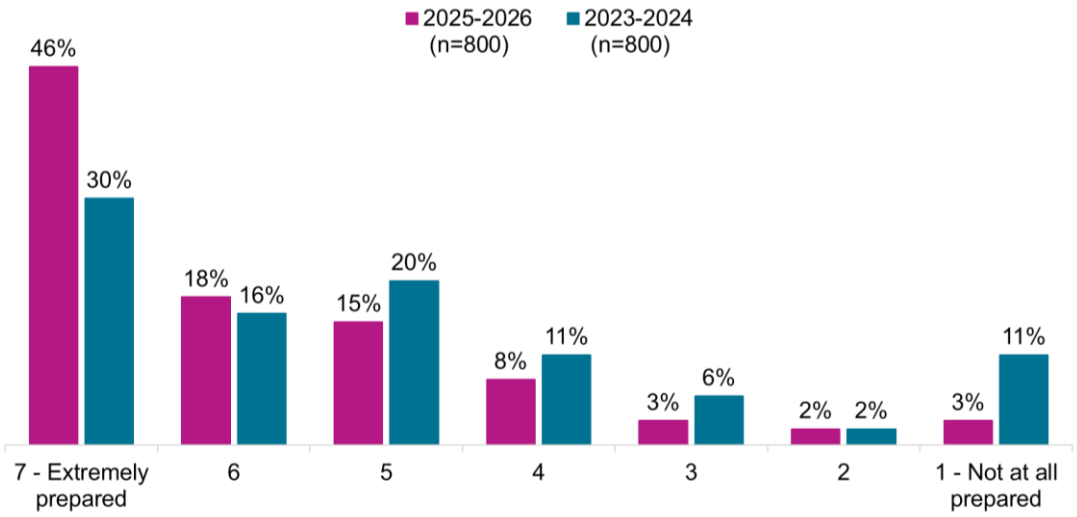
This section presents findings on Canadian business' preparedness for data breaches and experience with them.

Nearly two-thirds of businesses are highly prepared to respond to a data breach

Nearly two-thirds of business representatives (64%) said their company is highly prepared to respond to a data breach involving personal information (scores of 6 or 7 on the 7-point scale), including 46% who consider their company extremely prepared. One-quarter (26%) rated their company as moderately prepared (scores of 3 to 5). Overall, the vast majority (90%) of surveyed companies are at least moderately prepared to respond to a data breach, while few (5%) indicated low preparedness (scores of 1 or 2).

Compared with 2023, perceptions of preparedness have improved, with the proportion rating their company as highly prepared (scores of 6 or 7) increasing from 46% to 64% in 2025. Comparisons over time should take into account the change to the target population this year, as differences may reflect this change, at least in part, rather than true shifts over time.

Figure 26: Preparedness to deal with data breaches



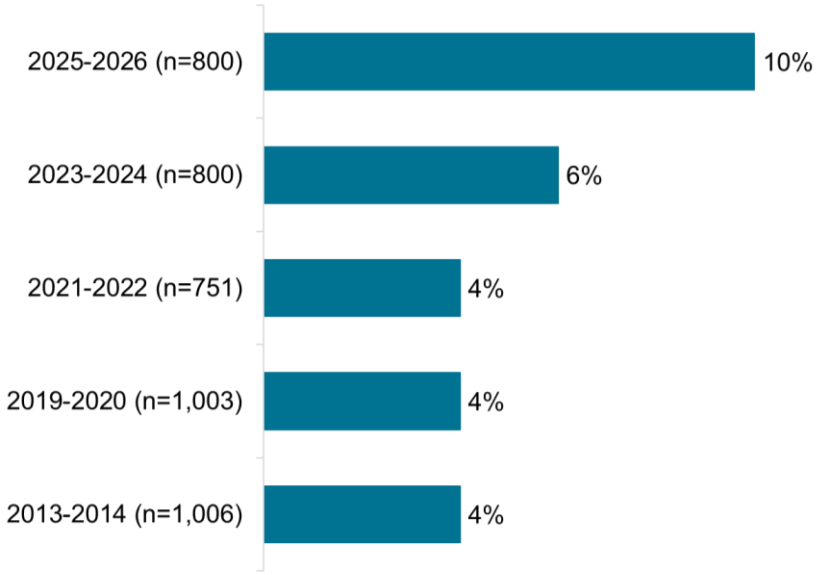
Q30. To what extent is your company prepared to respond to a data breach involving personal information? Please use a scale of 1 to 7, where 1 is not at all prepared to respond in the event of a privacy breach, and 7 is extremely prepared to respond. Base=all respondents. "Don't know" 2025: 4%.

Perceptions of being highly prepared increase with business size, from 57% among small businesses (1-19 employees) to 77% among large businesses (100+ employees). It is also higher among business that have used the OPC's tools (78%).

Reported data breaches among businesses have increased

One in 10 business representatives (10%) reported that their company has experienced a breach where the personal information of customers was compromised, up from 6% in 2023. Differences over time may reflect the change in the target population this year rather than true shifts over time.

Figure 27: Percentage of companies that have experienced a privacy breach

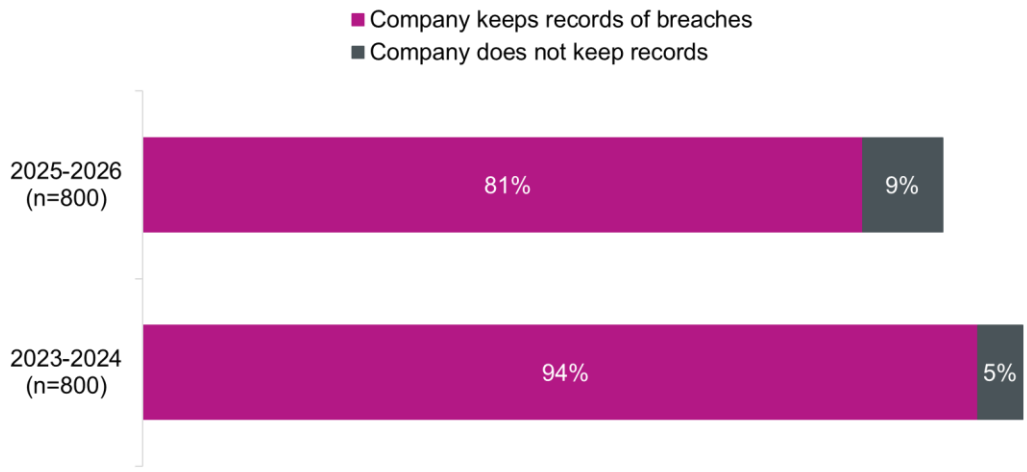


Q31. Has your company ever experienced a breach where the personal information of your customers was compromised? Base=all respondents. “Don’t know” 2025: 5%.

8 in 10 businesses report keeping records of data breaches

A large majority of business representatives reported that their company keeps records of data breaches involving customers' personal information. This year, 81% said their company keeps records of such breaches, down from 94% in 2023. The decrease may reflect, in part or in whole, the change in the target population this year rather than a true decline in record keeping.

Figure 28: Record keeping for data breaches



Q32. Does your company ensure that it keeps records of all data breaches involving your customers' personal information? Base=all respondents. "Don't know" 2025: 11%.

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.

Region	Percent
Atlantic Canada	38%
Quebec	24%
Ontario	45%
Prairies	7%
Alberta	10%
British Columbia (including the Territories)	10%

Number of employees	Percent
1 employee (self-employed)	7%
2-4 employees	13%
5-9 employees	14%
10-19 employees	12%
20-99 employees	32%
100+ employees	22%

Industry/sector	Percent
Accommodation, and Food Services	13%
Arts, Entertainment and Recreation	7%
Educational Services	5%
Finance and Insurance	7%
Health Care and Social Assistance	14%
Information and Cultural Industries	1%
Other Services (except Public Administration)	12%
Professional, Scientific and Technical Services	5%
Public Administration	2%
Real Estate and Rental and Leasing	5%
Retail Trade	21%
Transportation and Warehousing	7%
Other	2%

Respondent position	Percent
Manager (general)	44%
Owner, President, or CEO	25%
Administration	7%
Director (general)	5%
HR/Operations	5%
Vice President	1%
Privacy analyst/officer/coordinator	1%

Legal counsel/lawyer	1%
Accountant/Bookkeeper	1%
Chief Financial Officer	1%
Controller	1%
IT Manager	<1%
Office Manager	<1%
Secretary	<1%
Marketing and Sales	<1%
Other	9%

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? The Office of the Privacy Commissioner of Canada is conducting a survey. 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 Office of the Privacy Commissioner of Canada to better understand the needs and practices of companies 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 Office of the Privacy Commissioner of Canada to better understand the needs and practices of companies 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: 20251230-PH822. If further validation is needed, offer to email them the background letter from the OPC.

Screening and background information

1. Does your company sell or offer services or products directly to individual consumers?

   01. Yes

02. No [THANK AND TERMINATE]
99. [DO NOT READ] Don't know/refusal [THANK AND TERMINATE]

INTERVIEWER NOTE:
*IF ASKED ABOUT "CONSUMERS", SAY: This refers to an individual not a companies or organization.

2. Does your company collect personal information about customers?

01. Yes
02. No [THANK AND TERMINATE]
99. [DO NOT READ] Don't know/refusal [THANK AND TERMINATE]

INTERVIEWER NOTE:
*IF ASKED ABOUT "PERSONAL INFORMATION", SAY: By personal information, I mean things like a customer's name, email address, opinions, or financial information, but it can also include fingerprints or voice prints, photos or videos, instant message histories, or biometric data.

3. 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. 500-699
13. 700-799
14. 800-999
15. 1,000-2,499
16. 2,500-4,999
17. 5,000 or more
99. [DO NOT READ] Don't know/refusal [THANK AND TERMINATE]

Section 1. Customers' Personal Information

To start, I'd like to ask about the personal information your company collects about customers.

4. What does your company do with the personal information that it collects about customers? Is it used ...? [READ LIST. ROTATE ITEMS. 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
99. [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.

5. How does your company store the personal information of customers? Is the information…? [READ LIST. ROTATE ITEMS. 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. [VOLUNTEERED] Company does not store personal information about customers
   99. [DO NOT READ] Don't know

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

   01. Yes
   02. No [SKIP TO Q8]
   99. [DO NOT READ] Don't know [SKIP TO Q8]

7. [IF Q6=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
   99. [DO NOT READ] Don't know

Section 2: Technology

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

   01. Yes
   02. No [SKIP TO Q12]
   99. [DO NOT READ] Don't know [SKIP TO Q12]

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. Text/Data analysis
11. Research and document drafting
12. 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
99. [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.

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 companies should protect personal information. In Alberta, British Columbia and Quebec, the private sector is governed by provincial laws, which are similar to the federal law.

12. 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.

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

01. Yes
02. No [SKIP TO Q16]
99. [DO NOT READ] Don't know [SKIP TO Q16]

14. [IF Q13=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.

15. In the past 12 months, which of the following best describes your company's approximate financial cost of complying with Canada's privacy laws. Please include all categories of costs, such as staff time and training, IT, and legal fees. Is it…? [READ LIST; STOP WHEN THE RESPONDENT SELECTS AN ITEM] [NEW]

    01. No costs incurred
    02. Under $1,000
    03. $1,000 to just under $5,000
    04. $5,000 to just under $10,000
    05. $10,000 to just under $20,000
    06. $20,000 to just under $30,000
    07. $30,000 to just under $40,000
    08. $40,000 to just under $50,000
    09. $50,000 to just under $100,000
    10. $100,000 to just under $150,000
    11. $150,000 to just under $200,000
    12. $200,000 or more
    98. Prefer to not answer
    99. Don't know / Can't estimate

16. 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 [SKIP TO Q18]
    03. [DO NOT READ] Not aware of the OPC [SKIP TO Q18]
    99. [DO NOT READ] Don't know [SKIP TO Q18]

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

17. [IF Q16=01] Has your company ever used any of these resources? [READ LIST]

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

18. [IF Q16=02, 03 or 99, ADD: The OPC produces resources for companies to help them comply with their privacy obligations.] As the person at your company most familiar with the handling of customers' personal information, which of the following information and tools would you find most helpful? The first one is [ITEM 1] OR [ITEM 2]. REPEAT. [RANDOMIZED PAIRED COMBINATIONS ENSURING EACH ITEM APPEARS EQUALLY; TWO PER RESPONDENT; DO NOT REPEAT QUESTION UNLESS NEEDED.] [NEW]

    01. Step-by-step compliance guides
    02. Sector-specific checklists
    03. Templates (privacy policies, consent forms, data retention policies)

04. Breach reporting guidance and decision tools
05. Online training modules for staff
06. Webinars or virtual workshops
07. Self-assessment and diagnostic tools
08. Guidance for AI, biometrics, and/or other emerging technologies
09. Cybersecurity best practice guidance
10. Access to advice (help desk, email support, office hours)
11. Case summaries and real-world examples

Section 4: Company Privacy Practices

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

19. 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

20. Has your company 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

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

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

22. 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

23. 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

24. Does your company take any of the following actions to safeguard the personal information of customers? Please answer yes or no. [MODIFIED SINCE 2023: EMPLOYEES REMOVED] [READ ITEMS; ROTATE ITEMS]

    a. Require passwords to access accounts
    b. [SPLIT SAMPLE: 50%] Use multi-factor authentication
    c. [SPLIT SAMPLE: 50%] Use voice prints authentication
    d. [SPLIT SAMPLE: 50%] Use encryption

e. [SPLIT SAMPLE: 50%] Control employee access to electronic files
f. [SPLIT SAMPLE: 50%] Use intrusion detection systems [NEW]
g. [SPLIT SAMPLE: 50%] Use end-point protection tools, such as anti-malware or antivirus software [NEW]

RESPONSE OPTIONS:

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

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

01. Yes
02. No [SKIP TP Q27]
99. [DO NOT READ] Don't know [SKIP TO Q27]

26. [IF Q25=01] When collecting information from young people, does your company do any of the following? Please answer yes or no. [READ ITEMS; ROTATE ITEMS]

a. Verify age
b. [SPLIT SAMPLE: 50%] Obtain parental consent if under 13
c. [SPLIT SAMPLE: 50%] Explain privacy policies and practices in simple, age-appropriate language
d. [SPLIT SAMPLE: 50%] Use strong privacy settings by default, for example, automatically turning off location tracking
e. [SPLIT SAMPLE: 50%] 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

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

01. Yes
02. No [SKIP TO Q30]
99. [DO NOT READ] Don't know [SKIP TO Q30]

28. [IF Q27=01] Does your privacy policy explain in plain language...? [READ LIST; ROTATE ITEMS; SPLIT SAMPLE]

a) [SPLIT SAMPLE: 50%] How your company collects, uses and discloses customers' personal information?
b) [SPLIT SAMPLE: 50%] What personal information your company is collecting from customers?

c) [SPLIT SAMPLE: 50%] The reason customers' personal information is being collected, used or disclosed?
d) [SPLIT SAMPLE: 50%] With which parties customers' personal information will be shared?
e) [SPLIT SAMPLE: 50%] For how long your company keeps customers' personal information?
f) [SPLIT SAMPLE: 50%] The risk of harm to the individual, if any, in the event of data breach?
g) ALL 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…

29. [IF Q27=01] Does your company do any of the following? [READ LIST; ROTATE ITEMS; SPLIT SAMPLE]

a) [SPLIT SAMPLE: 50%] Notify customers when making changes to your company's privacy policy?
b) [SPLIT SAMPLE: 50%] Obtain consent from customers when making changes to your company's privacy practices?
c) [SPLIT SAMPLE: 50%] Make clear whether the collection, use or disclosure of information is a condition of service?
d) [SPLIT SAMPLE: 50%] Make privacy information easily accessible to your customers?
e) [SPLIT SAMPLE: 50%] Explain how customers can raise a privacy concern or ask a privacy question?
f) [SPLIT SAMPLE: 50%] Explain how customers can request access to their personal information?
g) [SPLIT SAMPLE: 50%] Explain how customers can file a formal privacy complaint?
h) [SPLIT SAMPLE: 50%] 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

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

30. 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.

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

    01. Yes
    02. No [SKIP TO Q33]
    99. [DO NOT READ] Don't know [SKIP TO Q33]

32. [IF Q31=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.

33. 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. Arts, Entertainment and Recreation
    03. Educational Services
    04. Finance and Insurance
    05. Health Care and Social Assistance
    06. Information and Cultural Industries
    07. Other Services (except Public Administration)
    08. Professional, Scientific and Technical Services
    09. Public Administration
    10. Real Estate and Rental and Leasing
    11. Retail Trade
    12. Transportation and Warehousing
    88. Other. Please specify:
    99. Don't know/no response

34. What is your own position within your company? [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.