

POLITIQUE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

1. **PRÉAMBULE.** Aux termes des lois sur la protection des renseignements personnels applicables, Broccolini, ses filiales et sociétés affiliées (« **Broccolini** », « **nous** ») sont responsables des renseignements personnels dont elles ont la possession ou le contrôle. Bien que Broccolini prenne les précautions requises et mette en place des mesures de sécurité raisonnables pour protéger les renseignements personnels, un incident de confidentialité est toujours possible. C'est pourquoi Broccolini se dote de la présente Politique afin de gérer d'éventuels incidents de confidentialité et limiter leurs conséquences.
2. **DÉFINITIONS**
 - 2.1. On entend par « **renseignements personnels** » toute information qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.
 - 2.2. On entend par « **incident de confidentialité** » tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection. Par exemple : (1) l'accès non autorisé par la loi à un renseignement personnel; (2) l'utilisation non autorisée par la loi d'un renseignement personnel; (3) la communication non autorisée par la loi d'un renseignement personnel; (4) la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.
 - 2.3. On entend par « **préjudice sérieux** » un acte ou à un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable. Il peut, par exemple, conduire à : l'humiliation; une atteinte à la réputation; une perte financière; un vol d'identité; des conséquences négatives sur un dossier de crédit; une perte d'emploi.
3. **OBJECTIFS.** La présente politique a pour objectif d'établir la procédure à suivre en d'incident de confidentialité.
4. **OBLIGATIONS DU RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS.** Le *Responsable de la protection des renseignements personnels* doit veiller au respect et de la mise en œuvre de la législation concernant l'accès, la collecte, la conservation, la diffusion et, éventuellement, la destruction des renseignements personnels confiés à Broccolini.
5. **PROCÉDURE À SUIVRE.** La procédure suivante sera appliquée en cas de survenance d'un incident de confidentialité :
 - (1) **Signalement.** Si un membre du personnel de Broccolini a des raisons de croire qu'un incident de confidentialité s'est produit, il doit immédiatement aviser son supérieur ou le *Responsable de la protection des renseignements personnels* (le « **Responsable** »);
 - (2) **Collecte d'informations et évaluation de la situation.** Il importe notamment de déterminer si nous sommes en présence d'un incident de confidentialité et, le cas échéant, d'établir les circonstances de l'incident, cibler les renseignements personnels concernés ainsi que les personnes visées et identifier le problème.

(3) **Diminution des risques, mesures correctives et cessation de l'incident.** Si possible, l'incident doit être mis à terme. À défaut des mesures de mitigation immédiates doivent être prises en tenant compte, notamment, des facteurs suivants: sensibilité des renseignements visés, les effets appréhendés de la divulgation ou de l'utilisation de tels renseignements et la probabilité de conséquences préjudiciables.

(4) **Inscription de l'incident au Registre des incidents** Le *Responsable de la protection des renseignements personnels* doit également veiller à la tenue du registre des incidents de confidentialité. Les renseignements contenus au registre doivent être tenus à jour et conservés pendant une période minimale de 5 ans après la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident. Le Registre doit contenir :

- une description des renseignements personnels visés par l'incident;
- une brève description des circonstances de l'incident;
- la date ou la période où l'incident a eu lieu;
- la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;
- le nombre de personnes concernées par l'incident;
- une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;
- si l'incident présente un risque qu'un préjudice sérieux soit causé, les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées;
- une brève description des mesures prises par l'organisation, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.

(5) **Avis au Comité d'accès à l'information.** Lorsque l'incident présente le risque qu'un préjudice sérieux soit causé, le *Responsable de la protection des renseignements personnels* doit aviser le Comité d'accès à l'information (« CAI ») de la survenance de l'incident. **Voir Formulaire de déclaration de la CAI en annexe.** L'avis au CAI doit contenir les informations suivantes :

- le nom de l'organisation ayant fait l'objet de l'incident de confidentialité et le numéro d'entreprise du Québec;
- le nom et les coordonnées du *Responsable de la protection des renseignements personnels*;
- description des renseignements personnels visés par l'incident;
- brève description des circonstances de l'incident;
- la date ou la période où l'incident a eu lieu;
- la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;
- le nombre de personnes concernées par l'incident;
- une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;

- les mesures que l'organisation a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident;
- les mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident.

(6) **Avis à la personne dont un renseignement personnel est concerné par l'incident.** Lorsque l'incident présente le risque qu'un préjudice sérieux soit causé, , le *Responsable de la protection des renseignements personnels* doit aviser les personnes visées par l'incident. L'avis doit contenir les informations suivantes :

- description des renseignements personnels visés par l'incident;
- brève description des circonstances de l'incident;
- date ou la période où l'incident a eu lieu;
- brève description des mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident.
- les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;
- les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

6. MISE À JOUR DE LA PRÉSENTE POLITIQUE. Nous pourrions modifier et mettre à jour notre politique de protection des renseignements personnels lorsque requis. Nous vous encourageons à consulter la présente page pour vous familiariser avec ces changements.

7. CONTACTEZ-NOUS. Si vous avez des questions au sujet de la présente politique ou si vous souhaitez demander l'accès aux renseignements personnels que nous avons recueillis à votre sujet, veuillez communiquer avec nous à l'adresse suivante :

Responsable de la protection des renseignements personnels (Privacy Officer)

Kristen Bruno

16766 rte Trans-Canada, bureau 500

Kirkland, Québec, H9H 4M7

vieprivee@broccolini.com

privacyofficer@broccolini.com