



NATECH

BATTERIES

Politique de confidentialité

TABLE DES MATIÈRES

1. CONTEXTE.....	3
2. RESPONSABILITÉ.....	3
3. RAISONS DE LA COLLECTE DES RENSEIGNEMENTS PERSONNELS	3
4. CONSENTEMENT	3
5. LIMITES ET MOYENS DE LA COLLECTE	3
6. LIMITE DE L'UTILISATION ET DE LA COMMUNICATION DES RP	4
7. EXACTITUDE DES RENSEIGNEMENTS PERSONNELS DÉTENUS.....	4
8. MESURES DE SÉCURITÉ	4
9. TRANSPARENCE	4
10. ACCÈS AUX RENSEIGNEMENTS PERSONNELS DÉTENUS	5
11. PROCESSUS DE TRAITEMENT DES PLAINTES	5
12. MISE À JOUR DE LA POLITIQUE.....	6
13. MESSAGE DE COMMUNICATION INTERNE.....	6

1. Contexte

- a. Batteries Natech (BN) a été créée en 2003 et fait l'assemblage, la vente et la réparation de batteries industrielles. BN est située à Saint-Jean-sur-Richelieu et emploie une trentaine d'employés annuellement.
- b. BN fait affaire avec d'autres entreprises et ne vend pas directement aux consommateurs.
- c. BN doit utiliser des renseignements personnels (RP) pour identifier, contacter et payer (Paie) ses employés.

2. Responsabilité

- a. BN a la responsabilité de protéger les RP obtenus pour des fins liées à ses opérations en tant que personne morale faisant affaire au Québec et au Canada.
- b. Dans le but de se conformer aux exigences de la loi 25, un responsable de la protection des renseignements personnels a été nommé, une Politique de confidentialité a été publiée sur son site web et des Politiques et pratiques de gouvernance à l'égard des renseignements personnels ont été mises en place, afin d'assurer que les rôles et responsabilités en matière de protection des renseignements personnels, notamment en ce qui concerne leur collecte, leur utilisation, leur communication, leur conservation et leur destruction, sont bien définis et clairs.

3. Raisons de la collecte des renseignements personnels

- a. Pour identifier et contacter les employés actuels, passés et futurs.
- b. Pour préparer les paies et les documents fiscaux requis par les gouvernements locaux
- c. Pour contacter les employés et/ou leur famille en cas d'urgence ou pour les aviser au besoin.
- d. Pour garder en dossier les problèmes de santé ou de blessures au travail (SST).
- e. Pour confirmer si les antécédents criminels de nos employés peuvent leur restreindre accès chez nos clients pour des visites de réparations ou d'entretien.
- f. Pour fins fiscales des données financières peuvent être communiquées aux comptables externes sur la base d'une plateforme sécurisée.

4. Consentement

- a. À l'embauche des nouveaux employés, un formulaire de consentement sera signé par ces derniers.
- b. Ce formulaire détaillera les types de renseignements personnels demandés par BN, les fins pour lesquels ils sont collectés, les tiers à qui ils pourraient être communiqués, la durée pour laquelle les renseignements seront conservés, ainsi que les modalités concernant les droits d'accès et de rectifications ou le droit de retirer leur consentement.
- c. Pour les employés actifs, un nouveau formulaire leur sera présenté pour signature au moment de la présentation de la Politique de confidentialité ainsi que de certains détails supplémentaires comme le formulaire de plaintes.

5. Limites et moyens de la collecte

- a. La collecte se limite aux données requises pour la paie, l'identification, les contacts d'urgence, les informations santé et sécurité, les antécédents criminels ou tout autre renseignement qui pourrait être directement utile aux fins mentionnées au point #3, dans les limites permises par la loi.
- b. Une partie des renseignements personnels sont collectés avant l'embauche, lors de la réception du Curriculum Vitae, soit à travers la plateforme *Indeed*, par la poste, par courriel, par l'entremise d'un chasseur de tête ou directement en main propre.
- c. La majorité des renseignements est par la suite collectée de vive voix et via un formulaire papier lors du processus d'embauche.

6. Limite de l'utilisation et de la communication des RP

- a. Les RP seront uniquement utilisés pour les besoins/raisons identifiés au point #3.
- b. La communication à des tiers de ces RP sera limitée aux cas suivants :
 - i. RP hébergés dans le service externe de paie
 - ii. RP hébergés hors Québec dans l'infrastructure de Microsoft
 - iii. RP SST communiqués sur demande à la CNESST par les canaux de communications approuvés par cette dernière
 - iv. RP communiqués à des organismes gouvernementaux selon les exigences de la loi par les canaux de communications approuvés par ceux-ci
 - v. Les RP concernant les antécédents criminels ne sont pas communiqués aux clients de BN, mais le résultat positif (antécédents criminels identifiés) ou négatif (antécédents criminels non identifiés) pourrait être communiqué aux clients de BN au besoin.
 - vi. Pour fins fiscales, des RP peuvent être communiqués aux comptables externes via l'utilisation des formulaires gouvernementaux T4 et R1 et par l'utilisation d'une plateforme sécurisée avec double authentification.
 - vii. Toutes autres communications ne nécessitant pas le consentement de la personne concernée et permises par la loi.

7. Exactitude des renseignements personnels détenus

- a. Les RP détenus et utilisés par BN peuvent être mis à jour par l'employé (e.g. : changement d'adresse) ou sur demande de l'employeur lorsque la situation le suggère.
- b. BN s'engage à mettre à jour et à maintenir l'intégrité des renseignements personnels détenus par des efforts raisonnables.

8. Mesures de sécurité

- a. Les RP sont protégés par les mesures suivantes :
 - i. Documents physiques dans des classeurs sous clés dans un bureau verrouillé.
 - ii. Toutes les plateformes informatiques hébergeant des RP ne sont accessibles que par des comptes sécurisés par une authentification à double facteurs
 - iii. Les procédures et politiques se trouvant dans les documents suivants :
 - iv. Politique de confidentialité
 - v. Politiques et pratiques de gouvernance concernant les renseignements personnels
 - vi. Les RP ne seront pas manipulés par d'autres employés de BN que ceux initialement autorisés ou par des professionnels de la destruction de documents.

9. Transparence

- a. BN s'engage à mettre à la disposition des personnes concernées toute l'information concernant sa *Politique de confidentialité* et ses *Politiques et pratiques de gouvernance à l'égard des renseignements personnels* lors de la collecte des renseignements personnels (entre autres via le formulaire de consentement à la collecte mentionné au point #4 et via son site web)
- b. BN s'engage également à répondre à toute demande d'information soumise par écrit au RRP, notamment en ce qui concerne les renseignements personnels recueillis auprès d'elle, les catégories de personnes qui ont accès à ces renseignements au sein de l'organisation et la durée de conservation de ces RP.

10. Accès aux renseignements personnels détenus

- a. L'accès aux RP protégés détenus par BN ne sera possible que pour le responsable des RP (RRP), la haute direction de l'entreprise et dans certains cas le superviseur direct de l'employé concerné.
- b. Si des demandes d'accès à certaines informations contenues dans les RP sont faites à BN, le RRP devra s'assurer que ces demandes sont basées sur les possibilités déjà énumérées dans cette politique. Toutes autres demandes devront être analysées et/ou communiquées aux employés pour obtenir leur consentement.

11. Processus de traitement des plaintes

- a. Un formulaire de plainte sera préparé et présenté aux employés
- b. Une plainte peut résulter d'un incident de confidentialité ou simplement du doute qu'un tel incident se soit passé ou risque de se passer.
- c. Les incidents de confidentialité peuvent avoir produit un préjudice, un risque de préjudice ou peuvent ne pas engendrer de préjudice.
- d. Un préjudice se définit comme 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 conduire, par exemple :
 - ✓ À l'humiliation
 - ✓ À une atteinte à la réputation
 - ✓ À une perte financière
 - ✓ À un vol d'identité
 - ✓ À des conséquences négatives sur un dossier de crédit
 - ✓ À une perte d'emploi.
- e. Un incident de confidentialité se définit comme étant un accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection. Par exemple :
 - ✓ Un membre du personnel qui consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions en outrepassant les droits d'accès qui lui ont été consentis, ou un pirate informatique qui s'infiltre dans un système.
 - ✓ Un membre du personnel qui utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne.
 - ✓ Une communication faite par erreur à la mauvaise personne par son employeur.
 - ✓ Une personne qui perd ou se fait voler des documents contenant des renseignements personnels.
 - ✓ Une personne qui s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer.

12. Mise à jour de la politique

- a. La politique sera mise à jour aux 5 ans.
- b. Prochaine mise à jour : 2030

13. Message de communication interne

- a. Une communication à tous les employés sera faite pour annoncer l'implantation de cette politique de confidentialité et la conformité à la loi 25.
- b. Cette communication aura lieu avant le 31 janvier 2025.
- c. Tous changements à la politique de confidentialité devront être communiqués aux employés par le RRP.

