BAILEY

Privacy Policy - Quebec

Purpose

Protecting the privacy and confidentiality of personal information is an important aspect of the way The Bailey Group of Companies “Bailey” conducts its business. Collecting, using, and disclosing personal information appropriately, responsibly, and ethically is fundamental to the company’s operations.

Scope

This policy is intended to describe the guidelines to appropriately protect the privacy and personal information of our associates, customers, vendors and any individuals who conduct business with Bailey in the province of Quebec.

Definitions

Associate: any individual employed by the Bailey Group of Companies

Confidentiality incident: Any access, use, communication, or loss of personal information not authorized by law, or any other breach of the protection of such information.

De-identifying: Ensuring the individual whose personal information is in question can no longer be directly identified by the personal information.

Personal information: Any information that relates to a natural person and allows that person to be identified.

Profiling: The collection and use of personal information to assess certain characteristics of a natural person, for the purpose of analysing that person’s work performance, economic situation, health, personal preferences, interests, or behaviour.

Sensitive information: Personal information that due to its nature, in particular its medical, biometric, or otherwise intimate nature, or the context of its use or communication, entails a high level of reasonable expectation of privacy.

Guidelines

The company strives to protect and respect personal information of its customers, associates, business partners, and others in accordance with all applicable statutory requirements. All associates must abide by the procedures and practices set out in this policy while handling personal information, in compliance with An *Act respecting the protection of personal information in the private sector* (the Act) and the *Civil Code*.

At Bailey, the designated privacy officer is Sergio Di Fruscia. They are responsible for ensuring the company remains compliant with the Act and personal information is handled appropriately. Any individual charged with the use of another individual’s personal information must do so in conformance with this policy and the Act.

When collecting personal information for serious and legitimate reasons, the company will determine and explicitly state the purpose for doing so before collecting it. The company will only collect as much personal information as is necessary to achieve the

stated purpose, and all personal information will only be used for the stated purpose of its collection. The source of all collected personal information will always be made known to the involved individual.

When collecting personal information, the company will inform the associate of the stated purpose of collecting the information, where it is kept and who will have access to it, and their right to access or rectify that information, as well as their right to withdraw consent for the information's use at any time.

If technology is used to collect information, that technology is clearly described to any individual whose personal information is collected in that manner. Additionally, anyone whose information is collected using technology is informed of the means available to identify, locate, or profile them using technology.

Bailey may use artificial intelligence tools for internal activities. Bailey takes steps to protect the confidentiality of information entered into artificial intelligence tools, including removing personal information as necessary. Associates are prohibited from entering confidential or proprietary information into artificial intelligence tools. In all instances, Bailey follows all applicable provincial privacy legislations and Personal Information Protection and Electronics Documents Act (PIPEDA).

Associates may request details on all personal information held by the company about them and may obtain a copy of that information at any time. Accommodation will be provided whenever necessary to ensure equal access for all.

No reprisal will be taken against anyone who files a complaint with the Commission d'accès à l'information (the Commission) in good faith or cooperates in an investigation, and threat of reprisal will never be used as a tactic against any associate. Associates are expected to cooperate with the Commission regarding any orders, demands, and investigations.

Consent and Rectification

Bailey will ensure associate consent for the use of personal information is clear, free, and informed, and given for specific purposes. Bailey requests consent for each such purpose, in clear and simple language. Consent that is not given in accordance with this policy and the Act is not considered valid.

Authorized associates or agents may have access to personal information without the consent of the person concerned only if the information is needed for the performance of their duties. Similarly, the company may communicate personal information without consent to their attorney if the information is required for criminal and penal prosecutions, whenever the situation is imminently dangerous, or any other reason specifically required by the Act.

The company may use personal information for reasons other than the stated purpose of its use without the associated individual's consent if the new purpose provides a clear and obvious means to achieving the stated purpose, if its use clearly benefits the individual, if its use is necessary for preventing or detecting fraud or assessing and improving security, if its use is necessary to provide a service or to deliver goods requested by the individual, or if the personal information is adequately de-identified and then used for statistical purposes. When using de-identified information, the

company is responsible for ensuring the involved individual cannot be identified by the information.

Associates have the right to require their personal information be rectified if it is inaccurate, incomplete, or equivocal, or if collecting, communicating, or keeping it is not authorized by law. Associates may rescind their consent to the use or communication of their personal information at any time.

Requests for access to personal information or rectification should be submitted in writing to the privacy officer. All such requests will be replied to in writing within 30 days. If the reply indicates a refusal to access or rectify personal information, the privacy officer will give reasons why this is the case, including any legal provisions, and available alternative remedies.

Securing, Retaining, and Destroying Personal Information

Bailey takes all security measures necessary to ensure that the protection of the personal information collected, used, communicated, kept, or destroyed are reasonable given:

- The sensitivity of the information;
- The purposes for which it is to be used;
- The quantity and distribution of the information; and
- The medium on which it is stored.

In general, databases and other digital means of containing personal information will be password protected, and hard copies of documents containing personal information will be kept under lock and key, at minimum. Monitoring the effectiveness and implementation of these safeguarding practices is the responsibility of the Payroll and Benefits Specialist and the privacy officer. Any complaints regarding the protection of personal information should be directed to the Payroll and Benefits Specialist or the privacy officer.

All files containing personal information are kept up to date and accurate, specifically when used to make any decisions related to associates. The company will not communicate personal information to a third party without consent unless a specific legislative exception applies.

All personal information collected and used by the company is retained for a maximum of seven (7) years after its appropriate and consented use. At the end of the retention period, the personal information will be permanently destroyed or anonymized. Personal information is considered adequately destroyed or anonymized if it is reasonably foreseeable that the person can no longer be identified directly or indirectly by the information, and the destruction or anonymization is done in an irreversible way. The Payroll and Benefits Specialist is responsible for ensuring personal information scheduled to be destroyed or anonymized is completed as required and in accordance with applicable legislation.

Privacy Impact Assessments

Privacy impact assessments are conducted whenever a project requires the acquisition, development, or overhaul of an information system or electronic delivery system that involves the collection, use, communication, storage, or destruction of

personal information, or when the company intends to communicate personal information outside of Quebec. The privacy officer will be made aware of any such project before any work takes place. The purpose of these assessments is to ensure adequate steps are taken to protect personal information during the project, such as appointing someone responsible for implementing protection measures, implementing new protection measures, specifically detailing project participants' related responsibilities, and to ensure any necessary training is provide.

When completing assessments relating to communicating information outside of Quebec, the legal framework of the region when the information is being communicated to is also considered.

Confidentiality Incidents

Whenever it is believed that a confidentiality incident may have taken place, the privacy officer will take steps to reduce the risk of harm resulting from the incident and to prevent similar incidents from happening in the future.

If the incident presents a serious risk, the privacy officer will contact the Commission, as well as the individuals whose personal information was involved in the confidentiality incident. Any communication with third parties to help reduce the risk of the incident will be documented. If informing an involved individual would present additional risk to any investigation, prevention, detection, or repression of a crime or statutory offence, they will not be informed of the incident until the risk is no longer present.

When assessing the risk of injury to a person after a confidentiality incident, the privacy officer considers the sensitivity of the information concerned, any anticipated consequences of it use, and the likelihood the information will be used inappropriately to determine whether the information will be adequately protected.

The privacy officer will keep a register of all confidentiality incidents that occur and will send it to the Commission upon request.