Deloitte.

Your Data Protectors, Your Growth Enablers

Mariama Zhouri, Senior Manager, Risk Advisory

Data Protection and Privacy

Why does it matter to you?

How is my privacy protected in Canada?

Who is responsible for protecting data and privacy within organizations?

How can data breaches or improper data handling impact my life?

How do emerging technologies and data analytics impact my privacy?

Key Concepts

What is Data Protection and Privacy?

Key Terms: Personal Information vs. Confidential Information

The two sides of the same coin

Personal information is confidential, but not all confidential information is personal

PEOPLE

"**personal information"** means any information relating to an identified or identifiable individual; an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier.

Examples: email address, contact details, employment information.

DATA

"confidential information or data" that one or the other party requires to be maintained on a "need-to-know" basis is often exchanged in the course of communicating and transacting business.

Examples: client & vendor related information, IP information, strategy documents, legal documents, unpublished financial information, business plans.

Note New privacy laws around the world are starting to include the following elements as part of the definition of "personal information": **location data**, **online identifiers, genetic data** and **biometric data**.

Key Terms: Privacy vs. Security

Security is a privacy enabler: There is no privacy without security and no security without privacy

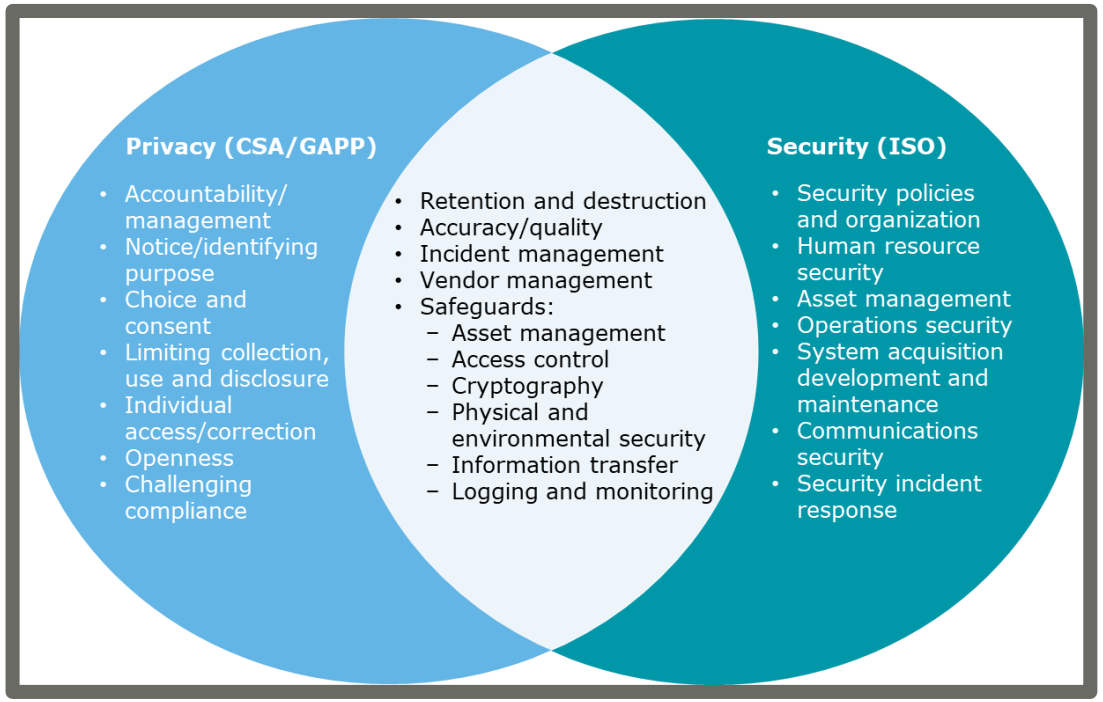
The Privacy and Security Paradox

Privacy

Strong privacy requires protecting a user's identity and preventing unauthorized access or unintended use of personal information.

Security

Strong security requires binding a user's identity to their behavior in support of monitoring and individual accountability.



Regulatory Requirements

Regulations in Québec, Canada and around the world

Current Canadian Regulatory Landscape

Provincial and federal bodies responsible for enforcement

The map below provides a representative list of privacy laws in Canada:

Canada *Privacy Act*
Canada *Personal Data Protection and Electronic Documents Act*
Canada's *Anti-Spam Law* (CASL)

Office of the Privacy Commissioner of Canada (OPC)

The OPC is the federal privacy regulator of Caned and oversees compliance with PIPEDA and the Privacy Act, which protect and promote the privacy rights of individuals

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian federal law relating to data privacy. It sets out the ground rules for how organizations collect, use and disclose personal data in the course of commercial activity.

Northwest Territories *Access to Information and Protection of Privacy Act*
Northwest Territories *Health Information Act*

Yukon *Access to Information and Protection of Privacy Act*
Yukon *Health Information Privacy and Management Act*

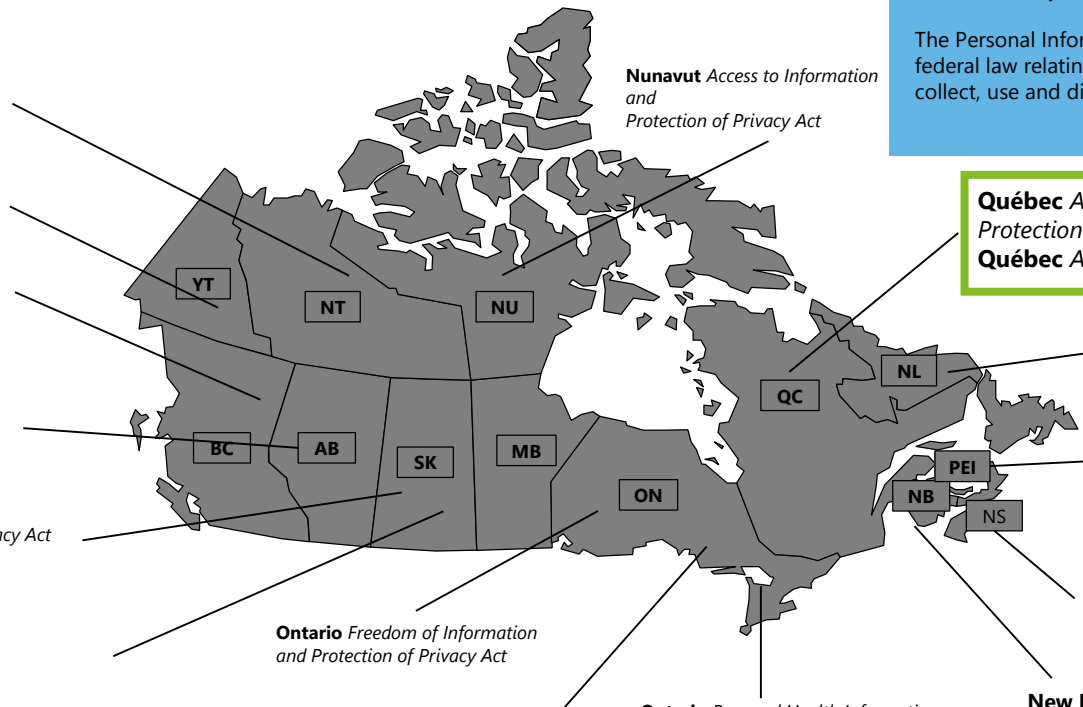
***BC** Freedom of Information and Protection of Privacy Act*
BC *Personal information Protection Act*
BC *E-Health (Personal Health Information Access and Protection of Privacy) Act*

Alberta *personal data Protection Act*
Alberta *Freedom of Information and Protection of Privacy Act*
Alberta *Health Information Act*

Sask. *Freedom of Information and Protection of Privacy Act*
Sask. *Local Authority Freedom of Information and Protection of Privacy Act*
Sask. *Health Information Protection Act*

Manitoba *Freedom of Information and Protection of Privacy Act*
Manitoba *Personal Health Information Act*

Source: Office of the Privacy Commissioner website http://www.priv.gc.ca/resource/prov/index_e.asp#001.



Nunavut *Access to Information and Protection of Privacy Act*

Québec *Act Respecting Access to Documents held by Public Bodies and the Protection of personal data*
Québec *Act Respecting the Protection of personal data in the Private Sector*

Newfoundland & Labrador *Access to Information and Protection of Privacy Act*
Newfoundland & Labrador *Personal Health Information Act*

Prince Edward Island *Freedom of Information and Protection of Privacy Act*

Nova Scotia *Freedom of Information and Protection of Privacy Act*
Nova Scotia Part XX of the *Municipal Government Act*
Nova Scotia *personal data International Disclosure Protection Act*
Nova Scotia *Personal Health Information Act*

New Brunswick *Right to Information and Protection of Privacy Act*
New Brunswick *Personal Health Information Privacy and Access Act*

Ontario *Freedom of Information and Protection of Privacy Act*

Ontario *Municipal Freedom of Information and Protection of Privacy Act*

Ontario *Personal Health Information Protection Act*

Canada’s PIPEDA and the Digital Privacy Act

- PIPEDA, also known as the Personal Information Protection and Electronic Documents Act, is Canada’s federal privacy law for the private sector and applies to personal information collected during the course of commercial activities.
- Effective November 1, 2018 the Digital Privacy Act introduced amendments to PIPEDA, requiring organizations to report to the OPC privacy breaches that pose a risk of significant harm.

Breach notification requirements under the Digital Privacy Act [amendments to PIPEDA]	
Notify Regulators	• As soon as feasible, when there is a ***real risk of significant harm (e.g., bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property)***
Notify Individuals	• As soon as feasible, when their personal information has been lost or stolen
Notify External Organizations	• Notify any other organization or government institution of a breach, if such organizations or institutions may be able to reduce the risk of harm or mitigate the harm.
Breach Record Keeping	• Keep and maintain a record of every breach of security safeguards involving personal information under its control, regardless of risk of significant harm to individuals • Produce these records upon request by the Office of the Privacy Commissioner of Canada
Penalties	• Fines up to $100,000 per individual not informed.

Global Regulations

Canada

- **PIPEDA**: Personal Information Protection and Electronic Documents Act
- **LPRPDE**: Loi sur la protection des renseignements personnels et les documents électroniques

Europe

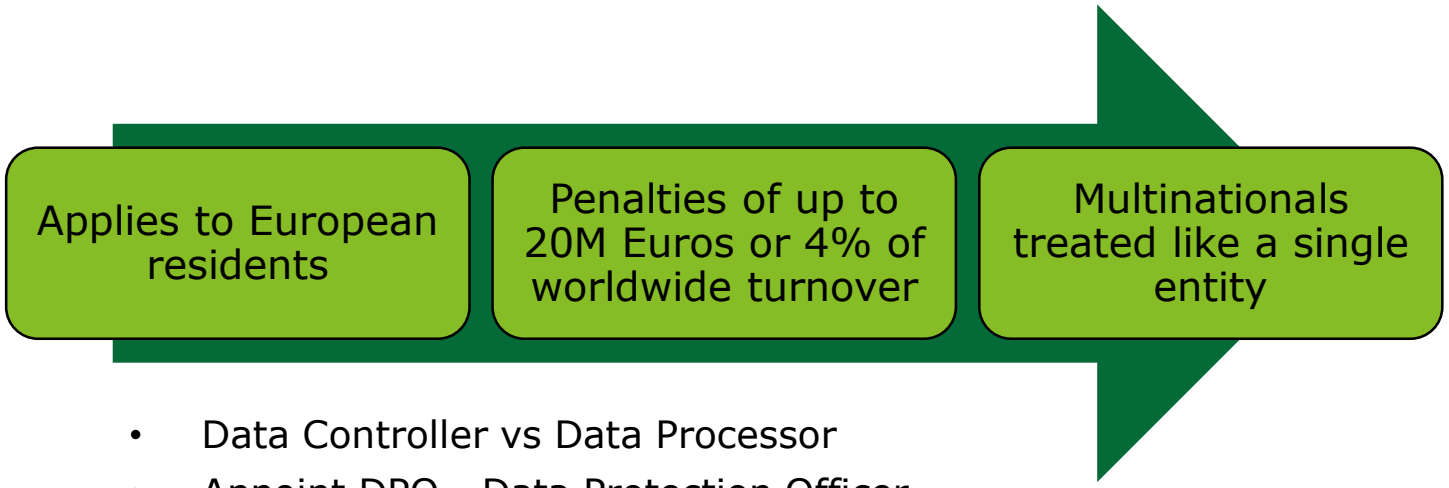
- **GDPR** (General Data Protection Regulation)
- In force since: May 25th, 2018

USA

- Multiple sectorial laws
- **CCPA** (California Consumer Privacy Act of 2018 AB 375
  - ➢ Effective January 1st, 2020

General Data Protection Regulation

GDPR – May 25th, 2018



- Data Controller vs Data Processor
- Appoint DPO - Data Protection Officer
- Data Protection "By Design"
- Consent vs Legitimate Interests

1. Right to information (e.g. the retention period)
2. Right to access
3. Right to rectification
4. Right to erasure ("to be forgotten")
5. Right to restriction of processing
6. Right not to be subject to automated decision-making
7. Right to data portability
8. Right to object
9. Right to withdraw consent
10. Right to complain to a supervisory authority

Why Data Protection and Privacy?

Key issues for an organization

Privacy Concerns for Startups

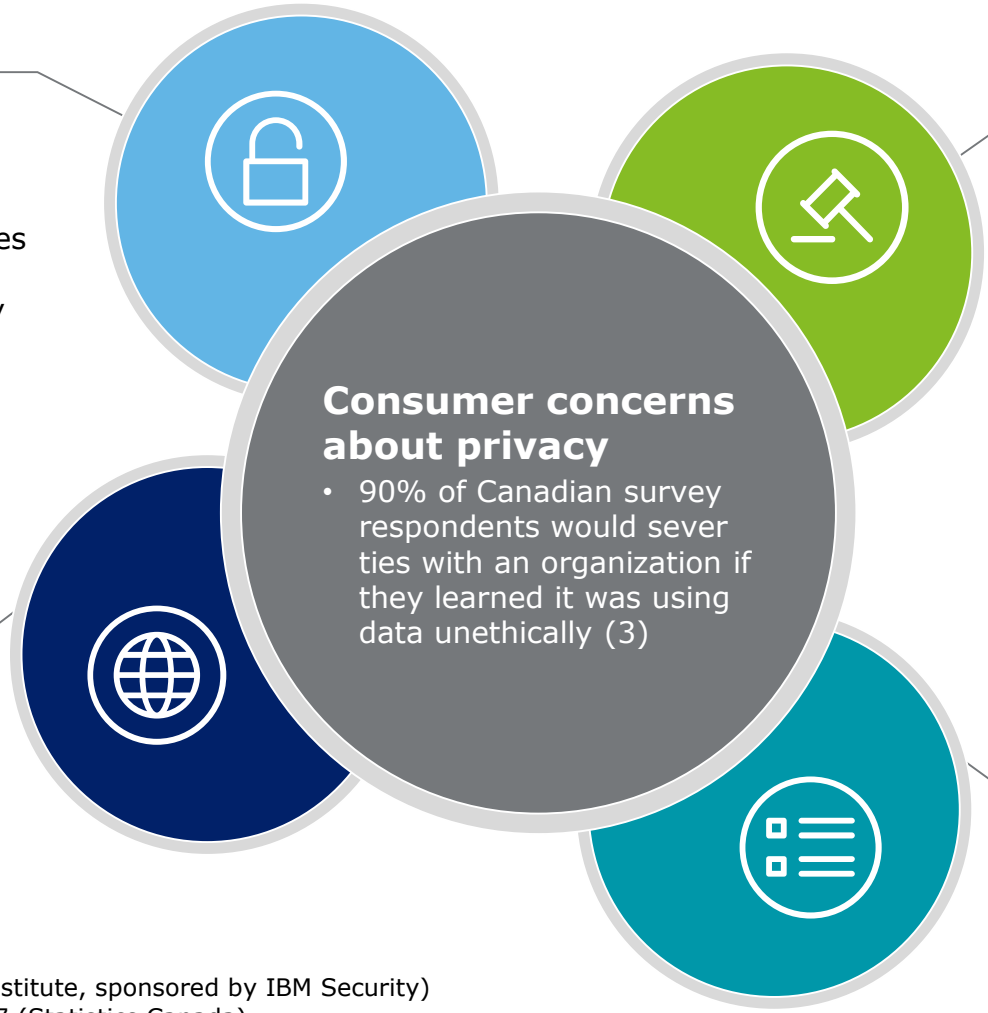
Impacts across the ecosystem

Data breaches

- The average cost of a data breach in Canada is 4.74 million USD (202 USD per lost/stolen record) (1)
- In 2017, 19% of small businesses and 28% of medium businesses were impacted by cyber security incidents (2)
- Many technologies like cloud computing and IoT are being increasingly adopted by organizations, but may pose security risks

Third parties

- Subservice organizations and other third parties might collect, process, or store personal data that an organization is accountable for, but might not do so securely or ethically



Regulations

- In 2018, multiple new data protection laws came into effect, most notably the GDPR
- New PIPEDA breach notification requirements as of Nov. 1, 2018 affect many Canadian organizations
- Non-compliance can result in heavy fines and hinder global partnerships and sales

Widespread data collection

- Artificial Intelligence, Big Data, and IoT are among many new trends that involve large-scale data collection to develop or improve products and services

(1) 2018 Cost of a Data Breach Study (Ponemon Institute, sponsored by IBM Security)
(2) Cyber Security and Cybercrime in Canada, 2017 (Statistics Canada)
Note: Small businesses: 10-49 employees, medium businesses: 50-249 employees
(3) Data and Ethics Survey, 2016 (Deloitte)

Why Now?

Data Protection and Privacy as a growth enabler

Data Protection and Privacy in Growing Organizations

Why now?

Save **time, money, and effort** in the long run.

- Fewer people to train
- Less data to manage
- Lower resistance to change

Differentiate your organization from competitors and instill trust in customers.

- Ethical use of data is an increasing driver of consumer trust
- When customers **trust** an organization, they are more likely to give their data, and less likely to leave in the event of a data breach

Secure new **business opportunities** and partnerships.

- Operate in regions and sectors with additional data protection and privacy restrictions
- Partner with organizations who require robust data protection and privacy practices

Future-proof your business model.

- Be able to **adapt** to future regulatory changes and cybersecurity risks
- Ensure that **innovative technologies and core strategies** are designed to protect personal data

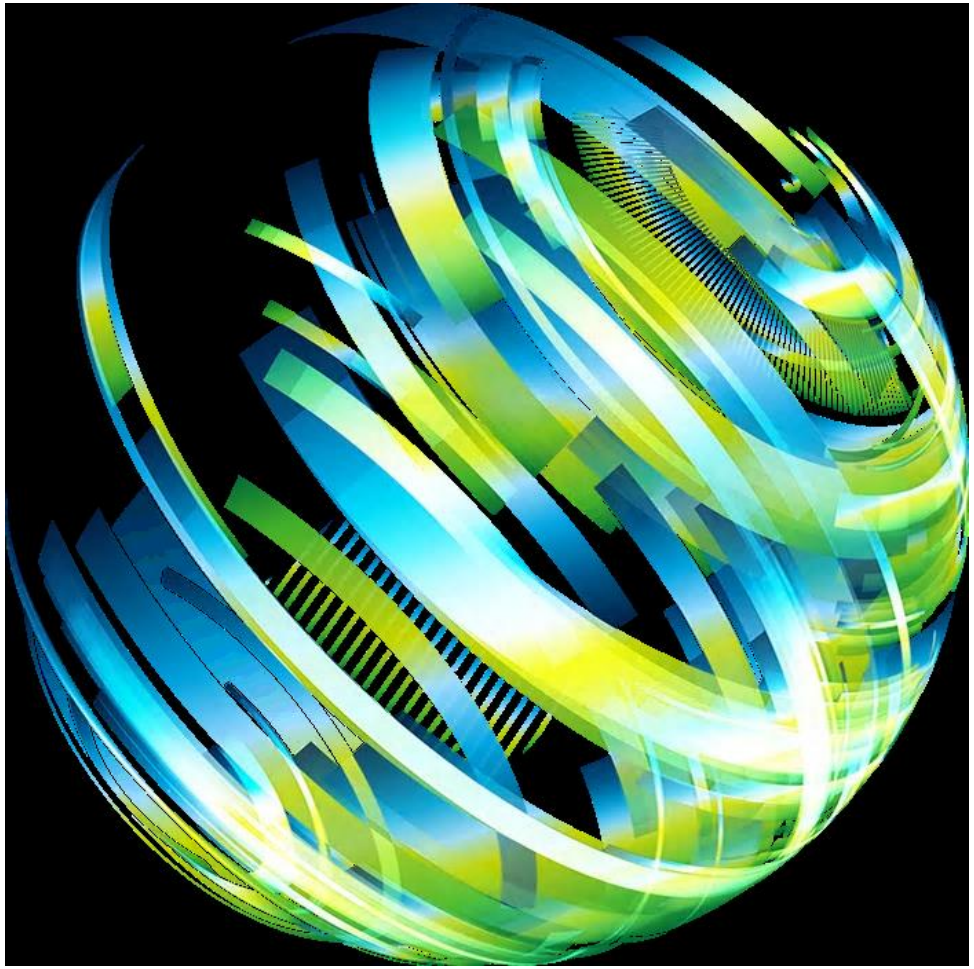
Case Study

A success story from a Canada's Technology Fast 50™ winner

The Technology Fast 50™ program celebrates innovation, rapid revenue growth, and entrepreneurial spirit. Winners include some of the fastest-growing technology companies.

Deloitte provided data protection and privacy services for one of these companies.

By achieving GDPR compliance, this firm was able to secure **multiple global partnerships** and receive **hundreds of millions of dollars in additional funding**.



Key Takeaways

Data Protection and Privacy is making its way onto CEOs' agendas.

- The budget for privacy is beyond just compliance
- Privacy by Design and Security by Design

Data Protection and Privacy is a revenue generator.

- Good data management practices foster new business relationships

Digital transformation can lead to both risks and opportunities when it comes to secure and compliant data management.

- Security and privacy risks from increased data collection and unsecure technologies
- New tools to manage compliance and security

Good data management practices involve not only your organization, but also your third parties.

- Understand who is managing your organization's data, and how they are doing it

Our Services

How Deloitte can help you implement Data Protection and Privacy

Our Data Protection and Privacy offerings are organized around 8 major areas:

Data Discovery and Classification: Understand where sensitive data exists across the organization. Enable organizations by providing mitigation strategy to protect and manage sensitive data identified (“crown jewel programs”).

Data Risk Assessment and Strategy: Understand key risks the organization is facing as well as capability maturity and existing gaps. Provide a data protection and privacy roadmap to define the components and capabilities needed to build a data protection program.

Data Exfiltration Risk Assessment: Identify areas in organization that are most at risk for data being exfiltrated. Provide remediation activities to strengthen at-risk areas.

Data Protection Technology Implementation: Implement and deploy data protection technology solutions and capabilities (Data Loss Prevention, Encryption, Data Classification, Tokenization, Data Rights Management and Data Access Governance).

Data Protection and Privacy Program Foundation Development: Develop supporting capabilities (e.g., governance, policies, operating model, key risk indicators) to strengthen data protection and privacy program and ensure compliance with regulatory requirements.

Managed Services: Provide incident and event management, system maintenance, reporting and other operational risks.

Ethical Use of Data: Incorporate ethical procedures for collecting and analyzing data in target operating model.

Data Governance and Data Risk Management: Understand how and by whom data is accessed. Provide a risk management plan to mitigate improper access to data.

Deloitte.

Your Data Defenders and Growth Enablers

Mariama Zhouri
Privacy Regional Leader
mzhouri@deloitte.ca

Beth Dewitt
Privacy National Leader
bdewitt@deloitte.ca