

Objectif

La protection de la vie privée et de la confidentialité des informations personnelles est un aspect important de la manière dont le groupe de sociétés Bailey "Bailey" mène ses activités. La collecte, l'utilisation et la divulgation d'informations personnelles de manière appropriée, responsable et éthique sont fondamentales pour les activités de l'entreprise.

Champ d'application

Cette politique a pour but de décrire les lignes directrices visant à protéger de façon appropriée la vie privée et les renseignements personnels de nos associés, clients, fournisseurs et de toute personne qui fait affaire avec Bailey dans la province de Québec.

Définitions

Collaborateur : toute personne employée par le groupe de sociétés Bailey.

Incident de confidentialité : Tout accès, utilisation, communication ou perte d'informations personnelles non autorisé par la loi, ou toute autre violation de la protection de ces informations.

Dé-identification : S'assurer que l'individu dont les informations personnelles sont en question ne peut plus être directement identifié par ces informations.

Informations personnelles : Toute information se rapportant à une personne physique et permettant d'identifier cette personne.

Profilage : La collecte et l'utilisation d'informations personnelles pour évaluer certaines caractéristiques d'une personne physique, dans le but d'analyser ses performances professionnelles, sa situation économique, sa santé, ses préférences personnelles, ses intérêts ou son comportement.

Informations sensibles : Informations personnelles qui, en raison de leur nature, notamment médicale, biométrique ou autrement intime, ou du contexte de leur utilisation ou de leur communication, suscitent des attentes raisonnables élevées en matière de respect de la vie privée.

Lignes directrices

L'entreprise s'efforce de protéger et de respecter les renseignements personnels de ses clients, associés, partenaires commerciaux et autres, conformément à toutes les exigences légales applicables. Tous les associés doivent respecter les procédures et les pratiques énoncées dans la présente politique lorsqu'ils traitent des renseignements personnels, conformément à la Loi sur la protection des renseignements personnels dans le secteur privé (la Loi) et au Code civil.

Chez Bailey, le responsable de la protection de la vie privée est Sergio Di Fruscia. Il est chargé de veiller à ce que l'entreprise reste conforme à la loi et à ce que les renseignements personnels soient traités de manière appropriée. Toute personne

chargée d'utiliser les informations personnelles d'une autre personne doit le faire conformément à cette politique et à la loi.

Lorsque l'entreprise recueille des informations personnelles pour des raisons sérieuses et légitimes, elle détermine et énonce explicitement l'objectif de cette collecte avant de la réaliser. L'entreprise ne recueillera que la quantité d'informations personnelles nécessaire pour atteindre l'objectif déclaré, et toutes les informations personnelles ne seront utilisées que pour l'objectif déclaré de leur collecte. La source de toutes les informations personnelles collectées sera toujours communiquée à la personne concernée.

Lors de la collecte d'informations personnelles, l'entreprise informera l'associé de l'objectif déclaré de la collecte des informations, de l'endroit où elles sont conservées et des personnes qui y auront accès, ainsi que de son droit d'accéder à ces informations ou de les rectifier, et de son droit de retirer à tout moment son consentement à l'utilisation de ces informations.

Si une technologie est utilisée pour collecter des informations, cette technologie est clairement décrite à toute personne dont les informations personnelles sont collectées de cette manière. En outre, toute personne dont les informations sont collectées à l'aide de la technologie est informée des moyens disponibles pour l'identifier, la localiser ou la profiler à l'aide de la technologie.

Bailey peut utiliser des outils d'intelligence artificielle pour ses activités internes. Bailey prend des mesures pour protéger la confidentialité des informations saisies dans les outils d'intelligence artificielle, notamment en supprimant les informations personnelles si nécessaire. Il est interdit aux associés d'entrer des informations confidentielles ou propriétaires dans les outils d'intelligence artificielle. Dans tous les cas, Bailey respecte toutes les législations provinciales applicables en matière de protection de la vie privée et la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE).

Les associés peuvent demander des détails sur toutes les informations personnelles détenues par l'entreprise à leur sujet et peuvent obtenir une copie de ces informations à tout moment. Des aménagements seront apportés chaque fois que nécessaire pour garantir l'égalité d'accès pour tous.

Aucune mesure de représailles ne sera prise à l'encontre d'une personne qui dépose de bonne foi une plainte auprès de la Commission d'accès à l'information (la Commission) ou qui coopère à une enquête, et la menace de représailles ne sera jamais utilisée comme tactique à l'encontre d'un associé. Les associés sont tenus de coopérer avec la Commission en ce qui concerne les ordres, les demandes et les enquêtes.

Consentement et rectification

Bailey s'assurera que le consentement des associés pour l'utilisation des informations personnelles est clair, libre et informé, et qu'il est donné à des fins spécifiques. Bailey demande le consentement pour chacun de ces objectifs, dans un langage clair et simple. Le consentement qui n'est pas donné conformément à cette politique et à la loi n'est pas considéré comme valide.

Les associés ou agents autorisés peuvent avoir accès aux informations personnelles sans le consentement de la personne concernée uniquement si les informations sont nécessaires à l'exercice de leurs fonctions. De même, l'entreprise peut communiquer des renseignements personnels sans le consentement de l'intéressé à son avocat si ces renseignements sont nécessaires à des poursuites criminelles et pénales, lorsque la situation présente un danger imminent, ou pour toute autre raison spécifiquement requise par la Loi.

L'entreprise peut utiliser des informations personnelles pour des raisons autres que l'objectif déclaré de leur utilisation sans le consentement de la personne concernée si le nouvel objectif constitue un moyen clair et évident d'atteindre l'objectif déclaré, si son utilisation profite clairement à la personne, si son utilisation est nécessaire pour prévenir ou détecter la fraude ou évaluer et améliorer la sécurité, si son utilisation est nécessaire pour fournir un service ou livrer les biens demandés par la personne, ou si les informations personnelles sont dépersonnalisées de manière adéquate et utilisées ensuite à des fins statistiques. Lors de l'utilisation d'informations dépersonnalisées, l'entreprise est tenue de s'assurer que la personne concernée ne peut être identifiée par ces informations.

Les associés ont le droit de demander que leurs informations personnelles soient rectifiées si elles sont inexactes, incomplètes ou équivoques, ou si leur collecte, leur communication ou leur conservation n'est pas autorisée par la loi. Les associés peuvent à tout moment annuler leur consentement à l'utilisation ou à la communication de leurs informations personnelles.

Les demandes d'accès aux informations personnelles ou de rectification doivent être soumises par écrit au responsable de la protection de la vie privée. Toutes ces demandes recevront une réponse écrite dans un délai de 30 jours. Si la réponse indique un refus d'accès ou de rectification des informations personnelles, le responsable de la protection de la vie privée en donnera les raisons, y compris les éventuelles dispositions légales, et les autres recours possibles.

Sécurisation, conservation et destruction des informations personnelles

Bailey prend toutes les mesures de sécurité nécessaires pour garantir que la protection des informations personnelles collectées, utilisées, communiquées, conservées ou détruites est raisonnable :

- la sensibilité de l'information
- Les objectifs pour lesquels elles doivent être utilisées ;
- de la quantité et de la répartition des informations ; et
- du support sur lequel elles sont stockées.

En général, les bases de données et autres moyens numériques contenant des informations personnelles seront protégés par un mot de passe, et les copies papier des documents contenant des informations personnelles seront conservées sous clé, au minimum. Le contrôle de l'efficacité et de la mise en œuvre de ces pratiques de protection incombe au spécialiste de la paie et des avantages sociaux et au responsable de la protection de la vie privée. Toute plainte concernant la protection des données personnelles doit être adressée au spécialiste de la paie et des avantages sociaux ou au responsable de la protection de la vie privée.

Tous les dossiers contenant des informations personnelles sont tenus à jour et exacts, en particulier lorsqu'ils sont utilisés pour prendre des décisions relatives aux associés. L'entreprise ne communiquera pas d'informations personnelles à un tiers sans son consentement, à moins qu'une exception législative spécifique ne s'applique.

Toutes les informations personnelles collectées et utilisées par l'entreprise sont conservées pendant un maximum de sept (7) ans après leur utilisation appropriée et consentie. À la fin de la période de conservation, les informations personnelles seront définitivement détruites ou rendues anonymes. Les informations personnelles sont considérées comme adéquatement détruites ou anonymisées s'il est raisonnablement prévisible que la personne ne peut plus être identifiée directement ou indirectement par les informations, et que la destruction ou l'anonymisation est effectuée de manière irréversible. Le spécialiste de la paie et des avantages sociaux est chargé de veiller à ce que les informations personnelles devant être détruites ou rendues anonymes soient complétées comme il se doit et conformément à la législation en vigueur.

Évaluations de l'impact sur la vie privée

Des évaluations des facteurs relatifs à la vie privée sont effectuées chaque fois qu'un projet nécessite l'acquisition, le développement ou la révision d'un système d'information ou d'un système de livraison électronique qui implique la collecte, l'utilisation, la communication, le stockage ou la destruction de renseignements personnels, ou lorsque l'entreprise a l'intention de communiquer des renseignements personnels à l'extérieur du Québec. Le responsable de la protection de la vie privée sera informé d'un tel projet avant le début des travaux. L'objectif de ces évaluations est de s'assurer que des mesures adéquates sont prises pour protéger les renseignements personnels au cours du projet, telles que la désignation d'une personne responsable de la mise en œuvre des mesures de protection, la mise en œuvre de nouvelles mesures de protection, la définition précise des responsabilités des participants au projet et l'assurance que la formation nécessaire est dispensée.

Lors des évaluations relatives à la communication d'informations à l'extérieur du Québec, le cadre juridique de la région à laquelle les informations sont communiquées est également pris en compte.

Incidents de confidentialité

Lorsqu'il estime qu'un incident de confidentialité a pu avoir lieu, le responsable de la protection de la vie privée prend des mesures pour réduire le risque de préjudice résultant de l'incident et pour empêcher que des incidents similaires ne se reproduisent.

Si l'incident présente un risque sérieux, le responsable de la protection de la vie privée contactera la Commission, ainsi que les personnes dont les données personnelles ont été impliquées dans l'incident de confidentialité. Toute communication avec des tiers visant à réduire le risque de l'incident sera documentée. Si le fait d'informer une personne concernée présente un risque supplémentaire pour l'enquête, la prévention, la détection ou la répression d'un crime ou d'un délit, cette personne ne sera pas informée de l'incident tant que le risque n'aura pas disparu.

Lorsqu'il évalue le risque de préjudice pour une personne à la suite d'un incident de confidentialité, le responsable de la protection de la vie privée tient compte de la



Politique de confidentialité - Québec

sensibilité des informations concernées, des conséquences prévues de leur utilisation et de la probabilité que les informations soient utilisées de manière inappropriée, afin de déterminer si les informations seront protégées de manière adéquate.

Le responsable de la protection de la vie privée tient un registre de tous les incidents de confidentialité qui se produisent et le transmet à la Commission sur demande.