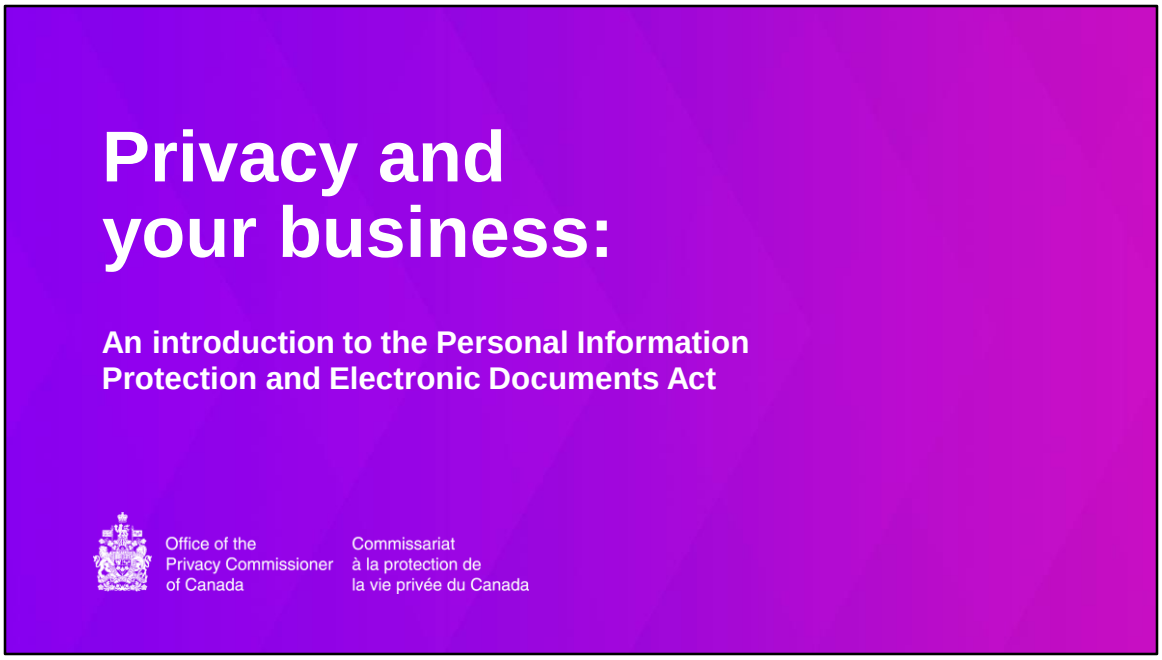
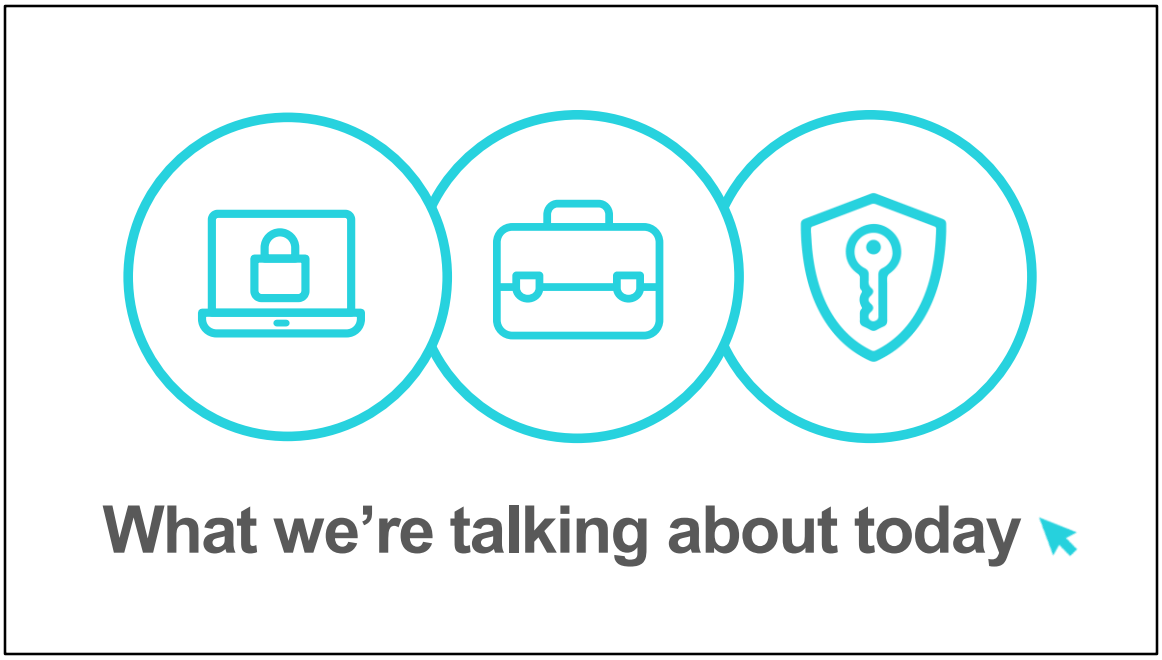


SLIDE (1) Title Slide

PRIVACY AND YOUR BUSINESS:

An introduction to the *Personal Information Protection and Electronic Documents Act.*



SLIDE (2)

WHAT WE'RE TALKING ABOUT TODAY

Today, we'll be talking about the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the federal private sector privacy law.

The goal of this presentation is to offer you information to help your business comply with the federal privacy law, and to help you learn why good privacy practices are good for business.

Today, we'll cover:

- The role of the Office of the Privacy Commissioner or Canada
- Overview of PIPEDA and who it applies to
- Why privacy is important
- What Canadians think about privacy
- PIPEDA's 10 fair information principles

SLIDE (3)

THE ROLE OF THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

The Office of the Privacy Commissioner of Canada (OPC) oversees both the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*, also known as PIPEDA.

These laws establish rules for how federal government institutions and commercial organizations, respectively, handle personal information.

The OPC's core responsibility is to protect Canadians' privacy rights. This is done by conducting investigations, promoting awareness and understanding of privacy rights and obligations, and providing advice to Parliament on potential privacy implications of proposed legislation and government programs.

The OPC has practical resources on its website – www.priv.gc.ca – to support and guide you and your business in protecting your customers and employees' privacy rights and meeting your legal obligations.

SLIDE (4)

PIPEDA IN BRIEF

So, what exactly is PIPEDA?

In a nutshell, PIPEDA is a federal law that sets out the rules for the collection, use, and disclosure of personal information in the course of commercial activities.

PIPEDA outlines ten (10) Fair Information Principles that businesses must follow – regardless of their size. We will explain these later in the presentation.

But first, we'll talk a bit about the law, the importance of privacy, and Canadians' views on it.

SLIDE (5)

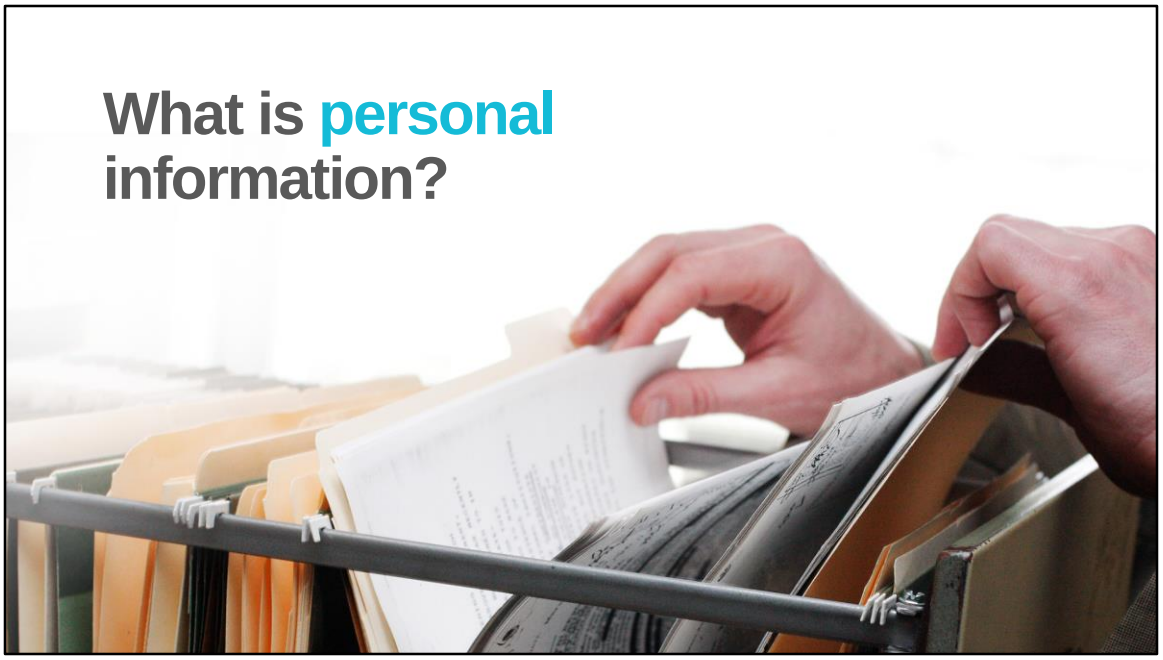
DOES PIPEDA APPLY TO YOUR BUSINESS?

PIPEDA applies to most businesses across Canada except in Quebec, British Columbia and Alberta. These provinces have their own private sector laws that are quite similar to PIPEDA.

But even in those provinces, PIPEDA covers federally regulated industries, like transportation, telecommunications and banking.

In addition, all businesses that operate in Canada and handle personal information that crosses provincial or national borders are subject to PIPEDA, regardless of which province or territory they are based in.

Finally, all businesses in the three territories fall under PIPEDA.



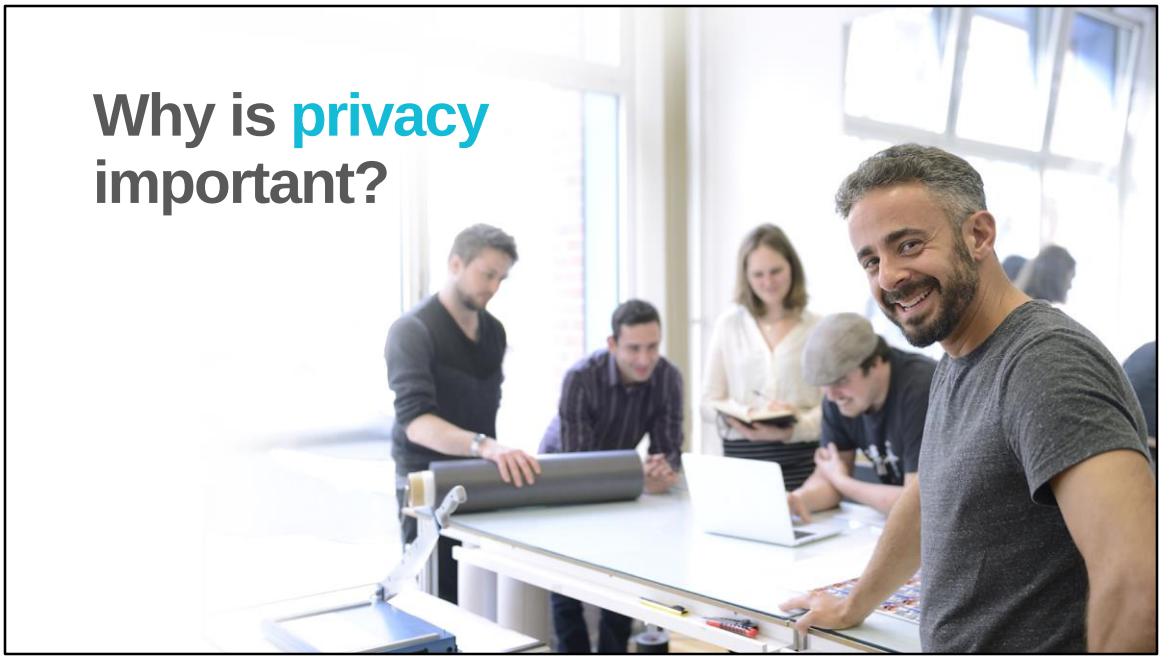
SLIDE (6)

WHAT IS PERSONAL INFORMATION?

Another good starting point is to understand what is meant by “personal information” because it’s more than just a name or address. It’s information about an **identifiable individual**.

It is information that, on its own or combined with other information, can identify a person. It can be a person's age, ethnicity, medical information, credit card number or even income level.

“Personal information” does not include information about a business or information that has been made anonymous – that isn’t possible to link back to an identifiable individual.



SLIDE (7)

WHY IS PRIVACY IMPORTANT?

Though small businesses may have a small number of employees, given the nature of the digital economy, they can handle vast amounts of personal information.

Regular surveys done by the OPC suggests that small businesses tend to be less aware of their privacy responsibilities than larger organizations. In 2017:

- 65% of large organizations (100+ employees) indicated they were aware
- 43% of small businesses indicated they were aware

Small companies may not have dedicated compliance officers, let alone extensive privacy knowledge.

The compliance challenge for smaller organizations is made more difficult by the limited human – and sometimes financial – resources they have, and the gap in knowledge about their privacy obligations.

Lack of awareness can potentially lead to complaints about your business, which may have an impact on your business' reputation.

SLIDE (8)

CANADIANS' ATTITUDES TOWARDS PRIVACY
Polls consistently show that an overwhelming majority of Canadians (more than 90%) are concerned about their privacy.

Canadians expect businesses to take the appropriate measures to protect the personal information they share with them. Yet, they believe that companies – and governments – are not doing all they can to protect their personal information.

According to the OPC's survey of Canadians:
- Nearly 80% of Canadians are reluctant to share their personal information, given news reports about information being lost, stolen or made public.
- Most have refused to provide their information to an organization at some point.
- Half have chosen not to do business with a company due to its privacy practices.
- Nearly half said they felt as though they've lost control over how organizations collect and use their data.

But the more they trust a company, the more likely they are to do business with them. Businesses that don't have strong privacy controls risk losing their competitive advantage in today's increasingly privacy-conscious marketplace.

On the flip-side, good privacy can be very good for business.
- 81% of Canadians said they would choose to do business with a company because it has good privacy practices.

SLIDE (9)

10 FAIR INFORMATION PRINCIPLES

PIPEDA includes ten (10) fair information principles that all businesses subject to the Act must follow.

The 10 fair information principles are:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

The OPC has developed a Privacy Guide for Businesses that outlines each of the principles.

Here are a few highlights for each principle, to give you a sense of what they mean and what you can do to fulfill your responsibilities.

It is important for all businesses subject to PIPEDA to fully familiarize themselves and

be compliant with consent obligations – outlined in detail in this guidance.

SLIDE (10)

ACCOUNTABILITY

Your organization is responsible for personal information under its control.

Develop and implement personal information policies and practices, and train your staff. Appoint someone in your business to be responsible for privacy compliance.

Make sure your staff knows who this person is, and that customers can easily contact this person if needed.

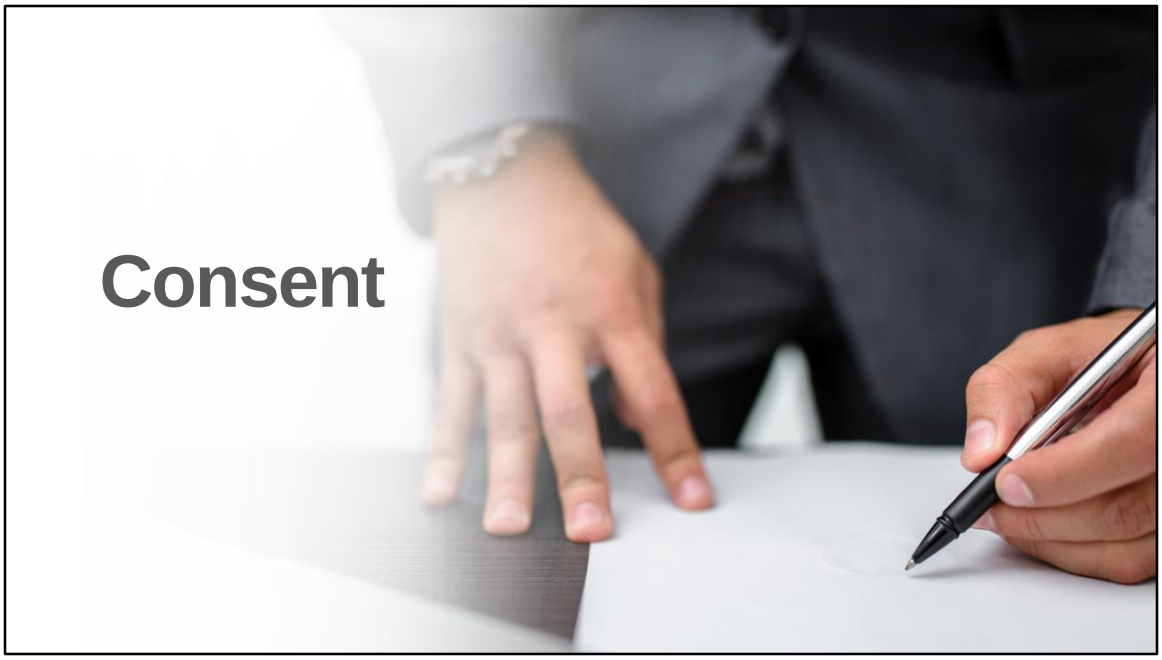
It’s also important to make sure your staff can explain your privacy policy to customers.

SLIDE (11)

IDENTIFYING PURPOSES

Clearly explain to your customers what personal information you're collecting and why, before or at the time of collection.

Ensure that these purposes are limited to what a reasonable person would expect under the circumstances.



SLIDE (12)

CONSENT
Businesses that wish to collect, use or disclose personal information must first seek and obtain consent.

This is at the heart of PIPEDA and gives individuals control over their personal information.

Many privacy policies and terms of use can be lengthy and full of legal jargon.

Instead, provide this information to your customers in a timely, user-friendly way to ensure meaningful consent.

In fact, more robust guidelines on obtaining meaningful consent officially apply as of January 1, 2019 (available since May).

They require businesses to clearly explain the following key elements (among other things) to customers:

- what personal information is being collected
- why they are asking for this personal information
- who they're going to share it with
- any potential harms that may arise from collecting or sharing their information

It is important for all businesses subject to PIPEDA to fully familiarize themselves and be compliant with consent obligations – outlined in detail in this guidance.

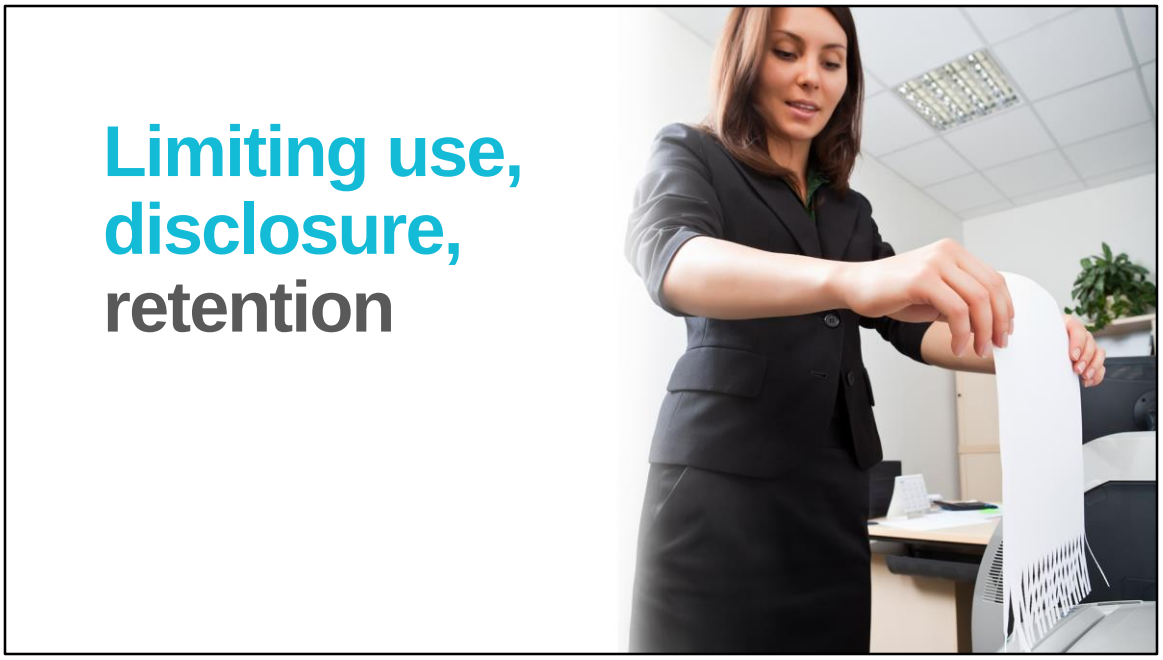
SLIDE (13)

LIMITING COLLECTION

Limit your collection of personal information to only what is currently necessary.

Collecting less information reduces the risk of inappropriate access, use, disclosure and loss.

For example, the OPC cautions businesses against asking for a person's Social Insurance Number, since few organizations are legally required to collect it.



SLIDE (14)

LIMITING USE, DISCLOSURE, RETENTION

Only use personal information for the reasons you explain to your customer and don't keep it any longer than you need it.

You cannot use the information you collected for a different purpose unless you obtain your customer's clear and meaningful consent to do so.

Be sure to dispose of the information securely to prevent a privacy breach. Before disposing of electronic devices, ensure all personal information is fully removed.

SLIDE (15)

ACCURACY

Make sure that personal information is as accurate, complete and up-to-date as necessary.

This will minimize the possibility of using incorrect information when making a decision about an individual or disclosing the information to a third party.

SLIDE (16)

SAFEGUARDS

Use appropriate security safeguards to protect personal information against loss, theft, unauthorized access, disclosure, copying, use or modification.

This means physical measures (such as locked cabinets), technological tools (such as passwords or encryption) and organizational controls (such as security clearances).

SLIDE (17)

OPENNESS

Show customers you take their privacy seriously.

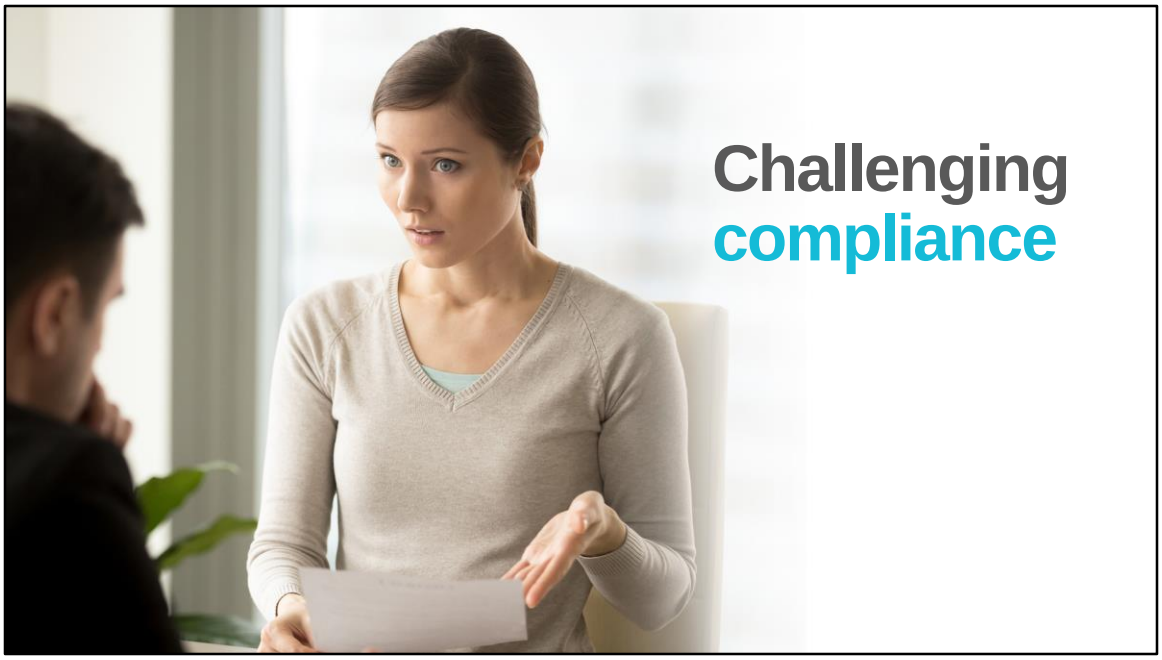
- Inform customers and employees that you have established policies and practices for the management of personal information.
- Make these polices understandable and available.
- Put up signs, post information on your website and look for other ways to actively share this information.

SLIDE (18)

INDIVIDUAL ACCESS

Your customers have a right to see the personal information you hold about them, so be ready to respond to requests.

Develop a procedure for responding promptly, informing your customers how their personal information (if any) has been used and amending it if it's found to be deficient.



SLIDE (19)

CHALLENGING COMPLIANCE

Let your customers know what they can do if they have concerns or further questions about how you handle their personal information.

Develop simple and accessible complaint procedures, and investigate all complaints you receive. If an investigation uncovers problems, take appropriate measures to address your personal information handling practices.

SLIDE (20)

PRIVACY BREACHES
Have procedures in place in the event of a breach. You should have strong safeguards – as required by law – to protect the personal information in your care.

Sometimes breaches happen, despite best efforts. It might involve the theft of personal information by computer hackers, the loss of a flash drive containing customer data or even a disgruntled ex-employee walking off with clients' information or contact lists.

So, what can you do?
- For starters, test your technology for vulnerabilities and make sure old systems or databases aren't vulnerable when you upgrade to newer technology.
- There are off-the-shelf solutions, and security specialists that can help with this if you don't have an IT Department.
- It's also a good idea to be aware of breaches within your industry. Hackers will often employ the same tricks against multiple businesses. The more alert you are, the more likely you will avoid the same pitfalls.

New regulations came into force in November 2018 regarding breaches of security safeguards. These regulations require businesses to **keep records** of any and all breaches of security safeguards and to **report any breach with real risk of significant harm** to the OPC and to any affected customers.

If you do experience a breach that could potentially harm your customers, contact the OPC immediately.

SLIDE (21)

CANADA'S ANTI-SPAM LEGISLATION AND PIPEDA

You may have heard of CASL or Canada's Anti-Spam Legislation. The enforcement of CASL is shared by the OPC, the Competition Bureau and the Canadian Radio-television and Telecommunications Commission (CRTC).

The OPC focuses on two types of violations:

- address harvesting, which generally involves using computer programs to automatically mine the Internet for email addresses in order to compile lists for marketing purposes; and
- collecting information with spyware or malware.

Businesses doing email marketing need to exercise due diligence to avoid inadvertently harvesting or using harvested email addresses.

Take appropriate precautions when working with a third party that has been contracted to do email marketing, or when buying a list from a vendor to do email marketing in-house.

Consult **www.priv.gc.ca/casl** or fightspam.ca learn how to comply with PIPEDA when

collecting and using electronic addresses for e-marketing.

SLIDE (22)

PRIVACY IS GOOD FOR BUSINESS

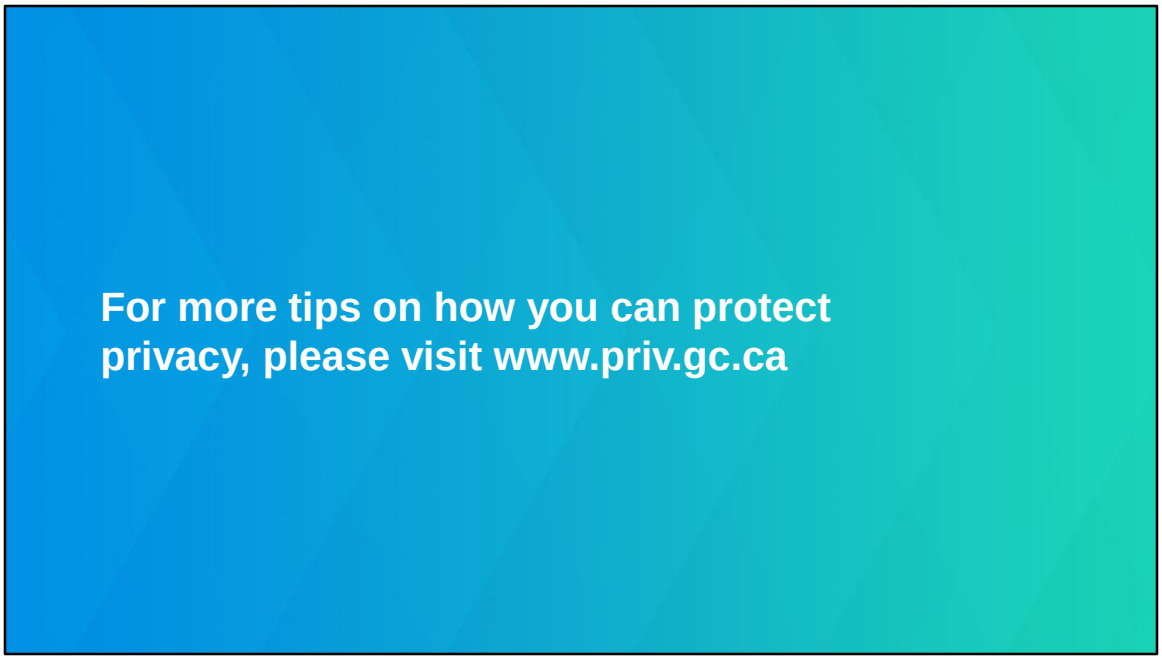
Poor privacy protection can damage your company's reputation and cut into your profit margin. Conversely, businesses that are proactive on privacy enjoy the confidence and trust of their customers.

Canadians tell us that the more they trust a company, the more likely they are to do business with it and provide the data businesses so value. Getting privacy right is your opportunity to demonstrate that you deserve their trust – and their business.

Remember that one of the fair information principles outlined earlier is **accountability**. At the end of the day, you are responsible for protecting the personal information you have collected.

Build privacy protections into everything you do as a business and have clear policies and procedures for the collection, use and disclosure of personal information. The best way to do this is by developing a privacy management program that covers all aspects of how you handle the personal information.

The OPC can help. There is guidance on this and much more at **www.priv.gc.ca**.



SLIDE (23)

For more tips on how you can protect privacy, visit www.priv.gc.ca.