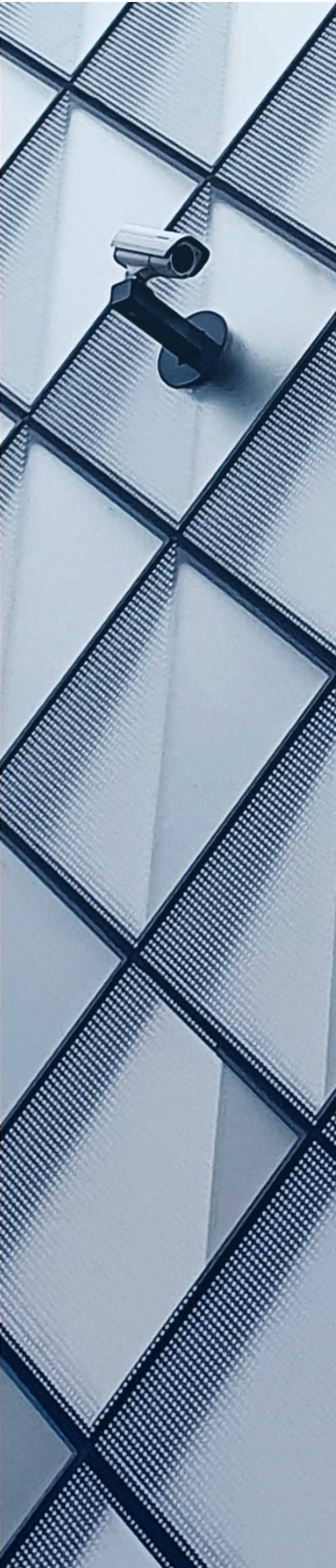




Loi 25

Protection des renseignements personnels

Aide mémoire

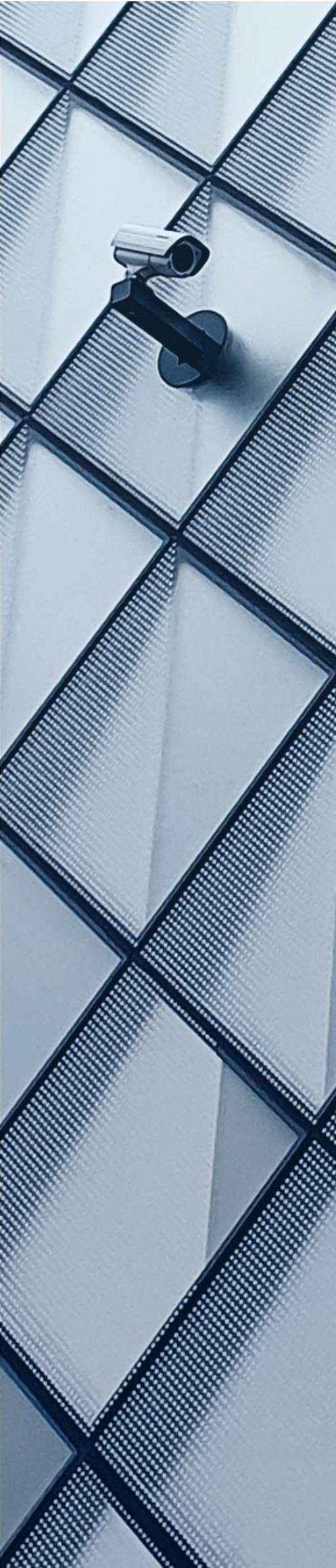


Protection des renseignements personnels : de nouvelles obligations sont arrivées et d'autres s'en viennent

Les entreprises évoluent dorénavant dans un contexte technologique en constante évolution. L'information est source de savoir et les renseignements que nous transmettons dans le cadre d'activités commerciales quotidiennes exposent plus que jamais les entreprises à des enjeux de sécurité, des risques réputationnels et des sanctions pénales sévères en cas de non-conformité.

Selon les fonctions que vous occupez au sein de votre entreprise, vous serez assurément appelés à participer à des discussions entourant la protection des renseignements personnels (« **RP** ») détenues par votre entreprise.

L'équipe de protection des données et vie privée de BCF peut vous accompagner vers une mise en conformité et vous outiller dans l'opérationnalisation des changements imposés en raison de l'entrée en vigueur de la Loi C-25 (Projet de Loi 64), qui encadre la protection et le traitement des RP.



Des sanctions pour vous aider à vous conformer...

SANCTIONS ADMINISTRATIVES PÉCUNIAIRES

SAP pouvant aller jusqu'à **10 millions \$** ou **2 %**
du chiffre d'affaires mondial de l'exercice financier précédent
(le plus élevé de)

SANCTIONS PÉNALES

Amendes pouvant aller jusqu'à **25 millions \$** ou **4 %**
du chiffre d'affaires mondial de l'exercice financier précédent
(le plus élevé de)

Un petit rappel

UN RENSEIGNEMENT PERSONNEL C'EST QUOI?

Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet directement ou indirectement de l'identifier. Trois critères permettent de déterminer ce qu'est un renseignement personnel. Il doit s'agir d'un renseignement qui fait connaître quelque chose sur une personne physique et qui permet de l'identifier. Si une seule information peut paraître anodine, elle peut, quand elle est combinée à d'autres, permettre d'identifier une personne physique. Dans ce contexte, ces informations constituent des renseignements personnels.

Quand?

SANCTIONS ADMINISTRATIVES PÉCUNIAIRES

- 22 septembre 2022 (ex.: Désignation du responsable et avis d'incidents de confidentialité et registre des incidents de confidentialité);
- 22 septembre 2023 juste la grande majorité des modifications et
- 22 septembre 2024 (droit à la portabilité des RP).

Par où commencer ?

1. Identification du responsable de la protection des renseignements personnels

Pour indiquer son titre et ses coordonnées sur le site Internet de l'entreprise et prévoir, le cas échéant, une délégation écrite de cette fonction par la personne ayant la plus haute autorité dans l'entreprise.

2. Création d'un registre des incidents de confidentialité

Pour y inscrire tout incident de confidentialité survenu depuis le 22 septembre 2022 ainsi que ceux à venir et être en mesure de communiquer sur demande ce registre à la Commission d'accès à l'information.

3. Création d'un registre de traitement des renseignements personnels

Pour identifier les renseignements personnels recueillis et comprendre leurs cycles de vie afin de permettre l'élaboration de vos politiques et pratiques en matière de protection des renseignements personnels.

4. Élaboration de vos politiques et pratiques relatives à la protection des renseignements personnels

Pour publier sur votre site Internet des informations détaillées, en termes simples et clairs, relatives à vos politiques et pratiques encadrant la gouvernance des renseignements personnels (conservation et destruction des renseignements personnels, rôles et responsabilités des employés, processus de traitement des plaintes, etc.).

Pour obtenir le consentement des personnes concernées à la collecte, l'utilisation et la divulgation de leurs renseignements personnels.

5. Identification et Maîtrise des technologies

Pour informer les individus sur les traitements entièrement automatisés de prises de décisions afin qu'ils sachent les raisons ainsi que les principaux facteurs et paramètres ayant mené à la décision.

Pour s'assurer que les paramètres des produits ou services technologiques qui recueillent des renseignements personnels offrent le plus haut niveau de confidentialité, sans aucune intervention de l'utilisateur.

Pour s'assurer que toute fonctionnalité d'une technologie permettant d'identifier, de localiser ou d'effectuer du profilage, soit désactivée par défaut.

Pour s'assurer de divulguer à la Commission d'accès à l'information la création d'une banque de caractéristiques ou de mesures biométriques et d'obtenir le consentement exprès de la personne concernée à l'utilisation de mesures d'identification ayant recours à la biométrie.

... Suite

Par où commencer ?

6. Établissement d'un programme de formation des employés

Pour faire vivre vos politiques et pratiques en matière de protection des renseignements personnels, les employés doivent les connaître et comprendre les enjeux que pose le traitement des renseignements personnels par l'entreprise.

7. Création d'un registre des incidents de confidentialité

Pour s'assurer que les fournisseurs et sous-traitants de l'entreprise sont eux aussi conformes aux lois relatives à la protection des renseignements personnels puisque l'entreprise est responsable de leurs manquements. Une bonne pratique sera de :

- A. vérifier s'ils ont identifié un responsable de la protection des renseignements personnels;
- B. analyser leurs politiques de protection des renseignements personnels;
- C. obtenir le lieu où ils traitent les renseignements personnels transmis par l'entreprise;
- D. obtenir les informations relatives aux mesures de sécurité de leurs systèmes informatiques assurant la sécurité des renseignements personnels transmis;
- E. obtenir l'identité de leurs propres sous-traitants à qui ils transmettent les renseignements personnels ainsi que les informations mentionnées en a), b), c) et d) ci-devant au sujet de leurs sous-traitants.

8. Rédaction de modèles de contrats de traitements de renseignements personnels

Pour encadrer le traitement des renseignements personnels entre l'entreprise qui transmet les renseignements personnels et celle qui les traite pour le compte de l'autre. Ces contrats devraient définir l'objet et la durée du traitement, la nature et la finalité du traitement, le type de renseignements personnels et les catégories de personnes concernées, ainsi que les obligations et les droits des parties encadrant ce traitement. Ce contrat devra notamment inclure des mesures afin d'assurer le caractère confidentiel des renseignements personnels, que les renseignements personnels communiqués ne soient pas utilisés pour d'autres fins que l'exécution du contrat principal entre les parties qui requiert le traitement de renseignements personnels, que les renseignements personnels ne soient pas conservés par le sous-traitant après l'exécution du contrat et que le client puisse vérifier le respect des engagements pris en vertu du contrat. Si les renseignements personnels sont transférés à un sous-traitant hors du Québec ou que ce dernier les transfère à son tour à l'extérieur du Québec, une évaluation des facteurs relatifs à la vie privée devra être effectuée et des dispositions particulières devront être insérées à ce contrat.

... Suite

Par où commencer ?

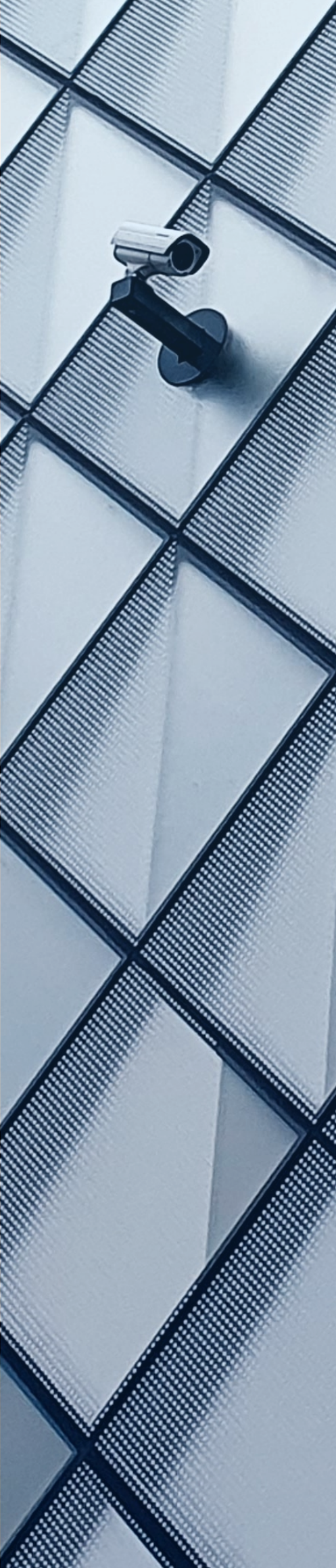
9. Conservation et traitement de l'information de façon à respecter les droits d'une personne concernée

Pour faciliter la réponse aux demandes des personnes concernées dans l'exercice de leurs droits à l'égard de leurs renseignements personnels. Dans le cas où une personne concernée s'interroge sur la manière dont l'entreprise traite ou a traité ses renseignements personnels, ceux-ci doivent être facilement localisables et retraçables. L'entreprise doit être en mesure de répondre à ces demandes rapidement tout en respectant les lois applicables. À compter du 22 septembre 2024, elle devra être en mesure de fournir les renseignements personnels qu'elle a colligés électroniquement dans un format technologique structuré et couramment utilisé à la personne concernée et à tout tiers à sa demande. L'entreprise devra donc posséder un système informatique qui permettra d'effectuer rapidement et simplement ces tâches. Elle devra aussi s'assurer que la sécurité de ses systèmes soit en tout temps à la dernière norme utilisée dans son industrie.

10. Réalisation d'évaluations des facteurs relatifs à la vie privée

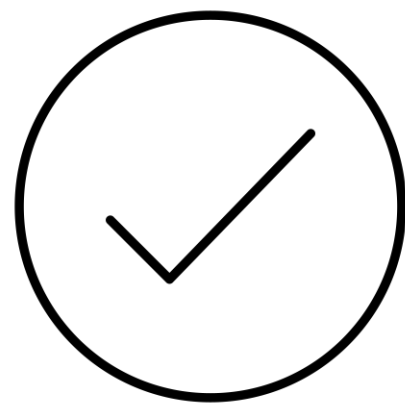
Pour évaluer si le traitement de renseignements personnels par l'entreprise peut se faire en toute légalité, sans encourir de risques trop importants pour les personnes concernées. L'évaluation des facteurs relatifs à la vie privée (l'« EFVP ») est un nouvel outil qui se retrouvera au cœur de la plupart des activités de l'entreprise qui impliquera des renseignements personnels. Il sera donc important de le maîtriser. Essentiellement, une EFVP permet aux entreprises d'évaluer, de pondérer et de mitiger, le cas échéant, les risques liés à la protection des renseignements personnels dans le cadre de leurs activités. L'EFVP permet également d'assurer la mise en place de mesures adéquates afin de protéger les renseignements personnels (par exemple, l'obtention des consentements appropriés, la conclusion d'ententes de confidentialité, l'utilisation de renseignements dépersonnalisés seulement). Plus spécifiquement, une EFVP est requise :

- A. pour tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels (par exemple, le développement d'un algorithme, le recours à l'intelligence artificielle, la conception d'une nouvelle interface pour les clients, le lancement d'une campagne publicitaire, la sous-traitance en mode infonuagique). Mentionnons toutefois que cette exigence n'est pas rétroactive et s'applique uniquement aux nouveaux projets mis en œuvre après le 22 septembre 2023; et
- B. avant de communiquer un renseignement personnel à l'extérieur du Québec. Cela signifie qu'une EFVP est nécessaire dans tous les cas où les renseignements personnels sont conservés ou peuvent être accédés à l'extérieur du Québec par un sous-traitant ou un partenaire, par exemple. L'évaluation devra d'ailleurs tenir compte du régime juridique applicable dans l'État où les renseignements seront communiqués. Une attention particulière devra être apportée aux transferts aux États-Unis.



Principales obligations à considérer

Protection des renseignements personnels :
de nouvelles obligations sont arrivées et
d'autres s'en viennent



Désignation d'un responsable
à l'interne ou à l'externe

Mise en œuvre de politiques et pratiques de protection des RP
à publier sur le site Web

EFVP pour nouveaux systèmes et services impliquants des RP
Évaluation des facteurs relatifs à la vie privée

Gestion des incidents de confidentialité
Avis si risque de préjudice sérieux; et registre

Protection de la vie privée par défaut
Dénonciation des technologies d'identification, localisation ou profilage et opt-in; Opt-in pour les paramètres de confidentialité des produits/ services technologiques

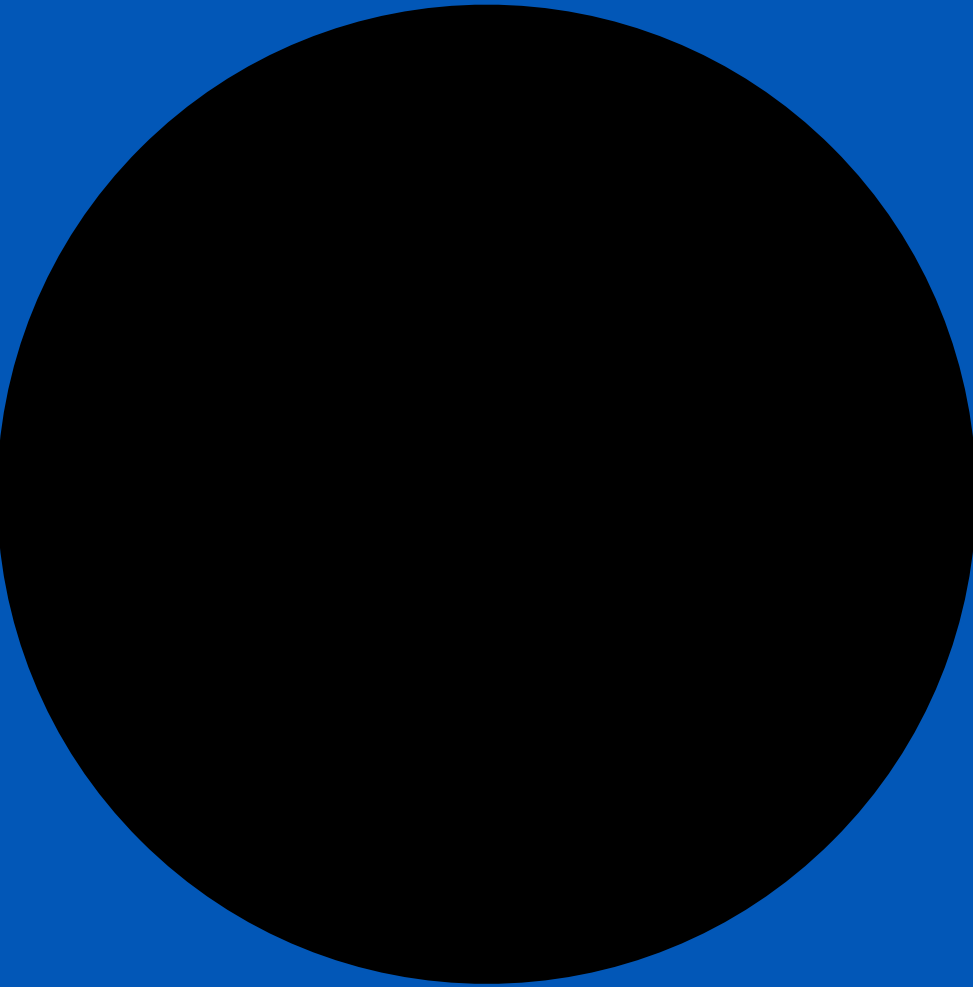
Information sur les décisions entièrement automatisées
au plus tard au moment de la décision

Destruction ou anonymisation des RP
lorsque les finalités sont accomplies

Portabilité des RP
pour RP recueillis de manière informatisée – communication dans un format technologique structuré et couramment utilisé

Droit à l'oubli
arrêt de diffusion et désindexation

Responsabilité
chaque entreprise est responsable des RP qu'elle détient



BCF, Avocats d'affaires
1100, boul. René-Lévesque O.
25e étage
Montréal (Québec) H3B 5C9
T. 514 397-8500
F. 514 397-8515

BCF, Avocats d'affaires
Complexe Jules-Dallaire, T1
2828, boul. Laurier, 12e étage
Québec (Québec) G1V 0B9
T. 418 266-4500
F. 418 266-4515

BCF Global
75, rue de Tocqueville 75017 Paris,
France

T. +33 (0)1 44 17 14 14
F. +33 (0)1 44 17 98 99