Consent Management Provisions across Nations

Wednesday Wisdom
16-10-2024

The enforcement of India's Digital Personal Data Protection Act (DPDP Act)) is round the corner, and data protection is becoming an increasingly important subject for all entities.[1] It is important to note that as per UNCTAD statistics, 71% of the countries have data protection and privacy legislations and about 9% have draft legislations.[2]

While every legislation deals with data protection, the compliance provisions sometimes differ and thus the applicability of specific data protection rules is very critical to be understood, especially in international context. The recent arrest of Mr. Pavel Durov, CEO of messaging app Telegram for failure to co-operate with law enforcement over drug trafficking, child sexual content and fraud has resulted due to violations of data protection legislation which sent shock waves throughout the world.[3]

For instance, ABC, a company incorporated in India is engaged in the business of providing software services to its users across the world. In order to provide services, ABC is required to collect personal information of users based out of India, mostly European countries. ABC follows the policies and practices for protecting the data at its organizational level in a secure manner as it deems fit.

It is important to note that in this context, the European Union General Data Protection Regulation **("EU GDPR")** is likely to be applicable to ABC as the EU GDPR has extraterritorial reach, i.e. it applies to any company that processes personal data of EU residents, regardless of where the data collecting entity is located. Thus, compliance guidelines under EU GDPR which may provide for consent management, data protection officers, timely breach notification etc. may become applicable.

While general data protection principles may be followed by ABC, if the specific requirement of applicable legislation is not met, it may be deemed as non-compliance.
This article brings forth certain salient aspects of important data protection legislations. Provisions relating to EU GDPR have been briefly covered under our previous article[4].

[1] The article reflects the general work of the authors, and the views expressed are personal. No reader should act on any statement contained herein without seeking detailed professional advice
[2] Data Protection and Privacy Legislation Worldwide | UNCTAD
[3] https://www.bbc.com/news/articles/cp8ne8r1yy0o
[4]https://www.ynzgroup.co.in/articles/Corporate%20law/DPDP%20Act%202023%20And%20GDPR%20Provisions%20Key%20Points%20Of%20Distinction.pdf

Consent Management for Personal Data varies with jurisdictions across the world. For a better understanding of the same, let us understand the comparative analysis of Consent Management in the territories of Canada and European Union which are governed by Personal Information Protection and Electronic Documents Act, Canada[5] (PIPEDA) and EU GDPR respectively.

Like most data protection regulations, both these Regulations also share same fundamentals with respect to the principles relating to Consent for processing the Personal Data:

1. **Mandatory Consent:** Consent is required for collection of personal information and subsequent use or disclosure of this information.
2. **Processing without consent permissible in certain exceptional cases:** In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example -
   a. legal, medical, or security reasons may make it impossible or impractical to seek consent.
   b. When information is being collected for the detection and prevention of fraud or for law enforcement seeking the consent of the individual might defeat the purpose of collecting the information.
3. **Free Consent:** Organization shall not compel any individual to give consent for collection, use or disclosure of information beyond the required and legitimate purpose.
4. **Purpose specific consent:** Form for consents sought by organizations may vary depending upon the circumstances and type of information.
5. **Authorized representative:** Consent can also be given by an authorized representative (such as legal guardian or a person having power of attorney)[6].

Let us understand the comparative analysis of the Consent Management across European Union and Canada:

[5] Canada has 28 federal, provincial and territorial data privacy statutes, however for the purpose of this Article, we shall be covering the provisions of Personal Information Protection and Electronic Documents Act, Canada. Organizations in the Northwest Territories, Yukon and Nunavut are considered FWUBs and therefore are covered by PIPEDA. PIPEDA does not apply to provincially-regulated organizations within the province of Quebec

[6] Schedule 1 Principle 4.3 of Personal Information Protection and Electronic Documents Act, Canada Article 7 of EU GDPR

Provision of the Act	EU General Data Protection Regulation	Personal Information Protection and Electronic Documents Act, Canada
What is the applicability of the Regulations?	Applies to processing of Personal Data wholly or partly by automated means[7]. Applicable to organizations established in the European Union which process the Personal Data. Also applicable to any Organization which processes Personal Data of any EU individuals regardless of the Organization location[8]	Applies to every Organization in Canada that collects, uses or discloses the Personal Data in course of commercial activities. Applies to Organizations that use Personal Data of an employee with the Organization that collects, uses or discloses such data in connection to the operations of federal work, undertaking or business[9].
What do you mean by Valid Consent?	Freely given, specific, informed and unambiguous indication of individual's wishes. By way of a statement or clear affirmative action signifying agreement to processing of Personal Data[10].	If the individual consenting to the processing of Personal Data understands the nature, purpose and consequences of collection, use or disclosure of Personal Data[11].
In what format can the Consent be collected by an Organization?	Consent can be collected from an individual by any of the following ways: • An opt-in form such as ticking box while visiting a website • Choosing technical setting for services • A declaration • In electronic format[12]	A consent can be given by individuals in any of the following ways: • An application form • Checkoff box • Oral consent over telephone • Consent of an individual at the time of use of product or service[13]

[7] Article 2 of EU GDPR
[8] Article 3 of EU GDPR
[9] Section 4 of Personal Information Protection and Electronic Documents Act, Canada
[10] Article 4(11) of EU GDPR
[11] Section 6.1 of Personal Information Protection and Electronic Documents Act, Canada
[12] Recital 32 of EU GDPR and https://gdpr-info.eu/issues/consent/
[13] Schedule 1 Principle 4.3 of Personal Information Protection and Electronic Documents Act, Canada

Provision of the Act	EU General Data Protection Regulation	Personal Information Protection and Electronic Documents Act, Canada
Who shall be accountable for compliances relating to Personal Data in Organizations?	The Organization which determines the purpose of processing the Personal data shall be accountable. They shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation[14].	Every organization should designate an individual or group of individuals who shall be accountable for organization's compliance. Identity of such designated individuals can be made known upon request[15].
What are the general Safeguards an Organization needs to maintain to secure the Personal Data?	• pseudonymization and encryption of personal data; • the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; • the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; • a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing[16].	Security safeguards are to be implemented by Organizations appropriate to the sensitivity of the Personal data, irrespective of format in which it is held vide any of the following methods: • physical measures, for example, locked filing cabinets and restricted access to offices; • organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and • technological measures, for example, the use of passwords and encryption. Along with the above methods, Organizations shall make their employees aware of importance of maintaining the confidentiality of Personal Data[17].

[14] Article 24 of EU GDPR
[15] Schedule 1 Principle 4.1 of Personal Information Protection and Electronic Documents Act, Canada
[16] Article 32 of EU GDPR
[17] Schedule 1 Principle 4.7 of Personal Information Protection and Electronic Documents Act, Canada

Provision of the Act	EU General Data Protection Regulation	Personal Information Protection and Electronic Documents Act, Canada
Can individuals withdraw their Consent to processing Personal Data?	Yes, and the withdrawal of consent must be an easy process and similar to giving consent.[18]	Yes, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal[19].
Who shall be notified in case of non-compliances by the Organization?	Each member state of European Union shall designate one or more independent public authorities to be responsible for monitoring and application of EU GDPR.[20]	Commissioner appointed by the Office of the Privacy Commissioner of Canada is designated to oversee the application of statute and to investigate the disputes between Organizations and individuals[21]
What are the Penalties which are levied on Organizations?	The maximum fine that can be imposed under the GDPR is either 20 million euros or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher[22].	Offences under this Regulation are typically do not exceed $10,000 or $100,000 depending on the type of violation[23]

[18] Article 7 of EU GDPR
[19] Schedule 1 Principle 4.3 of Personal Information Protection and Electronic Documents Act, Canada
[20] Article 51 of EU GDPR
[21] Section 10(11) of Personal Information Protection and Electronic Documents Act, Canada
[22] Article 83 of EU GDPR
[23] Section 28 of Personal Information Protection and Electronic Documents Act, Canada

Each framework has its strengths depending on the sensitivity of the information and the regulatory context. However, GDPR's strict guidelines and heavier penalties encourage a higher degree of compliance and transparency in consent management across the board and thus PIPEDA may also undergo amendments as per the new bill proposed in the Canadian parliament[24].

Irrespective of the jurisdiction, one must remember certain key principles of data protection:

a) Consent is a quintessential regime in the legal provisions for data protection;
b) Each organization must implement strict data protection policies and review them regularly;
c) Organizations must establish proper procedures for consent management and to receive grievances;
d) Employees and persons handling personal data should be trained and sensitized towards security policies;
e) Organizations should publish brochures explaining organization policies for providing and withdrawing consents for the individual.

[24] Law in Canada - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com)

For any feedback or response on this article, the authors can be reached on riddhi.bhosale@ynzgroup.co.in and ashvini.kandalgaonkar@ynzgroup.co.in

Author: Riddhi Bhosale

Riddhi is an Associate at YNZ Legal. By qualification she has completed her Bachelor of Science in Biotechnology and Bachelor of Law from University of Mumbai.

Co-author: Ashvini Kandalgaonkar

Ashvini is a Partner- Corporate Legal Advisory, She is experienced in corporate litigation and non- litigation. She provides training required under POSH Act.