

Aurexia

Organization around data

Key roles and responsibilities

Data Office Chief Data Officer Responsible for data management and quality

The Data Office is responsible for the data management and governance policy. And the CDO oversees the collection, management, and storage of data across an organization

Security Office

Chief Information Security Officer Responsible to manage risk and implement an information security program

The Security Office ensures the security of all the organization's infrastructures (physical and application)

Privacy Office Data Privacy Officer

Data Use and Retention Compliance Officer

The Privacy Office ensures the confidentiality and sovereignty of the data through their collection, processing and storage in compliance with the appropriate regulations

ZOOM ON :

- Companies are facing massive use of data combined with increased regulatory requirements, resulting in the critical importance of data management roles in the organization
- More than 120 countries are already engaged in international privacy laws with regards to data protection
- Regulations vary significantly from country to country
- Canada is considered an international hub, making it key to understand how data privacy is regulated worldwide

Aurexia Data protection in Canada

 \checkmark The level of data protection in Canada can be considered equivalent to the EU level

The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to private sector and commercial organizations across Canada to collect and use personal information. Attention point : it will soon be replaced by the Consumer Privacy Protection Act (CPPA) introduced in the Digital Charter Implementation Act, 2022, currently known as <u>Bill C-27</u>

The Digital Charter Implementation Act --

- **Consumer Privacy Protection Act (CPPA)** Is an Act to support and promote electronic commerce by protecting personal information that is collected, used, or disclosed in the course of commercial activities. Once passed, this law **will replace** the Personal Information Protection and Electronic Documents Act (**PIPEDA**).
- Personal Information and Data Protection Tribunal Act Is an Act that provides a recourse mechanism for enforcement of the CPPA. The Tribunal would impose monetary penalties and rule on appeals from orders by the federal Privacy Commissioner.
- Artificial Intelligence and Data Act (AIDA) is an Act that will rule over the development and deployment of high-impact AI systems.

... to be implemented

-- US regulations challenges -

- July 2020 The Court of Justice of the European Union (CJEU) has annulled the Privacy Shield, which guaranteed the free flow of data between the EU and the US (Schrems II).
- For each transfer (outside the US), a **case-by-case analysis (risk assessment)** is made to ensure that U.S. law does not compromise the adequate level of protection
- March 2022, a first step towards a new agreement : the Trans-Atlantic Data Privacy Framework.
- **December 2022** the Commission entered into talks with the U.S. government with a view to a possible **new adequacy decision**.

... in progress for March 2023



Aurexia Data protection in Canada (2/2)

Impact of CPPA new regulation on PIPEDA

The CPPA (Consumer Privacy Protection Act) is intended to replace and reinforce PIPEDA. It aims at giving consumers control over their private data while providing transparency about how businesses use their personal data



OBJECTIVES

Aur<u>exia</u> Cross border data transfers



Aurexia Data protection

The differences between PIPEDA / CPPA and GDPR

- Doesn't mention extraterritoriality
- Focuses on organizations in the Canadian private sector that carry out "commercial activities" and collect, use, or disclose personal data
- It doesn't apply to government entities and some provinces that have their own privacy laws (Alberta, British Columbia, Quebec)
- According to the Office of the Privacy Commissioner of Canada (OPC), PIPEDA could apply in a foreign country if the organization has a real and substantial connection to Canada
- Unlike the GDPR, Bill C-11 would only regulate commercial activities
- Organizations to take physical, organizational, and technological precautions to guarantee that personal information is not lost or stolen, accessed without authorization, disclosed to unauthorized individuals, copied, or modified
- It also requires the organization to be held accountable and nominate one or more persons to be in charge of privacy compliance
- o Justify the reason for the use of the personal data
- o Right to Data Portability
- o Right to Erasure
- o Right of Access
- Right to Be Informed
- Right to Object

Implied consent is deemed acceptable for less sensitive personal information. Consent must be explicit and explained in clear terms

Under **PIPEDA**, penalties for a data breach can be as high as \$100,000, plus costs for the audit and investigation. Penalty of up to 3% of sales (not to exceed 10 million Canadian dollars) for routine cases. Penalty of up to 5% of sales (not to exceed 25 million Canadian dollars) for serious cases. GDPR

Application,

Jurisdiction &

Enforcement

Individual & Data

Protection

Individual Rights

Data Processing Consent

& Privacy Requirements

Penalties &

Compensation

processes any personal data of any EU residents, whether they have EU offices or not.
Is enforced by <u>data protection authorities</u> (DPAs) from the 27 EU member states.

• Includes an extraterritoriality provision, it has a widespread impact on companies, even those outside of Europe

o Applies to any organization or entity (>250 employees) that

- Companies must guarantee its data security (including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage).
 Busingers must adhere to Data Protection Principles on
- Businesses must adhere to Data Protection Principles and have a legal representative in the EU (in some cases, a Data Protection Officer).
- Right to Data Portability
- o Right to Erasure
- o Right of Access
- Right to Be Informed
- Right to Object

Data controllers are only permitted to process personal data where there is a valid legal basis for doing so.

Penalties under **G DPR** can amount to €20 million, or 4% of global revenue.

-					
μ	rı	n	\cap	n	es
		11		Ρ	L J

GDPR

Data protection officer

Privacy from start to finish

Mandatory breach reporting

Individual rights

Consent

Wider scope

Data portability

Penalties

PIPEDA

- Accountability
- Identifying Purposes
- 📋 Consent
- Limiting Collection
- .
- 💉 Accuracy
- ✓ Safeguards
- Openness
- Individual Access
- Challenging Compliance
- ◎ Limiting Use, Disclosure, and

Retention



PIPEDA applies to private-sector organizations across Canada that collect, use or disclose personal information during a commercial activity.

British Columbia

Alberta

They have their own private-sector privacy laws (similar to PIPEDA)

www.aurexia.com



Data from study "10 Biggest Data Breaches in Finance" updated August 2022



Our contacts





Dominique HERROU Partner dominique.herrou@aurexia.com Fabien RUER Director fabien.ruer@aurexia.com



Marilyne SOCHET Manager marilyne.sochet@aurexia.com





Our data protection specialists give you the tools, information & confidence that you need, to manage risk and make informed decisions. Combining expert legal advice with leading technology, we guide you through the complex international regulation, strengthening your data and compliance processes, and helping you achieve your goals

EX C

Bringing value, together

TATAN