Data Privacy Regulation Chart

	GDPR	PIPEDA	PIPA
What event triggers the obligation?	Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that has been transmitted, stored, or otherwise processed is subject to the breach reporting rules.	A breach of security safeguards involving personal information is subject to the breach reporting rules.	Any incident involving the loss of or unauthorized access to or disclosure of personal information is subject to the breach reporting rules.
Is there a threshold standard when reporting is mandatory?	Notification must be given unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.	An organization must report any breach of security safeguards involving personal information if it is reasonable to believe that the breach creates a real risk of significant harm to an individual.	Notification of a breach must be given where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss, or unauthorized access or disclosure.
Does the law define factors that influence the risk or harm?	No.	Definition: "significant harm includes 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." Factors indicating a real risk of significant harm are the sensitivity of the personal information involved in the breach; and the probability that personal information has been, is being or will be misused.	No.
Does the law define how quickly one must report?	The processor shall notify the controller without undue delay after becoming aware of a personal data breach. The controller shall, within 72 hours of becoming aware of a breach, notify the supervisory authority.	The notification must be given as soon as feasible after the organization determines that the breach has occurred.	Notification must be given without unreasonable delay.

	Where notification is not made within 72 hours, reasons must be given for the delay. When it would cause undue delay to provide the required information at the same time, the information may be provided in phases.		
Reporting to the commissioner?	Controllers must notify the supervisory authority of the given EU member state.	Yes, to the federal Privacy Commissioner (in this column, the "Commissioner").	Yes, to the provincial Information and Privacy Commissioner (in this column, the "Commissioner").
Does the law prescribe what must be reported to the commissioner?	The notice must contain: (a) a description of nature of personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) the name and contact details of the data protection officer or other contact person; (c) a description of the likely consequences of the personal data breach; and (d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate possible adverse effects.	The notice must contain: (a) a description of the circumstances of the breach; (b) the day on which, or the period during which, the breach occurred; (c) a description of the personal information involved in the breach; (d) an estimate of the number of individuals to whom there is a real risk of significant harm; (e) a description of any steps the organization has taken to reduce the risk of harm; (f) a description of any steps the organization has taken to notify individuals of the breach; and (g) the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the breach.	The notice must contain: (a) a description of the circumstances of the breach; (b) the day on which, or the period during which, the breach occurred; (c) a description of the personal information involved in the breach; (d) an assessment of the risk of harm to individuals as a result of the breach; (e) an estimate of the number of individuals to whom there is a real risk of significant harm; (f) a description of any steps the organization has taken to reduce the risk of harm; (g) a description of any steps the organization has taken to notify individuals of the breach; and (h) the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the breach.
What sanction arises if one fails to report to the commissioner?	The supervisory authority of the given EU state may issue orders, warnings, or reprimands (including administrative fines) against a controller or processor.	It is an offence to fail to provide notice to the Commissioner, and may result in a fine of up to $100,000 for an organization. The Court may order the organization to: correct its practices; and publish a notice of any action taken to correct its practices.	It is an offence to fail to provide notice to the Commissioner, and may result in a fine of up to $100,000 for an organization.
Reporting to the individual?	When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall	An organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the	The Privacy Commissioner may require the organization to notify individuals' of the loss of their personal data.

	communicate the personal data breach to the data subject without undue delay.	organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.	
Does the law address reporting to others?	No.	An organization that notifies an individual of a breach of security safeguards shall notify any other organization, including government institutions, of the breach if the notifying organization believes that the other organization concerned may be able to reduce the risk of harm.	No.
Does the law prescribe what must be reported to the individual?	The notice must include: • a description, in clear and plain language, of the nature of the personal data breach; • the name and contact details of the data protection officer or other contact person; • a description of the likely consequences of the personal data breach; and • a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate possible adverse effects.	The notice must include: • a description of the circumstances of the breach; • the day on which, or period during which, the breach occurred; • a description of the personal information that is the subject of the breach; • a description of the steps that the organization has taken to reduce the risk of or mitigate any harm to the affected individual; • a description of the steps that the affected individual could take to reduce the risk of or mitigate any harm resulting from the breach; • a toll-free number or email address that the affected individual can use to obtain further information about the breach; and • information about the organization's internal complaint process and about the affected individual's right, under PIPEDA, to file a complaint with the Commissioner.	The notice must include: • a description of the circumstances of the breach; • the date on which or time period during which the breach occurred; • a description of the personal information involved in the breach; • a description of any steps the organization has taken to reduce the risk of harm; and • contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure.
Does the law permit indirect notification of individuals?	Yes, provided that notifying the individual or individuals would involve "disproportionate effort."	Yes, provided that: • direct notification would be likely to cause further harm to the affected individual; • direct notification would be likely to cause undue hardship for the organization; or • the organization does not have contact information.	Notification may be given to an individual indirectly if the Commissioner so allows.

What sanction arises if one fails to report to the individual?	The data subject has the right to: • lodge a complaint with a supervisory authority; • an effective judicial remedy against a controller or processor (where the supervisory authority does not handle the complaint within three months); and • receive compensation for material or non-material damage suffered.	The Court may order the organization to: • correct its practices, pay damages to the complainant, including damages for humiliation; and • publish a notice of any action taken to correct its practices.	The Commissioner may make any order it considers appropriate. The Court may order the organization to pay damages to the complainant for loss or injury.
Does the law mandate record keeping requirements?	The controller shall document any personal data breaches, including facts relating to the breach, its effects, and the remedial action taken. This documentation will allow the supervisory authority to verify compliance with the GDPR.	• Organizations must keep and maintain a record of every breach of security safeguards involving personal information under its control. • Records must be kept for 24 months following the date the organization determines that the breach has occurred.	PIPA does not impose any specific requirements to keep records related to breaches.
Does the law contemplate exemptions to the notification responsibilities?	Notice to the individual is not required in any of the following circumstances: • the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption; • the controller has taken subsequent measures which ensure that the risk to the rights of data subjects is no longer likely to materialize; or • it would involve disproportionate effort, in which case there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	The organization is not required to notify the individual of a breach if doing so is prohibited by law. The organization is not required to notify the Commissioner or the individual if it is not reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.	The organization is not required to give notice to the Commissioner if there is no real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure of personal information. The organization is not required to give notice to the individual unless so ordered by the Commissioner.

Reference: https://www5.bennettjones.com/Blogs-Section/Breach-Notification-Rules-under-GDPR-PIPEDA-and-PIPA