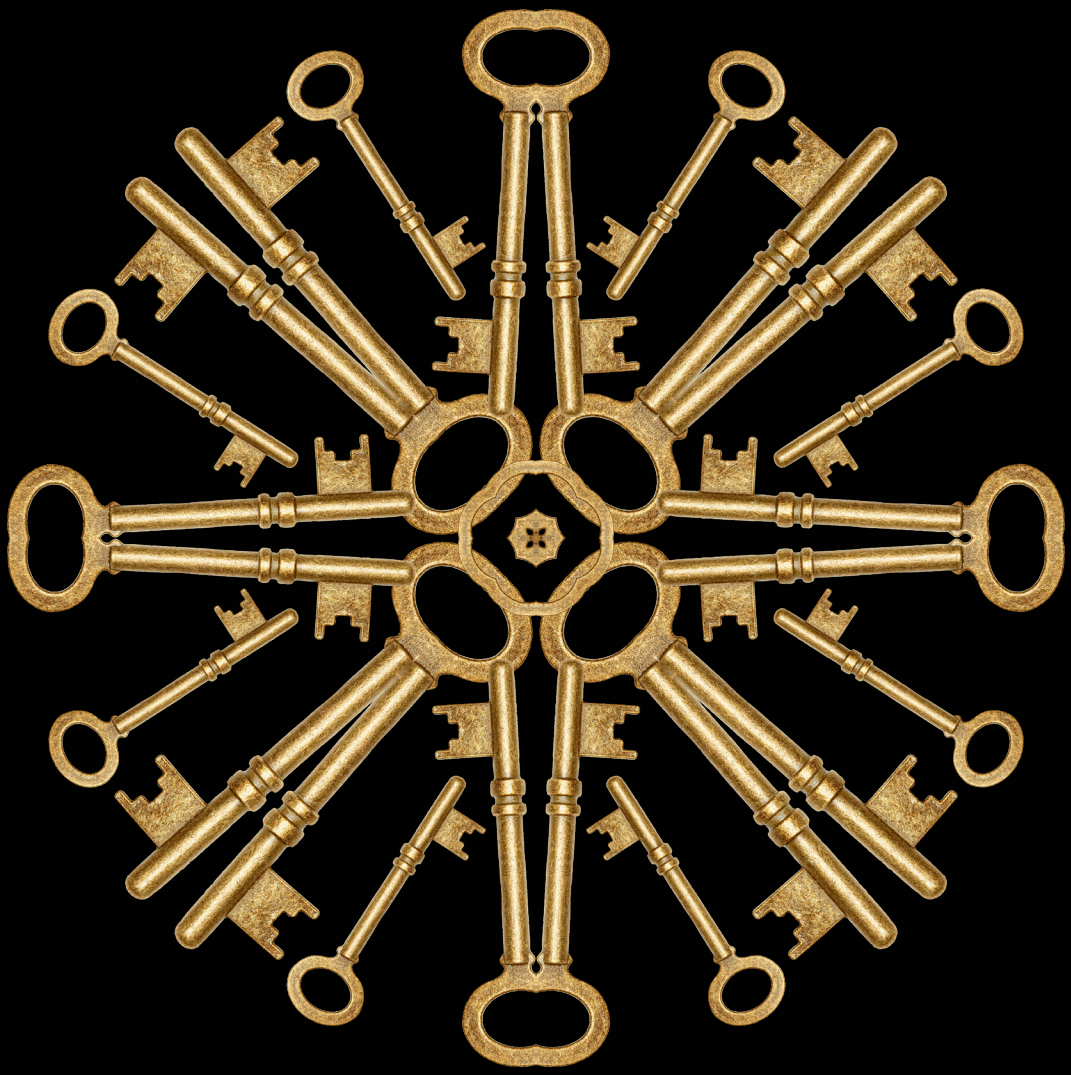
Deloitte.



GDPR and Canadian organizations: Addressing key challenges

Cyber Risk

The regulation frequently referred to as the strictest data-protection law in the world is coming into full effect in just a few months. While it originated overseas, the European General Data Protection Regulation (GDPR) will affect all Canadian organizations that handle the personal data of anyone in the European Union—and they need to be ready for it.

The GDPR strengthens the rights of individuals over their personal data, setting a higher threshold for both transparency and consent. Any organization that collects, uses, stores, discloses, or processes the personal data of anyone residing in the European Union (EU)—regardless of the individual's citizenship or the location of the organization's headquarters—will be subject to the GDPR. It's serious business: fines for non-compliance are up to €20 million or four percent of an organization's worldwide annual turnover, whichever is higher.

Approved by the European Parliament in April 2016, the GDPR will become effective on May 25, 2018. The grace period to prepare for full compliance is running out; soon those who aren't ready may feel the sting of those hefty fines.

Impact on Canadian companies

Beyond its aims to strengthen individuals' rights over their personal data and to harmonize data protection requirements across the EU, the GDPR represents a new set of legislative requirements that directly affects organizations in Canada. One of the most relevant aspects is its principle of extraterritoriality: the regulation will apply to all organizations around the world that handle the personal data of people who are located within the EU, regardless of the individual's citizenship status and the location of the organization.

This means that whether or not an organization has a physical presence in the EU, it will have to comply with the GDPR if it offers goods or services to individuals located in the EU. For instance, a Canadian retail company that doesn't have offices or stores on EU soil but still collects the personal data of clients located there through its websites and/or mobile apps will need to comply with the GDPR.

To fully understand their compliance obligations, Canadian companies affected by the GDPR will need to identify and address requirements beyond existing Canadian privacy laws, such as those under the Personal Information Protection and Electronic Documents Act (PIPEDA). Although specific measures will have to be assessed on a case-by-case basis, the following provide an overview of key compliance areas as well as potential solutions to challenges.

1. Accountability

Many of the accountability efforts Canadian organizations have been making so far to ensure their compliance with Canadian privacy laws will have to be augmented to meet the GDPR's mandatory requirements. In particular, organizations subject to the GDPR will soon be required to demonstrate their compliance and be transparent about it. For many, this will mean extending their current privacy practices to explicitly include the protection of the personal data of both their customers and employees in the European Union.

Organizations should also implement or enhance an accountability framework to govern personal data processing, establishing a culture of privacy across the business. This framework should ensure the organization documents and keeps records of the technical and organizational measures it implements for protecting personal data. For instance, they should document roles and responsibilities for privacy, develop and implement internal and external privacy policies and processes, maintain up-to-date records of data-processing activities, demonstrate that documented privacy impact assessments are conducted before they use new technologies, and track employee attendance at privacy training sessions.

Key privacy protection measures, which Canadian organizations were only required to adhere to under Canadian sector-specific legislation, or that were generally recommended as privacy best practices, will now be mandatory legal requirements under the GDPR. These include:

- Appointing a Data Protection Officer (DPO): Organizations whose core activities include regular or systematic monitoring of personal data or large-scale data processing must hire a DPO. Those that don't have a physical presence in the EU but still process EU data subjects' personal data must designate a representative in the EU to act on its behalf.
- Conducting privacy impact assessments (PIAs): Canadian organizations must perform a PIA before conducting any data processing operations likely to result in a high risk to the rights and freedoms of EU data subjects, such as migrating

information to the cloud or performing data analytics. Companies must also document how the PIA recommendations will be incorporated into the project implementation. Furthermore, where a PIA identifies a high risk, the organization must consult the corresponding EU supervisory authority and incorporate the authority's recommendations into the final solution or project before they launch it.

- Keeping records of processing activities: Although subject to legal exemptions, Canadian organizations as a rule must create and retain records of certain data processing activities, such as purposes of the processing, categories of data, categories of recipients of data, and retention periods. They can achieve this by developing data inventories and performing data mapping exercises, which will provide them with visibility into their data assets. Getting a clear picture of where data lives in the organization and where it will be held after it's shared with third parties is the first step toward the design and implementation of adequate data protection strategies.
- Protecting personal data by default and by design: Companies can only collect, process, share, and store the minimal amount of data required for the intended purpose and, where possible, use pseudonymization techniques at the earliest opportunity. They should also be able to demonstrate that "privacy by default" is at the core of the design of any product, service, or application. "Privacy by design" is demonstrated when a solution is configured such that the default settings protect user privacy, or when architectural and technical documents show that privacy was a prerequisite at the design stage.

The GDPR augments several requirements already imposed by PIPEDA. Some of these include:

- Security: Canadian organizations must implement security measures that are appropriate to the risk, nature, scope, context, and purposes of processing. Beyond this general obligation, four solutions are specifically mentioned:
  - Pseudonymization and encryption
  - Ongoing confidentiality, integrity, availability, and resilience of systems and services
  - Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident
  - Regularly testing, assessing, and evaluating the effectiveness of measures
- Liability of third parties: Any third party processing EU data subjects' personal data on behalf of another organization also has to comply with the GDPR. For Canadian organizations, this means they will have to evaluate and ensure that any third parties processing EU data subjects' data on their behalf comply with the regulation. Further, Canadian organizations that do not have operations in the EU or offer goods and/or services to EU data subjects but still process EU data subjects' data on behalf of another organization would fall under the scope of the GDPR.

Any third party processing EU data subjects' personal data on behalf of another organization also has to comply with the GDPR.

2. Transparency

Recent amendments to PIPEDA imposed by the Digital Privacy Act require a higher transparency standard from Canadian organizations, including using clear and simple language when communicating requests for consent. Requirements about notifying individuals affected by a breach have expanded to include notifying the Office of the Privacy Commissioner as well, along with an obligation to keep and maintain a record of data breaches.

Canadian organizations that have recently revised their privacy notices and breach response programs to ensure compliance with the Digital Privacy Act will need to update those notices and programs to ensure compliance with the GDPR in two main ways:

- Transparency of data processing operations: Organizations will have to explain in concise, transparent, and plain language what personal information they collect, use, and share, in which countries the processing happens, the means by which the data is protected, and the rights of customers and employees regarding their information. They can use videos, tutorials, blogs, and diagrams to provide this level of transparency.
- Breach notification: When a data breach could result in a risk to the rights and freedoms of individuals, organizations must report it to the appropriate supervisory authority within 72 hours of becoming aware of it, and to affected individuals without undue delay. They must also document any breaches involving personal data, including the facts relating to the breach, the impact of it, and the remedial action taken.

3. Consent and other legal grounds

Under PIPEDA, Canadian organizations can ask for express or implied consent, depending on the sensitivity of the personal information and the reasonable expectations of the individual. Similarly, the GDPR requires express consent to process personal information when the organization doesn't have other legitimate grounds to handle it.

In particular, the regulation requires organizations to assess and ensure all their data protection activities rely on one of the following legal grounds:

- Unambiguous, opt-in consent: Organizations must obtain consent from EU data subjects, which must be freely given, specific, informed, and unambiguous (such as ticking a box on a website). The organization's system or application must also have the ability to document consent options, and verifiable parental consent is required for processing the personal data of minors.
- Other legal grounds for processing: In some instances, data may be collected and processed without consent if a limited set of alternative criteria is met (e.g., performance of a contract, legal obligation, vital interest of the data subject, or public interest).

It's key for organizations to evaluate and document the legal grounds that legitimize all their existing data processing activities. This exercise will lead to the identification of those purposes for processing that only rely on the individual's consent (such as the use of personal data for data profiling activities), triggering the need to obtain and manage the unambiguous, opt-in consent of the data subject.

4. Granting of new and stronger rights

Canadian organizations that, as required by PIPEDA, grant individuals the rights to gain access to and correct their personal information need to consider the new set of rights the GDPR entrenches. The purpose of these new rights is to provide EU data subjects with greater knowledge and control over their personal information, and include:

- Right to erasure or "right to be forgotten": Individuals can ask organizations to erase their personal data.
- Right to object to data processing: Individuals can oppose the processing of their personal data, including automated data processing and profiling.
- Right to data portability: Companies must provide individuals with the personal data they hold, in a commonly used and machine-readable format, and transmit it to another organization upon request.

The GDPR also includes legal exemptions that would prevent organizations from granting individual rights. It's therefore key for Canadian organizations to develop processes to grant such rights considering when legal exemptions apply. They should then review the functionality of the systems, tools, and software used to process EU data subjects' personal data to ensure these allow for the implementation of the above-mentioned rights. Such features may include data purging, anonymization capabilities, and data extraction and export mechanisms.

5. Cross-border data transfers

When transferring EU data subjects' data outside the EU, Canadian organizations need to make sure the data is transferred to one of the countries that has been granted an adequacy decision by the European Commission, such as Canada. Otherwise, there must be an adequate data mechanism in place (e.g., Standard Contractual Clauses, Binding Corporate Rules, Privacy Shield, consent).

In practice, one common example is of Canadian organizations that use third-party data processors (such as CRM solutions or cloud service providers) located in the US. While ensuring these third parties are GDPR-compliant and that existing service agreements contain adequate privacy and security provisions, Canadian organizations should focus on identifying in which cases valid data transfer mechanisms are missing, since this would imply an illicit processing of EU data subjects' personal data.

It is also worth noting that Canada's adequacy designation by the European Commission is only partial given that PIPEDA solely applies to employers that are "federal works, undertakings, or businesses" and therefore doesn't afford equivalent protection to the personal data of employees. This implies that private sector organizations regulated under PIPEDA still need to look at model clauses and binding corporate rules before transferring personal information from their EU-based employees to Canada.

The GDPR also includes legal exemptions that would prevent organizations from granting individual rights. It's therefore key for Canadian organizations to develop processes to grant such rights considering when legal exemptions apply.

6. Unstable regulatory privacy landscape

Although the main purpose of the GDPR is to harmonize privacy and data protection requirements across the EU, the regulation does contain open clauses. These allow EU member states to introduce local variations to their national data protection acts in some pre-established areas, such as the age of consent and the processing of employees' personal data. EU member states are in the process of introducing and passing bills to amend their national data protection acts to align with the GDPR. In many cases, the divergences per country resulting from the open clauses are still unclear.

Canadian organizations will also need to pay attention to another EU regulation with extraterritorial effect: the upcoming ePrivacy Regulation. This new piece of legislation is set to replace the current EU ePrivacy Directive, which regulates privacy in electronic networks, to complement and supplement the GDPR.

In preparation for the enforcement of the General Data Privacy Regulation in May 2018, we encourage all affected Canadian organizations to:

- Determine the scope of applicability of the regulation to their business operations.
- Develop a record of data processing activities to provide insights on the personal data assets they're responsible for protecting, including the legal grounds and security measures that support each processing activity.
- Review existing privacy policies and ensure key GDPR compliance areas are included (e.g., legal basis for processing, transfers to third countries, existence of automated decision-making).
- Conduct a gap assessment to identify which existing privacy practices can be used to comply with GDPR.
- Review existing contracts to assess if third-party vendors are GDPR-compliant and, where appropriate, if valid cross-border data transfer mechanisms are in place.
- Train employees in all relevant privacy topics that affect their job duties (e.g., privacy by design, PIAs, breach response protocol, data retention, and destruction practices).
- Assess both IT processes and functionality alongside IT security controls to determine how best to embed GDPR requirements in technology.
- Prioritize and sequence changes required by executing a risk and cost/benefit analysis.
- Set up and undertake regular compliance audits or reviews.

The silver lining

For Canadian organizations subject to the General Data Protection Regulation, it's important to understand how the regulation will affect their business operations and what steps they need to take to ensure the appropriate level of compliance.

It's also important they look at the silver lining: The GDPR presents opportunities to improve their overall privacy and security risk posture, as well as to build a differentiated brand and earn long-term consumer trust.

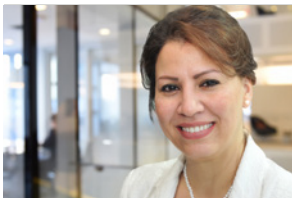
Canadian organizations would serve themselves well to think of these data protection developments as potential springboards to competitive advantage rather than as mere compliance issues that hinder growth.

Contacts

Author

Irene Reverte Sanchez
416-874-4228
irevertesanchez@deloitte.ca

Contacts



East
Mariama Zhouri
514-393-7317
mzhouri@deloitte.ca

West
Don MacPherson
604-640-3120
donmacpherson@deloitte.ca

Toronto
Beth Dewitt
416-643-8223
bdewitt@deloitte.ca

Deloitte.

www.deloitte.ca

About Deloitte

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights and service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals—9,400 of whom are based in Canada—make an impact that matters, please connect with us on LinkedIn, Twitter or Facebook.

Designed and produced by the Deloitte Design Studio, Canada. 18-5535H