Castra Technologies

Cybersecurity and Data Privacy Experts

GDPR and Canadian Privacy Legislative Update – 23 FEB 26

CastraTech.com

GDPR Updates, 2023-26

- **GDPR Procedural Regulation (2023–2026):** Proposed 2023, agreed 16 JUN 25, regulation entered into force 01 JAN 26 and will fully apply from 02 APR 27. It aims to harmonize enforcement in cross-border cases. It clarifies complaint procedures and sets fixed deadlines for draft decisions, aiming for faster resolution of major international investigations and complaints initiated after 02 APR 27.
- **EU AI Act Integration (2024–2026):** Full effective 02 AUG 26, the AI Act works alongside GDPR to govern how personal data is used for training and deploying AI systems. High-risk AI systems now face specific transparency and data governance requirements that overlap with GDPR Article 22 on automated decision-making. The AI Act requires companies to explain AI-driven decisions affecting consumers and that law may see significant changes based on the EC's Digital Omnibus Regulation Proposal, so organizations should expect increased uncertainty and scrutiny around transparency, governance and unacceptable risk. On 02 FEB 25, prohibitions on "unacceptable risk" AI (e.g., social scoring began and on 02 AUG 26, most transparency duties, e.g., labeling deep fakes, became fully applicable.
- **EU Data Act:** Entered into force 12 SEP 23 and become effective 12 SEP 25, creates new rights for users to access and share data generated by connected (e.g., IoT) devices, with GDPR explicitly prevailing if personal data is involved. Design/manufacturing requirements apply to products on the market after 12 SEP 26.

Business Requirements Enacted, 2023-26

2023: Transatlantic Transfers

- Self-Certification for US Transfers: Businesses transferring data to the US must now certify under the EU-US Data Privacy Framework to avoid the heavy administrative burden of Standard Contractual Clauses (SCCs)
- Procedural Transparency: Organizations involved in cross-border disputes are now required to provide "administrative summaries" of their positions earlier in the investigation process to speed up EDPB enforcement

2024: AI & IoT Governance

- AI Data Literacy: Under the EU AI Act, businesses must ensure that staff handling personal data via AI systems possess "AI literacy"—formal training on the risks and GDPR implications of those tools
- IoT Data Portability: Per the EU Data Act, manufacturers of connected products must design interfaces that allow users to export personal data in real-time, moving beyond the "one-off" SAR (Subject Access Request) model

Business Requirements Enacted, 2023-26

2025: Streamlined Compliance & Breach Reporting

- New Breach Deadline (96 Hours): For certain low-complexity breaches, the reporting window was extended from 72 to 96 hours via the 2025 Procedural Regulation, provided a "preliminary notice" is sent within the first 24 hours
- SME Exemptions: Small businesses, those under 750 employees, are now officially exempt from maintaining a Record of Processing Activities (ROPA) unless they process "high-risk" biometric or health data

2026: Transparency & Deep Fake Labeling

- Mandatory AI Labeling: As of 2 Aug 26, businesses using AI to generate or manipulate "deep fake" content (including synthetic voices or images) must provide a clear and visible disclosure that the content is AI-generated, fulfilling GDPR transparency obligations (Articles 12-14)
- Standardized Information Notices: The EU Data Protection Board's 2026 Coordinated Action requires businesses to use standardized, machine-readable "Privacy Icons" in digital notices to ensure information is actually accessible to users

Notable GDPR Fines, 2023-26

2023:

Meta (€1.2 Billion): The largest GDPR fine in history, issued by the Irish DPC for transferring EU user data to the U.S. without adequate protections

Meta (€390 Million): Fined for "contract necessity" violations, effectively forcing users to accept personalized ads

TikTok (€345 Million): Penalized for default "public" settings on child accounts and failing to protect minors' privacy

2024:

LinkedIn (€310 Million): Fined for using an invalid legal basis for behavioral analysis and targeted advertising

Uber (€290 Million): Penalized by the Dutch DPA for transferring driver data to the U.S. following the invalidation of the Privacy Shield

Meta (€251 Million): A late-year penalty for a massive 2018 data breach that exposed tokens for 29 million accounts.

Notable GDPR Fines, 2023-26

2025:

TikTok (€530 Million): Fined in April 2025 for illegal data transfers to China and failing to prove equivalent privacy protections

Google (€325 Million): Combined fines from France's CNIL for "Gmail ads" that looked like emails and deceptive cookie consent steering

SHEIN (€150 Million): Fined for planting tracking cookies before users provided consent on its mobile and web platforms

Vodafone Germany (€45 Million): Penalized for security flaws in customer authentication and poor oversight of third-party contracts

2026:

Free / Free Mobile (€42 Million): France's CNIL issued this combined fine in January 2026 following a data breach affecting 24 million accounts and excessive data retention

France Travail (€5 Million): Fined for inadequate security measures that led to a major cyberattack on the public employment agency

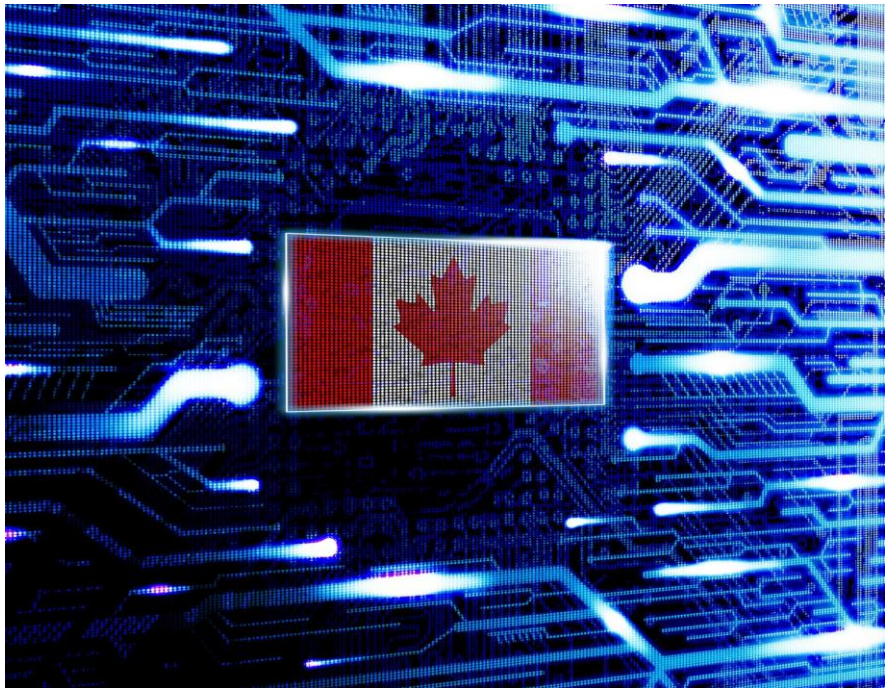
Netherlands Municipalities (€250,000): Ten municipalities were fined for the illegal profiling of Muslim residents, signaling a new zero-tolerance policy for public sector Article 9 (sensitive data) violations

General Data Protection Regulation (GDPR) Core Principles

The GDPR applies to any organization that handles EU resident data, not just EU-based companies. It sets a high bar for data protection by requiring valid consent through explicit, affirmative action, granting EU individuals the right to erasure and imposing heavy fines for non-compliance. Seven core principles are outlined in Article 5(1)-(2) that dictate how organizations must process personal data; these emphasize ethical handling, security and accountability.

- ❏ Lawfulness: Data must be processed legally, fairly, and openly, with valid legal bases (like consent), and in a manner that is not misleading
- ❏ Purpose Limitation: Data must be collected for specific, legitimate, and explicit purposes and not used for incompatible reasons
- ❏ Data Minimization: Organizations should only collect the minimum amount of data necessary for their intended purpose
- ❏ Accuracy: Data must be kept accurate and up-to-date, with incorrect data rectified or erased
- ❏ Storage Limitation: Personal data must not be kept longer than is necessary and should be deleted or anonymized once no longer needed
- ❏ Integrity and Confidentiality (Security): Data must be processed securely, utilizing measures like encryption or access controls to prevent unauthorized access, loss, or destruction
- ❏ Accountability: Data controllers are responsible for complying with these principles and must be able to demonstrate this compliance through documentation and policies

Federal Canadian Privacy Updates, as of Feb 2026



Federal Collapse of Digital Charter Implementation Act, 2022, Bill C-27, on 06JAN25

PIPEDA remains intact after Prime Minister (PM) Trudeau prorogued Parliament, causing Bill C-27 not to pass.

The proposed Consumer Privacy Protection Act (CPPA) and the Artificial Intelligence and Data Act (AIDA) were not enacted.

Canadian Provinces

Personal Information Protection & Electronic Documents Act (2020), PIPEDA – Canadian Federal Law

- Applies to both consumer and employee information
- New legislation is expected to be introduced in early 2026, with possible passage in 2028/29; the Carney government plans to reintroduce key components of the previous proposed CPPA:
  - Expected focus areas may be children's privacy, Artificial Intelligence (AI) and "deep fakes"
  - Includes stronger enforcement powers for the Office of the Privacy Commissioner (OPC), aligning fines with GDPR up to 5% of annual gross revenue or CA$25M
- Canada continues operating under PIPEDA, with Quebec's Law 25 functioning as a national standard; although this is not federal legislation, it serves as a higher baseline privacy program guidance and companies ignoring this reality face material financial exposure
- GDPR remains the international benchmark for Canadian businesses serving European customers because:
  - Segregating data by customer geography is complex, expensive, and open to error
  - GDPR's adequacy framework affects Canadian data transfer rights
  - Meeting the highest global standard provides defensibility across jurisdictions
  - New federal reform requirements will likely be met by current the GDPR standards
- Provincial fragmentation accelerates in Alberta, Ontario and British Columbia

Ideal Policy Components of PIPEDA Replacement

NOTE: Bill C-27 Introduced JUN22 to Replace/Supplement PIPEDA, Failed JAN 25 in Parliament and Again After the APR 25 Election

Enforceable Federal Legislation

- Penalties with consequence
- A functional judiciary with true decision-making power
- Requirements for algorithmic transparency
  - Explanations of the operation of consequential automated decision systems for individuals
  - Provision of choices for every individual
- Strengthened individual rights e.g., to access, amend, and delete information must respect international standards; transparency and choice must be fundamental tenets

Practical Impact: *Real enforcement risk for businesses*

Ideal Policy Components of PIPEDA Replacement, Cont.

Data Portability Rights - Canadians could gain legal entitlements for the transmission of personal information in machine-readable form among service providers, such that:

- The data of the financial services flows freely among financial institutions
- Medical records are made highly portable, but remain secured
- Customer profiles and preference data transfer between competitors
- Different systems are enabled to more easily work together

Business Impact: *Methods of customer retention based on data lock-in are no longer applicable; the value of competitive superiority changes from data ownership to use and service*

Ideal Policy Components of PIPEDA Replacement, Cont.

Relevant Digital Sovereignty - Canada would claim domain over the data infrastructure via:

- Risk-based cross-border data transfer assessments
- More stringent government data residency rules
- Preferences in Canadian procurement of infrastructure
- Industry-specific data localization of essential services

Business Impact: *Cloud architectural choices assume more importance. Cloud vendor choices involve assessment of risk based on jurisdiction too. American tech vendors see new barriers in the Canadian marketplace*

Ideal Policy Components of PIPEDA Replacement, Cont.

Comprehensive Artificial Intelligence (AI) Governance - Clear statutory obligations would govern AI deployment, e.g.:

- Mandatory impact assessments for high-risk AI systems
- Bias testing and mitigation requirements
- Human oversight over automated decision-making
- Transparency and choices offered in AI-driven processes

Business Impact: *AI implementation becomes a compliance-gated initiative requiring formal governance, documentation, and risk management, not merely a technical deployment.*

Canadian Provincial Updates: Quebec Law 25 – An Act to Modernize Legislative Provisions Regarding the Protection of Personal Information (PI)

Quebec, Canada

21 SEP 21

Bill 64 was introduced in Quebec as an effort to modernize privacy protections regarding PI. After passage, it became known as Law 25.

2022-25

Law 25 is a comprehensive privacy law that modernizes the handling of PI for any organization operating in or doing business with Quebec residents, with additional provisions of the law phasing in starting 22 SEP 22 and most recently on 21 JAN 25.

Quebec Law 25

22 SEP 22

Privacy Officer Appointment: The person with highest organizational authority is automatically the Privacy Officer, unless they delegate it in writing

Confidentiality Incident Management & Stringent Breach Notifications: Organizations must keep a registry of all, even minor, privacy breaches and notify the Quebec Access to Information Commission (CAI) and affected individuals of any incidents posing "risk of serious injury"

22 SEP 23

Privacy Policies: Organizations must implementation clear, transparent, and accessible privacy policies

Explicit Consent & Transparency: Organizations must obtain clear, informed, and explicit consent for data collection and use, particularly for profiling or identifying individuals

Public Disclosures and Notices.: Organizations must publish notices their website for personal information

Privacy by Default: Organizations must implement privacy options as "on" by default

Parental Consent: Required for children under age 14

Quebec Law 25

22 SEP 23, Continued

Cross Border Transfer Rules: Organizations must abide by new rules for transferring personal information outside Quebec

Data Retention & Destruction: Organizations must define how long data is kept and must securely destroy or anonymize it once it is no longer needed

Data Minimization: Personal information must only be retained for as long as necessary to fulfill the purpose for which it was collected

Third-Party Contracts: Specific, enhanced confidentiality requirements mut be included in agreements with service providers or third parties

Website Cookies & Tracking: Opt-in consent is required for tracking cookies; users must be able to withdraw consent as easily as they gave it

Administrative Monetary Penalties: The CAI can directly issue fines up to 2% of worldwide turnover or C$10M, while courts can impose up to 4% or C$25M for violations such as failing to report data breaches, conduct PIAs, or comply with data disposal rules, etc.

Quebec Law 25

22 SEP 24

Privacy Impact Assessments (PIAs): Mandatory for projects involving the collection, use, or disclosure of personal information

Right to Data Mobility/Portabilty and Deletion: Individuals have the right to demand their data be deleted, de-indexed (search engine removal), or transferred to another organization

01 JAN 25

Requirement for Anonymization Register: Organizations that choose to anonymize personal information, rather than destroy it, must document the process and maintain a register detailing anonymized data

Alberta, Canada

Canadian Provincial Updates: Alberta Public Sector Privacy Modernization

04DEC24 and 20MAR25
The *Protection of Privacy Act* (POPA) aims to modernize public sector privacy, with minor amendments introduced 20 MAR 25 to ensure compliance.

11JUL25
The *Freedom of Information and Protection of Privacy Act* (FOIP) was formally repealed and replaced with the POPA and the *Access to Information Act* (ATIA).

POPA, Bill 33, governs how public bodies collect, use and disclose personal information.

ATIA, Bill 34, governs how the public requests access to its records.

Alberta

11 JUN 25

Protection of Privacy Act (POPA) -Replaced the old Freedom of Information and Protection of Privacy (FOIP) Act of 2011 framework for public bodies; and includes:

- Breach Notification - Mandatory notification is required when personal information is involved in a breach with a "real risk of significant harm"
- Prohibition on Selling Data - Public bodies are banned from selling personal information
- Automated Systems - Public bodies must notify individuals if their personal information is used in automated systems to make decisions or recommendations
- Privacy by Design - Public bodies must adopt a privacy-by-design approach
- Higher Penalties - Fines for privacy breaches have increased to a maximum of C$200K for individuals and for organizations
- Access to Information -The new Access to Information Act (AIA) allows for faster (30 business days) responses but allows agencies to reject "overly broad" or "abusive" request

Alberta

11JUN26

Protection of Privacy Act (POPA) , Continued

- **Privacy Management Programs (PMPs)** – All public bodies are required to have fully implemented PMPs, including designated privacy officers and staff training

NOTE: A one-year grace period for public bodies to fully implement the required privacy management programs under POPA expires 11JUN26.

Alberta

11 JUN 25

The Access to Information Act (ATIA) - Replaced the old Freedom of Information and Protection of Privacy (FOIP) Act of 2011 framework for public bodies; it allows public bodies to disregard requests deemed abusive, frivolous or excessively broad, and includes:

- **Purpose:** The Act enhances accountability and transparency, allowing public access to records while protecting confidential information
- **Scope:** Applies to public bodies, including provincial health agencies, universities, technical institutes, colleges, and Metis settlements
- **Process:** Requests for information, such as city reports or, in some cases, personal records, usually require a $25 fee
- **Timelines:** Public bodies typically have 30 business days to respond to requests
- **Changes:** The new Act introduces broader exceptions for Cabinet confidences, workplace investigations, and labor relations, while exempting certain information from court databases

Canadian Provincial Updates: Ontario Bill 194 –Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024

01 JUL 25

Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act*, 2024, introduces major changes to the *Freedom of Information and Protection of Privacy Act (FIPPA)* and establishes new regulations for AI and cybersecurity, with key provisions taking effect throughout 2025 and 2026.

Ontario, Canada

Ontario Bill 194

24 NOV 24

Legislative Enactment: Received Royal Assent, amending FIPPA to require privacy breach reporting and Privacy Impact Assessments (PIAs) for provincial institutions, and creating the *Enhancing Digital Security and Trust Act* (EDSTA) to regulate AI and cyber security in the public sector. Also, the Supreme court ruled that the Charter applies to Ontario public school boards, impacting workplace privacy analysis.

01 JUL 25

Amendments Enacted: Mandating reporting of privacy breaches with a "real risk of significant harm" (RROSH) to the Ontario Information and Privacy Commissioner (IPC) and affected individuals, requiring PIAs for collecting personal information, and enhancing safeguards for personal data.

Ontario Bill 194

15 OCT 25

De-identification Guidelines for Structured Data: Released by the IPC as "not strictly mandated or legally binding regulation," but replacing 2016 guidance and serving as the authoritative standard for meeting legal obligations to protect personal information under Ontario's privacy laws such as FIPPA

Kids Online Safety and Privacy Month Act, 2025: enacted to raise awareness of children's online safety and privacy; legally recognized but not mandated as a strict, penalty-driven or funded regulation, instead serving as an awareness-focused annual observance to promote digital safety education

31 MAR 26

First annual reports on privacy breaches are due from provincial institutions

Nova Scotia, Canada

Canadian Provincial Updates: Nova Scotia Major Modernization Legislation

26SEP25

New Freedom of Information and Protection of Privacy (FOIPOP) Act, Bill 150, passed, consolidating old *FOIPOP Act*, the *Privacy Review Officer Act*, and the *Personal Information International Disclosure Protection Act (PPDPA)* into a single updated framework

03OCT25

Social Insurance Number Protection Act (SINPA) and the Frivolous and Vexatious Request Rules passed as part of the Protecting Nova Scotians Act (Bill 127)

Nova Scotia Bill 150 FOIPOP Act

26 SEP 25

Independent Oversight: The Information and Privacy Commissioner is now an Officer of the Legislature, strengthening independence from the government

Expanded Scope: Privacy oversight now extends to municipalities and villages

Mandatory Breach Notification: Public bodies must notify individuals if a privacy breach carries a "significant risk of harm"

Privacy Assessments: Public bodies are now required to conduct Privacy Impact Assessments (PIAs) for any new project involving personal information

Stricter Penalties: Maximum fines increased to $10,000 for individuals and $50,000 for organizations

Nova Scotia Bill 127
Protecting Nova Scotians Act

03 OCT 25

Social Insurance Number Protection Act (SINPA) (2025): Part of Bill 127 (the Protecting Nova Scotians Act), this law prohibits collecting an individual's Social Insurance Number (SIN) during commercial activities unless required by law. Violations can result in fines up to $500,000

Frivolous and Vexatious Request Rules (2025): In early 2025, new rules were added allowing public bodies to refuse requests that are deemed frivolous, vexatious, or unduly repetitive, subject to the Commissioner's approval

Alberta & British Columbia Personal Information Protection Act

PIPA-AB (Alberta)

- Updated 2014.
- Applies to consumers and employees
- Limitations on use
- Limitations on disclosure
- Limitations on collection
- Core rights of access, correction, accuracy
- Limits on retention
- Requires protection of the information

- Requires Consent to collect and process.
- Requires appointment of DPO or other person responsible for compliance with the law.
- Breach notification, including breach registry

PIPA-BC (British Columbia)

- Dates to 2003 with periodic, minor updates.
- Applies to consumers and employees
- Limitations on use
- Limitations on disclosure
- Limitations on collection
- Core rights of access, correction, accuracy
- Limits on retention
- Requires protection of the information