







COMPARATIVE TABLE OF SECURITY INCIDENT REPORTING MECHANISMS

Fasken's Privacy and Cybersecurity Practice Group

FASKEN

	CANADA 	ALBERTA 	EUROPEAN UNION 	QUÉBEC 
	<i>Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5</i>	<i>Personal Information Protection Act (Alberta), SA 2003, c P-6.5</i>	<i>General Data Protection Regulation (EU 2016/679)</i>	<i>Bill 64, An Act to modernize legislative provisions as regards the protection of personal information (Québec)</i>
1. Effective date	November 1, 2018	November 26, 2009	May 25, 2018	N/A
2. Affected organizations in Canada	All organizations that collect, use or disclose personal information as part of their commercial activities, except federal institutions under the Privacy Act (RSC 1985, c P-21).	All provincially regulated private organizations and enterprises operating under the jurisdiction of the Province of Alberta and, in some cases, non-profit organizations operating therein.	Extraterritorial application to any organization that processes any personal data connected with (a) goods or services offered to persons concerned in the European Union (the "EU"); (b) tracking a person's behaviour if this behaviour happens in the EU.	Any "enterprise" (within the meaning of the Civil Code of Québec) that collects, holds, uses or communicates personal information. This excludes public bodies within the meaning of the Act respecting access to documents held by public bodies and the protection of personal information
3. Nature and definition of protected information	"Personal information" meaning any information about an identifiable individual, in any format or medium.	"Personal information" meaning any information about an identifiable individual, in any format or medium.	"Personal data" meaning any information relating to an identified or identifiable natural person, in any format or medium.	"Personal information" meaning any information about a natural person allowing that person to be identified.
4. Nature of the triggering event	"[A]ny breach of security safeguards involving personal information under [an organization's] control".	Any incident involving the loss of or unauthorized access to or disclosure of the personal information that an organization has under its control.	A personal data breach.	The enterprise has cause to believe that a confidentiality incident has occurred involving personal information it holds.

	CANADA	ALBERTA	EUROPEAN UNION	QUÉBEC
5. Additional reporting criteria	When it is reasonable to believe that the breach creates a “real risk of significant harm” to the persons concerned. Significant harm has a broad interpretation and covers a wide range of situations such as bodily harm, humiliation, damage to the 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.	<p><u>Notice to the Commissioner:</u></p> <ul style="list-style-type: none"> where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the incident. <p><u>Notice to the persons concerned:</u></p> <ul style="list-style-type: none"> when the above criterion is met and the Commissioner, once notified, requires it. 	<p><u>Notice to the competent supervisory authority:</u></p> <ul style="list-style-type: none"> when the personal data breach is likely to result in a risk to the rights and freedoms of natural persons. <p><u>Notice to the persons concerned:</u></p> <ul style="list-style-type: none"> only if there is a “high risk to the rights and freedoms” of this person. 	<p>Must be reported if the incident presents a risk of serious injury. The incident must be reported to the supervisory authority and to the persons concerned.</p> <p>In assessing the risk of injury to a person whose personal information is concerned by a confidentiality incident, a person carrying on an enterprise must consider, in particular, the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes.</p>
6. Responsible organization to notify	Office of the Privacy Commissioner of Canada	Office of the Information and Privacy Commissioner of Alberta (the “Commissioner”)	Supervisory authority for each member State (CNIL, ICO, etc.)	The Commission d'accès à l'information
7. Reporting timeframe	“[A]s soon as feasible” after the organization determines that the breach has occurred.	“[W]ithout unreasonable delay”.	<p><u>Notice to the competent supervisory authority:</u></p> <ul style="list-style-type: none"> “[W]ithout undue delay and, where feasible, not later than 72 hours after the controller becomes aware of the data breach. Where the notification is not made within 72 hours, it shall be accompanied by reasons for the delay. <p><u>Notice to the persons concerned:</u></p> <ul style="list-style-type: none"> “[A]s soon as possible”. 	The incident must be reported “promptly”.

		CANADA	ALBERTA	EUROPEAN UNION	QUÉBEC
8.	Other particularities	Organizations that discover a security breach must keep and maintain a record of every breach so discovered whether or not an analysis of the situation shows that the breach creates a “real risk of significant harm”.		The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.	An enterprise that has cause to believe that a confidentiality incident has occurred involving personal information the person holds must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature. It must also keep a register of confidentiality incidents.