CANADA

CONSOLIDATION

CODIFICATION

Breach of Security Safeguards Regulations

Règlement sur les atteintes aux mesures de sécurité

SOR/2018-64

DORS/2018-64

Current to December 12, 2018

Last amended on November 1, 2018

À jour au 12 décembre 2018

Dernière modification le 1 novembre 2018

Published by the Minister of Justice at the following address:
http://laws-lois.justice.gc.ca

Publié par le ministre de la Justice à l'adresse suivante :
http://lois-laws.justice.gc.ca

OFFICIAL STATUS OF CONSOLIDATIONS

Subsections 31(1) and (3) of the *Legislation Revision and Consolidation Act*, in force on June 1, 2009, provide as follows:

Published consolidation is evidence

31 (1) Every copy of a consolidated statute or consolidated regulation published by the Minister under this Act in either print or electronic form is evidence of that statute or regulation and of its contents and every copy purporting to be published by the Minister is deemed to be so published, unless the contrary is shown.

...

Inconsistencies in regulations

(3) In the event of an inconsistency between a consolidated regulation published by the Minister under this Act and the original regulation or a subsequent amendment as registered by the Clerk of the Privy Council under the *Statutory Instruments Act*, the original regulation or amendment prevails to the extent of the inconsistency.

CARACTÈRE OFFICIEL DES CODIFICATIONS

Les paragraphes 31(1) et (3) de la *Loi sur la révision et la codification des textes législatifs*, en vigueur le 1er juin 2009, prévoient ce qui suit :

Codifications comme élément de preuve

31 (1) Tout exemplaire d'une loi codifiée ou d'un règlement codifié, publié par le ministre en vertu de la présente loi sur support papier ou sur support électronique, fait foi de cette loi ou de ce règlement et de son contenu. Tout exemplaire donné comme publié par le ministre est réputé avoir été ainsi publié, sauf preuve contraire.

[...]

Incompatibilité — règlements

(3) Les dispositions du règlement d'origine avec ses modifications subséquentes enregistrées par le greffier du Conseil privé en vertu de la *Loi sur les textes réglementaires* l'emportent sur les dispositions incompatibles du règlement codifié publié par le ministre en vertu de la présente loi.

LAYOUT

The notes that appeared in the left or right margins are now in boldface text directly above the provisions to which they relate. They form no part of the enactment, but are inserted for convenience of reference only.

MISE EN PAGE

Les notes apparaissant auparavant dans les marges de droite ou de gauche se retrouvent maintenant en caractères gras juste au-dessus de la disposition à laquelle elles se rattachent. Elles ne font pas partie du texte, n'y figurant qu'à titre de repère ou d'information.

NOTE

This consolidation is current to December 12, 2018. The last amendments came into force on November 1, 2018. Any amendments that were not in force as of December 12, 2018 are set out at the end of this document under the heading "Amendments Not in Force".

NOTE

Cette codification est à jour au 12 décembre 2018. Les dernières modifications sont entrées en vigueur le 1 novembre 2018. Toutes modifications qui n'étaient pas en vigueur au 12 décembre 2018 sont énoncées à la fin de ce document sous le titre « Modifications non en vigueur ».

TABLE OF PROVISIONS

Breach of Security Safeguards Regulations

Interpretation

1 Definition of Act

Report to Commissioner

2 Report — content, form and manner

Notification to Affected Individual

3 Contents of notification

4 Direct notification — form and manner

5 Indirect notification — circumstances

Record-keeping

6 Record-keeping requirements

Coming into Force

*7 S.C. 2015, c. 32

TABLE ANALYTIQUE

Règlement sur les atteintes aux mesures de sécurité

Définition

1 Définition de Loi

Déclaration au commissaire

2 Contenu et modalités de la déclaration

Avis à l'intéressé

3 Contenu de l'avis

4 Avis direct — modalités

5 Avis indirect — circonstances

Tenue du registre

6 Registre — modalité

Entrée en vigueur

*7 L.C. 2015, ch. 32

Registration
SOR/2018-64 March 27, 2018

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

Breach of Security Safeguards Regulations

P.C. 2018-368 March 26, 2018

Her Excellency the Governor General in Council, on the recommendation of the Minister of Industry, pursuant to subsection 26(1)[a] of the *Personal Information Protection and Electronic Documents Act*[b], makes the annexed *Breach of Security Safeguards Regulations*.

Enregistrement
DORS/2018-64 Le 27 mars 2018

LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES

Règlement sur les atteintes aux mesures de sécurité

C.P. 2018-368 Le 26 mars 2018

Sur recommandation du ministre de l'Industrie et en vertu du paragraphe 26(1)[a] de la *Loi sur la protection des renseignements personnels et les documents électroniques*[b], Son Excellence la Gouverneure générale en conseil prend le *Règlement sur les atteintes aux mesures de sécurité*, ci-après.

[a] S.C. 2015, c. 32, s. 21
[b] S.C. 2000, c. 5

[a] L.C. 2015, ch. 32, art. 21
[b] L.C. 2000, ch. 5

Breach of Security Safeguards Regulations

Règlement sur les atteintes aux mesures de sécurité

Interpretation

Definition of *Act*

1 In these Regulations, ***Act*** means the *Personal Information Protection and Electronic Documents Act*.

Report to Commissioner

Report — content, form and manner

2 (1) A report of a breach of security safeguards referred to in subsection 10.1(2) of the Act must be in writing and must contain

(a) a description of the circumstances of the breach and, if known, the cause;

(b) the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;

(c) a description of the personal information that is the subject of the breach to the extent that the information is known;

(d) the number of individuals affected by the breach or, if unknown, the approximate number;

(e) a description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;

(f) a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach in accordance with subsection 10.1(3) of the Act; and

(g) the name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach.

New information

(2) An organization may submit to the Commissioner any new information referred to in subsection (1) that the organization becomes aware of after having made the report.

Définition

Définition de *Loi*

1 Dans le présent règlement, ***Loi*** s'entend de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Déclaration au commissaire

Contenu et modalités de la déclaration

2 (1) La déclaration d'atteinte aux mesures de sécurité visée au paragraphe 10.1(2) de la Loi est faite par écrit et contient les renseignements suivants :

a) les circonstances de l'atteinte et, si elle est connue, la cause de l'atteinte;

b) la date ou la période où il y a eu atteinte ou, si elle n'est pas connue, une approximation de la période;

c) la nature des renseignements personnels visés par l'atteinte, pour autant qu'elle soit connue;

d) le nombre d'individus visé par l'atteinte ou, s'il n'est pas connu, une approximation de ce nombre;

e) les mesures que l'organisation a prises afin de réduire le risque de préjudice à l'endroit des intéressés qui pourrait résulter de l'atteinte ou afin d'atténuer un tel préjudice;

f) les mesures que l'organisation a prises ou qu'elle entend prendre afin d'aviser les intéressés de toute atteinte en application du paragraphe 10.1(3) de la Loi;

g) le nom et les coordonnées d'une personne qui peut répondre au nom de l'organisation aux questions du commissaire au sujet de l'atteinte.

Nouveaux renseignements

(2) L'organisation peut transmettre au commissaire tout nouveau renseignement visé au paragraphe (1) dont elle prend connaissance après avoir fait la déclaration.

Means of communication

(3) The report may be sent to the Commissioner by any secure means of communication.

Notification to Affected Individual

Contents of notification

3 A notification provided by an organization, in accordance with subsection 10.1(3) of the Act, to an affected individual with respect to a breach of security safeguards must contain

(a) a description of the circumstances of the breach;

(b) the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;

(c) a description of the personal information that is the subject of the breach to the extent that the information is known;

(d) a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;

(e) a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and

(f) contact information that the affected individual can use to obtain further information about the breach.

Direct notification — form and manner

4 For the purposes of subsection 10.1(5) of the Act, direct notification must be given to the affected individual in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances.

Indirect notification — circumstances

5 (1) For the purposes of subsection 10.1(5) of the Act, indirect notification must be given by an organization in any of the following circumstances:

(a) direct notification would be likely to cause further harm to the affected individual;

(b) direct notification would be likely to cause undue hardship for the organization; or

Moyen de communication

(3) La déclaration peut être transmise au commissaire par tout moyen de communication sécurisé.

Avis à l'intéressé

Contenu de l'avis

3 L'avis donné par l'organisation, en application du paragraphe 10.1(3) de la Loi à l'intéressé, relativement à l'atteinte aux mesures de sécurité, contient les renseignements suivants :

a) les circonstances de l'atteinte;

b) la date ou la période où il y a eu atteinte ou, si elle n'est pas connue, une approximation de la période;

c) la nature des renseignements personnels visés par l'atteinte, pour autant qu'elle soit connue;

d) les mesures que l'organisation a prises afin de réduire le risque de préjudice qui pourrait résulter de l'atteinte;

e) les mesures que peut prendre tout intéressé afin de réduire le risque de préjudice qui pourrait résulter de l'atteinte ou afin d'atténuer un tel préjudice;

f) les coordonnées permettant à l'intéressé de se renseigner davantage au sujet de l'atteinte.

Avis direct — modalités

4 Pour l'application du paragraphe 10.1(5) de la Loi, l'avis est donné directement à l'intéressé en personne, par téléphone, par courrier, par courriel ou par tout autre moyen de communication qu'une personne raisonnable estimerait acceptable dans les circonstances.

Avis indirect — circonstances

5 (1) Pour l'application du paragraphe 10.1(5) de la Loi, l'avis est donné indirectement par l'organisation dans l'une ou l'autre des circonstances suivantes :

a) le fait de donner l'avis directement est susceptible de causer un préjudice accru à l'intéressé;

b) le fait de donner l'avis directement est susceptible de représenter une difficulté excessive pour l'organisation;

(c) the organization does not have contact information for the affected individual.

Indirect notification — form and manner

(2) For the purposes of subsection 10.1(5) of the Act, indirect notification must be given by public communication or similar measure that could reasonably be expected to reach the affected individuals.

Record-keeping

Record-keeping requirements

6 (1) For the purposes of subsection 10.3(1) of the Act, an organization must maintain a record of every breach of security safeguards for 24 months after the day on which the organization determines that the breach has occurred.

Compliance

(2) The record referred to in subsection 10.3(1) of the Act must contain any information that enables the Commissioner to verify compliance with subsections 10.1(1) and (3) of the Act.

Coming into Force

S.C. 2015, c. 32

***7** These Regulations come into force on the day on which section 10 of the *Digital Privacy Act* comes into force, but if they are registered after that day, they come into force on the day on which they are registered.

* [Note: Regulations in force November 1, 2018, *see* SI/2018-32.]

c) l'organisation n'a pas les coordonnées de l'intéressé.

Avis indirect — modalités

(2) Pour l'application du paragraphe 10.1(5) de la Loi, l'avis est donné indirectement par une communication publique ou par toute mesure similaire dont on peut raisonnablement s'attendre à ce qu'elle permette de joindre l'intéressé.

Tenue du registre

Registre — modalité

6 (1) Pour l'application du paragraphe 10.3(1) de la Loi, l'organisation conserve le registre de toute atteinte aux mesures de sécurité pendant vingt-quatre mois après la date à laquelle elle conclut qu'il y a eu atteinte.

Conformité

(2) Le registre visé au paragraphe 10.3(1) de la Loi contient tout renseignement qui permet au commissaire de vérifier la conformité aux paragraphes 10.1(1) et (3) de la Loi.

Entrée en vigueur

L.C. 2015, ch. 32

***7** Le présent règlement entre en vigueur à la date d'entrée en vigueur de l'article 10 de la *Loi sur la protection des renseignements personnels numériques* ou, si elle est postérieure, à la date de son enregistrement.

* [Note : Règlement en vigueur le 1er novembre 2018, *voir* TR/2018-32.]