TABLEAU COMPARATIF DES MÉCANISMES DE SIGNALEMENT D'INCIDENTS DE SÉCURITÉ

Groupe de pratique Protection des renseignements confidentiels et vie privée de Fasken

FASKEN

		CANADA	ALBERTA	UNION EURPÉENNE	QUÉBEC
		Loi sur les renseignements personnels et les documents électroniques, LC 2000, c. 5	*Personal Information Protection Act, SA 2003, c P-6.5*	*Règlement général sur la protection des données (UE 2016/679)*	*Projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*
1.	**Date de prise d'effet**	1er novembre 2018	26 novembre 2009	25 mai 2018	N/A
2.	**Organisations assujetties au Canada**	Toutes les organisations qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de ses activités commerciales, à l'exclusion des institutions fédérales sujettes à la Loi sur la protection des renseignements personnels (LRC 1985, c P-21).	Toutes les organisations et entreprises du secteur privé sous réglementation provinciale opérant dans la juridiction de la province de l'Alberta et, dans certains cas, aux organismes sans but lucratif qui s'y trouvent.	Application extraterritoriale à toute organisation effectuant tout traitement de données à caractère personnel relativement à (a) l'offre de bien ou services à des personnes concernées dans l'Union européenne (l'« UE »); (b) au suivi du comportement de personnes si ce comportement a lieu au sein de l'UE.	Toute « entreprise » (au sens du Code civil du Québec) qui recueille, détient, utilise ou communique des renseignements personnels À l'exclusion des organismes publics au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
3.	**Nature et définition de l'information protégée**	Les « renseignements personnels », soit tout renseignement concernant un individu identifiable, quel que soit le support ou le format.	Les « renseignements personnels », soit tout renseignement concernant un individu identifiable, quel que soit le support ou le format.	Les « données personnelles » ou « données à caractère personnel », soit toute information se rapportant à une personne physique identifiée ou identifiable, quel que soit le support ou le format.	Les « renseignements personnels » sont tout renseignement qui concerne une personne physique et permet de l'identifier.
4.	**Nature de l'incident déclencheur**	« [T]oute atteinte aux mesures de sécurité qui a trait à des renseignements personnels dont une organisation a la gestion. »	Tout incident impliquant la perte, l'accès non autorisé ou la divulgation des renseignements personnels dont une organisation a le contrôle.	Une violation de données à caractère personnel.	L'entreprise a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient.

		CANADA	ALBERTA	UNION EURPÉENNE	QUÉBEC
5.	**Critères additionnels de signalement**	Lorsqu'il est raisonnable de croire que la violation engendrera un « risque réel de préjudice grave » aux personnes intéressées. Cette notion de préjudice grave est interprétée largement, comprenant un large éventail de situations telles que la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles	Avis au Commissaire : • lorsqu'une personne raisonnable estimerait qu'il existe un risque réel de préjudice important pour une personne en raison de cet incident. Avis aux individus concernés : • lorsque le critère ci-dessus est rencontré et que le Commissaire, une fois notifié, le requiert.	Avis à l'autorité de contrôle compétente : • lorsque l'atteinte est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Avis aux individus concernés : • qu'en présence d'un « risque élevé aux droits et libertés » de cet individu.	Signalement si l'incident présente un risque qu'un préjudice sérieux soit causé. Le signalement doit être fait à l'autorité de contrôle et aux individus concernés. Lorsqu'elle évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, la personne qui exploite une entreprise doit considérer notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.
6.	**Organisme responsable devant être notifié**	Commissariat à la protection de la vie privée du Canada	Commissaire à l'information et à la protection de la vie privée de l'Alberta (le « Commissaire »)	Autorité de contrôle propre à chaque État membre (CNIL, ICO, etc.)	La Commission d'accès à l'information
7.	**Délai de signalement**	« [L]e plus tôt possible » après que l'organisation ait conclu à l'atteinte.	« [S]ans délai raisonnable ».	Avis à l'autorité de contrôle compétente : • « [D]ans les meilleurs délais » et si possible, au plus tard 72 heures après que le responsable de traitement ait pris connaissance de la violation. Lorsque la notification n'a pas lieu dans les 72 heures, elle doit être accompagnée des motifs du retard. Avis aux individus concernés : • « [D]ans les meilleurs délais ».	L'incident doit être signalé « avec diligence ».
8.	**Autres particularités**	Les organisations qui découvrent une atteinte aux mesures de sécurité doivent tenir et conserver un registre de toutes les atteintes ainsi découvertes, et ce, qu'elles concluent à l'issue de leur analyse situation que cette atteinte pose ou non un « risque réel de préjudice grave ».		Le responsable du traitement doit documenter toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.	• Une entreprise qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent. Elle doit aussi doit tenir un registre des incidents de confidentialité.