INCIDENT DE CONFIDENTIALITÉ

DÉTAILS POUR LA TRANSMISSION D'AVIS ET LA TENUE D'UN REGISTRE

Votre gouvernement

Québec

TABLE DES MATIÈRES

INTRODUCTION

Les nouvelles obligations auxquelles doivent se conformer les organismes publics, lors de la survenance d'un incident de confidentialité, suscitent des questionnements. Le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité a produit une compilation de questions et de réponses en lien avec le Règlement sur les incidents de confidentialité. Le présent document porte exclusivement sur les avis qui doivent être transmis à la Commission d'accès à l'information et aux personnes concernées, de même que sur la tenue d'un registre qui fait état des incidents de confidentialité.

1. QU'EST-CE QU'UN INCIDENT DE CONFIDENTIALITÉ ?

En quoi un incident de confidentialité consiste-t-il ?

Conformément à l'article 63.9 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Loi sur l'accès), un incident de confidentialité se définit lorsqu'une ou plusieurs de ces situations surviennent :

- l'accès non autorisé par la loi à un renseignement personnel ;
- l'utilisation non autorisée par la loi d'un renseignement personnel ;
- la communication non autorisée par la loi d'un renseignement personnel ;
- la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Exemples :

- Un organisme public qui communique par erreur des renseignements personnels à un mauvais destinataire ;
- Un vol de dossiers qui contiennent des renseignements personnels ;
- Un employé qui accède à des renseignements personnels non nécessaires à l'exercice de ses fonctions ;
- Un employé qui utilise à ses propres fins des renseignements personnels détenus par son organisme public ;
- Un employé qui perd un ordinateur portable, un téléphone mobile ou une clé USB contenant des renseignements personnels.

Quelle est la différence entre un événement de sécurité et un incident de confidentialité ?

Cette distinction terminologique est importante.

Un événement de sécurité, comme défini dans la Directive gouvernementale sur la sécurité de l'information et dans le Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, correspond à « toute forme d'atteinte, présente ou appréhendée, telle une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle sous la responsabilité d'un organisme public ou d'une personne agissant pour ce dernier ».

Un événement de sécurité peut avoir lieu même en l'absence de renseignements personnels, car cela vise toute information ou ressource informationnelle sous la responsabilité d'un organisme public. Un événement de sécurité couvre les atteintes présentes et appréhendées, alors qu'un incident de confidentialité concerne seulement les atteintes présentes. Ainsi, tout événement de sécurité n'est pas nécessairement un incident de confidentialité. Cependant, celui-ci constitue généralement un événement de sécurité, car il s'agit d'une atteinte à la confidentialité d'une ressource informationnelle qui, dans certains cas, peut affecter la disponibilité ou l'intégrité.

2. AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION ET AUX PERSONNES CONCERNÉES

Avis transmis à la Commission d'accès à l'information

Est-il nécessaire de disposer d'un portrait complet de toutes les informations requises par le Règlement sur les incidents de confidentialité avant d'aviser la Commission d'accès à l'information et les personnes concernées ?

En vertu de l'article 63.8 de la Loi sur l'accès, la Commission d'accès à l'information (Commission) doit être avisée avec diligence. Ainsi, dès que l'organisme public a connaissance de la survenance d'un incident de confidentialité présentant un risque qu'un préjudice sérieux soit causé, il doit le déclarer à la Commission. Il doit transmettre un avis à la Commission, lequel comprend les informations requises à l'article 3 du Règlement sur les incidents de confidentialité (Règlement), et cela, en fonction des informations qu'il détient sur la situation à ce moment. En effet, il est possible que l'organisme public ne soit pas en mesure d'avoir un portrait complet de l'incident de confidentialité, au moment de transmettre son avis à la Commission, mais cela ne doit pas l'empêcher de faire sa déclaration.

Toutefois, en application de l'article 4 du Règlement, l'organisme public doit transmettre à la Commission tout renseignement requis devant être inclus dans l'avis, et ce, même lorsque celui ci a déjà été envoyé. L'information complémentaire doit alors être transmise dans les meilleurs délais, dès lors que l'organisme public en a pris connaissance.

N. B. : La Commission peut demander à l'organisme public d'autres informations liées à l'incident de confidentialité, mais non requises par le Règlement.

Quant aux personnes concernées, l'avis doit également être transmis avec diligence et comprendre l'ensemble des informations requises par l'article 5 du Règlement. Un certain délai peut s'appliquer entre le moment où l'organisme public prend connaissance de l'incident et celui où il en avise les personnes concernées.

Ce délai peut être nécessaire afin, par exemple, de cibler les renseignements personnels impliqués, les personnes concernées, les circonstances de l'incident, etc. L'organisme public donne les informations en fonction de sa connaissance, à ce moment, de l'incident de confidentialité.

Lorsqu'un organisme public détecte une intrusion dans son réseau, doit-il aviser systématiquement la Commission, en application du deuxième alinéa de l'article 63.8 de la Loi sur l'accès ?

Non. L'organisme public doit d'abord vérifier si l'intrusion implique des renseignements personnels.

Si tel est le cas, il doit ensuite vérifier si cette compromission présente un risque qu'un préjudice sérieux soit causé. Pour ce faire, il doit considérer notamment les critères de l'article 63.10 de la Loi sur l'accès (à savoir, entre autres, la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables). Si la réponse est oui, il doit alors aviser la Commission et les personnes concernées avec diligence.

Les coordonnées indiquées dans les avis, afin que la Commission ou la personne concernée puisse obtenir de plus amples informations sur l'incident, doivent-elles forcément être celles de la personne responsable de la protection des renseignements personnels ?

Non. Il n'est pas obligatoire que la personne à contacter soit responsable de la protection des renseignements personnels. Il pourrait s'agir, dans certains cas, d'une personne dont les fonctions sont en lien avec la sécurité de l'information dans l'organisme public. Les organismes publics disposent d'une certaine latitude dans la détermination des coordonnées à transmettre à cet égard. L'important est qu'il soit possible, avec ces coordonnées, de communiquer avec une personne apte à répondre aux questions en lien avec l'incident de confidentialité.

Quels sont les moyens susceptibles d'aider l'organisme public à transmettre ses avis avec diligence ?

En application de l'article 63.3 de la Loi sur l'accès, un organisme public doit adopter des règles qui encadrent sa gouvernance à l'égard des renseignements personnels (ex. : politique, directive, procédure, etc.). Ces règles devraient contenir des dispositions sur, notamment, la survenance d'un incident de confidentialité, et tenir compte de la transmission d'avis à la Commission et aux personnes concernées. Il serait opportun d'établir ces règles en collaboration avec les personnes responsables de la sécurité de l'information dans l'organisme public. Des règles claires permettent à l'organisme public de gérer plus efficacement les incidents de confidentialité et d'informer la Commission et les personnes concernées avec diligence.

Un organisme public X a signé un contrat de service d'hébergement d'une base de données qui comprend des renseignements personnels avec l'entreprise Y. Un incident de confidentialité, qui touche cette base de données et qui présente un risque qu'un préjudice sérieux soit causé, survient au sein de l'entreprise Y. À qui la responsabilité de transmettre un avis à la Commission et aux personnes concernées revient-elle ?

L'organisme public demeure, en tout temps, responsable des renseignements personnels qu'il détient, et ce, même si ces derniers sont conservés par un tiers. L'organisme public est donc tenu d'aviser la Commission et les personnes concernées.

N. B. : En vertu de l'article 67.2 de la Loi sur l'accès, le contrat doit inclure une clause qui oblige le prestataire de services à aviser sans délai la personne responsable de la protection des renseignements personnels de toute violation ou tentative de violation d'une exigence relative à la confidentialité du renseignement communiqué.

Si l'organisme public ne possède pas les coordonnées pour joindre toutes les personnes concernées par un incident de confidentialité, que doit-il faire ?

En semblable situation, sauf une exception prévue par le Règlement (ex. : difficulté excessive pour l'organisation), l'organisme public devrait :

- transmettre un avis aux personnes concernées dont elle a les coordonnées ;
- et diffuser un avis public qui lui permet de joindre celles dont il n'a pas les coordonnées.

Avis transmis aux personnes concernées

Avis transmis directement aux personnes concernées

Quels moyens de communication peuvent être utilisés pour transmettre un avis aux personnes concernées par un incident de confidentialité ?

Un tel avis peut être transmis, par exemple :

- par courrier ;
- par courriel ;
- par téléphone ;
- en personne.

N. B. : Il importe que l'organisme public s'assure qu'il s'adresse à la bonne personne concernée (ex. : par téléphone ou au comptoir) ou qu'il détient les bonnes coordonnées (ex. : adresse postale ou courriel). Par conséquent, tout organisme public doit s'assurer que les coordonnées et les renseignements qu'il détient présentent un certain degré de fiabilité.

Les avis doivent être donnés et rédigés en des termes clairs et compréhensibles pour en faciliter la compréhension par les personnes concernées.

Avis public diffusé par tout moyen jugé raisonnablement susceptible de joindre les personnes concernées

Que doit contenir l'avis public ?

Le contenu formulé dans l'avis public devrait correspondre à celui dont il est fait état à l'article 5 du Règlement.

Quels moyens de communication peuvent être utilisés aux fins de diffusion d'un avis public destiné à joindre les personnes concernées par un incident de confidentialité ?

L'alinéa 4 de l'article 6 du Règlement mentionne que l'avis public peut être diffusé par tout moyen jugé raisonnablement susceptible de joindre la personne concernée. L'expression « tout moyen » inclut, par exemple, une publication dans un journal (sur papier ou en ligne) ou la diffusion d'un message à la radio ou à la télévision. L'utilisation d'une combinaison de moyens est recommandée, pour plus de certitude.

L'utilisation d'un ou de plusieurs moyens dépend essentiellement du contexte. Dans certains cas, par exemple, la publication d'un avis, dans un journal local, pourrait être envisagée si l'incident est susceptible de concerner plusieurs personnes d'une même ville et que cette publication y est suffisamment populaire. Dans d'autres situations d'envergure plus importante (ex. : provinciale), un avis publié dans des journaux à grand tirage, voire télédiffusé, pourrait être considéré.

Le Règlement se veut le moins prescriptif possible quant aux moyens de communication préconisés, et ce, afin que l'utilisation d'éventuelles nouvelles formes ne soit pas écartée.

Est-ce que la publication d'un avis public d'incident de confidentialité sur le site Internet de l'organisme public pourrait être suffisante ?

Non. Cette publication ne serait vue que par les gens qui consultent le site, et le nombre de visites n'y est pas suffisant pour que ce moyen utilisé seul remplisse l'exigence réglementaire. Ainsi, la diffusion d'un avis sur le site Internet d'un organisme public ne doit pas être l'unique moyen employé, car à elle seule, elle n'est pas jugée raisonnablement susceptible de joindre les personnes concernées.

Qu'arrive-t-il lorsque l'organisme public ne possède pas les coordonnées des personnes concernées par l'incident de confidentialité (par exemple, s'il détient, dans le dossier d'une cliente ou d'un client, des renseignements personnels d'un tiers dont il ne possède pas les coordonnées) ?

Le paragraphe 3° de l'alinéa 2 de l'article 6 du Règlement prévoit que les personnes concernées dont l'organisme public ne possède pas les coordonnées devraient être informées par un avis public.

Cependant, si le nombre de personnes concernées est limité, l'organisme public peut tenter d'en trouver les coordonnées afin de les joindre individuellement (ce qui est toujours préférable). Il pourrait notamment effectuer des recherches dans des répertoires téléphoniques.

Si ces recherches s'avèrent infructueuses ou si elles aboutissent à seulement une partie des coordonnées, un avis public doit être diffusé.

Dans quelles circonstances un organisme public peut-il conclure que la transmission directe d'un avis est susceptible de représenter une « difficulté excessive » pour l'organisation et qu'un avis public est donc justifié ?

Cela serait le cas, par exemple, si le nombre de personnes concernées par l'incident de confidentialité était considérable et si les ressources humaines et financières affectées à cette démarche étaient proportionnellement moindres, de telle sorte que cela pourrait nuire au déroulement normal des activités de l'organisme public.

Ce serait aussi le cas si un nombre important de personnes étaient concernées par l'incident de confidentialité, mais que l'organisme public ne disposait que des numéros de téléphone de ces gens.

L'organisme public qui invoque des difficultés excessives doit être en mesure d'en faire la preuve, et ce, peu importe la raison mentionnée.

Dans quelles circonstances un organisme public peut-il conclure que la transmission d'un avis directement à la personne concernée est susceptible de causer un « préjudice accru » et qu'un avis public est donc justifié ?

Ces situations ne sont pas typiques et relèvent plutôt de l'exception. Il s'agit notamment de situations où cela pourrait porter atteinte à la vie privée ou à la réputation de la personne concernée. De fait, la transmission directe d'un avis risque de révéler des informations non connues, notamment, à un membre de la famille. Pensons à un cas où le conjoint va chercher le courrier et prend connaissance de l'avis sur lequel est indiquée la nature d'un service que la personne concernée aurait voulu garder confidentiel., on peut aussi songer à une personne ayant fait un don de sperme qui ne souhaiterait peut-être pas recevoir une communication écrite par la poste l'informant d'un incident de confidentialité en raison d'un « préjudice accru » potentiel, etc.).

À titre d'exemple, dans un cas survenu, par le passé, une entreprise qui avait fait l'objet d'un incident de confidentialité exploitait plusieurs sites Internet de rencontres pour adultes, dont l'un s'adressait à des personnes à la recherche d'une aventure extraconjugale en toute confidentialité. Dans ce contexte, la transmission d'un avis par la poste aurait pu créer des ennuis à la personne concernée et à son entourage.

Quelles mesures l'organisme public peut-il suggérer à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer un tel préjudice ?

La Commission a produit un aide-mémoire qui renferme des informations pertinentes quant aux mesures à recommander aux personnes concernées à la suite d'un incident de confidentialité.

3. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Quels incidents de confidentialité doivent être colligés dans le registre dont il est question à l'article 63.11 de la Loi sur l'accès ?

Tous ! Que l'incident présente ou non un risque qu'un préjudice sérieux soit causé, les informations visées à l'article 7 du Règlement devraient être inscrites au registre.

Est-il possible d'utiliser le même registre afin de répertorier les événements de sécurité (article 16 de la Directive gouvernementale sur la sécurité de l'information) et les incidents de confidentialité (article 63.11 de la Loi sur l'accès) ?

Un jumelage de ces informations peut être fait à l'intérieur d'un seul et même registre. Le critère de validité, relativement au registre des incidents de confidentialité, consiste cependant à s'assurer que toutes les informations exigées en vertu de l'article 7 du Règlement s'y trouvent. De plus, il doit être possible de repérer facilement les incidents de confidentialité, notamment dans le cas où la Commission voudrait obtenir une copie du registre.

Advenant que les avis aient été transmis aux personnes concernées par l'incident à plusieurs journées différentes, serait-il possible, dans le registre, d'inscrire une période plutôt que d'énumérer toutes les dates ?

L'article 7 du Règlement prévoit que le registre doit faire mention des dates de transmission des avis à la Commission et aux personnes concernées si l'incident de confidentialité présente un risque qu'un préjudice sérieux soit causé. Les dates peuvent ainsi toutes être indiquées ou, si la transmission des avis s'est échelonnée sur une certaine période, la mention « entre telle et telle date ». Il est toutefois recommandé de garder une trace de toutes les dates de transmission des avis, dans l'éventualité où des précisions seraient demandées par la Commission.