

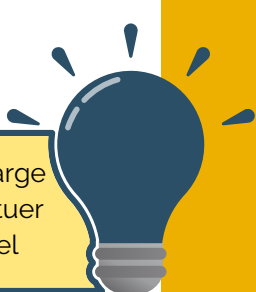
**CDC**Corporation de développement
communautaire de la MRC
de Bécancour

LOI 25 | AIDE-MÉMOIRE POUR LES ORGANISMES COMMUNAUTAIRES

DÉFINITION

«Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier.»

La loi n'exige pas que les renseignements soient intimement liés à l'individu et la loi s'applique peu importe la nature et la forme du support sous lequel ils ont été recueillis et qui sont désormais accessibles (écrite, graphique, sonore, visuelle ou informatisée)



Une note manuscrite en marge d'un document peut constituer un renseignement personnel

TYPES DE RENSEIGNEMENTS PERSONNELS

Renseignement anonymisé : Renseignement qui ne permet plus d'identifier directement ou indirectement une personne de manière irréversible. **Renseignement dépersonnalisé** : Renseignement qui ne permet plus d'identifier directement la personne concernée.

Renseignement personnel sensible : Renseignement qui a un haut degré d'attente en matière de respect à la vie privée (selon une personne raisonnable).

PORTABILITÉ

La portabilité des renseignements personnels permet à toute personne d'obtenir la communication, dans un format technologique structuré et couramment utilisé, des renseignements personnels informatisés qu'elle a fourni à une entreprise.

CONSENTEMENT

Pour qu'un consentement de collecte de renseignements personnels soit valide, il doit être manifeste, spécifique, libre et éclairé.

Le consentement relatif à l'utilisation d'un renseignement personnel doit être demandé pour chacune des fins auxquelles il est recueilli.

Le renseignement peut être utilisé à des fins autres à condition que l'organisme obtienne un nouveau consentement de la personne concernée. S'il s'agit d'un renseignement sensible, le consentement doit être exprès : donné par écrit ou de vive voix



OBLIGATIONS ENTRÉES EN VIGUEUR LE 22 SEPTEMBRE 2022

- Obligation de désigner une personne responsable de la protection des renseignements personnels et de publier ses coordonnées (habituellement la personne ayant la plus haute autorité);
 - Obligations en cas d'incident impliquant un renseignement personnel :
 - Tenir un registre des incidents de confidentialité;
 - Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé;
 - Aviser la personne concernée et la Commission d'accès à l'information dans le cas où l'incident présente un risque de préjudice sérieux.

Exemples d'incident de confidentialité :

- *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 consenti.*
 - *Un pirate informatique qui s'infiltré 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.*
 - *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.*
-
- Obligation de procéder à une évaluation des facteurs relatifs à la vie privée (EFVP) avant de communiquer des renseignements personnels sans le consentement des personnes concernées à des fins d'étude, de recherche ou de production de statistiques.

OBLIGATIONS ENTRANT EN VIGUEUR LE 22 SEPTEMBRE 2023

- Obligation de mise en œuvre des politiques et des pratiques de gouvernance (inventaire des renseignements personnels à jour et évaluation de leur sensibilité) concernant les renseignements personnels et publication sur le site web en termes clairs et simples;
- Obligation de transparence dans la collecte et l'utilisation des renseignements personnels;
- Obligation de détruire ou d'anonymiser les renseignements personnels lorsque les fins auxquelles ils ont été recueillis sont accomplies.
- Obligation de procéder à une évaluation des facteurs relatifs à la vie privée (EFVP) lors de **tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels** et avant de communiquer un renseignement personnel à l'extérieur du Québec.
 - L'EFVP consiste à protéger et respecter davantage la vie privée et considérer tous les facteurs qui auraient des impacts positifs et/ou négatifs sur les renseignements personnels. Pour en savoir plus sur l'EFVP :

<https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/evaluation-facteurs-relatifs-vie-privee>



OBLIGATIONS ENTRANT EN VIGUEUR LE 22 SEPTEMBRE 2024

Obligation de communiquer un renseignement personnel informatisé dans un format technologique couramment utilisé : droit à la portabilité.

Droits de la personnes concernée par le renseignement personnel :

- Droit d'accès et à la portabilité;
 - Un organisme **doit refuser** de communiquer un renseignement personnel à la personne concernée lorsque sa divulgation : révélerait un renseignement personnel sur un tiers, révélerait l'existence d'un renseignement personnel ou causerait un préjudice sérieux aux tiers.
- Droit de rectification et à l'effacement (lorsqu'un renseignement personnel est inexact, incomplet ou ambigu et lorsque sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi);
- Droit à la désindexation;
- Droit de retrait du consentement.

D'ici le 23 septembre 2024 : Informer la personne responsable de vos systèmes informatiques de vos nouvelles obligations concernant vos systèmes et les personnes autorisées à recevoir la communication des renseignements personnels informatisés.

SANCTIONS EN CAS DE MANQUEMENT OU D'INFRACTIONS

- Sanctions administratives pécuniaires : La Commission peut imposer une sanction pécuniaire pour un manquement concernant : l'obligation d'information, la vie du renseignement personnel, la déclaration d'incident de confidentialité, le devoir d'assurer la protection des renseignements personnels.

*** Il est possible en cas de manquement de prendre engagement auprès de la Commission pour remédier aux manquements ou en atténuer les conséquences.

Pour un organisme communautaire, la sanction est d'un maximum de 10 000 000\$

Critères guidant la détermination de la sanction :

- La nature, la gravité, le caractère répétitif et la durée du manquement;
- La sensibilité des renseignements personnels concernés;
- Le nombre de personne concernée par le manquement;
- Le risque de préjudice;
- Les mesures prises pour remédier ou atténuer le manquement;
- Le degré de collaboration que donne l'organisme à la Commission;
- Les compensations offertes aux personnes concernées;
- La capacité de l'organisme à payer la sanction.

- Sanctions pénales : L'administrateur, le dirigeant ou le représentant de l'organisme peut être accusé de l'infraction et se voir imposer une amende s'il a : ordonné ou autorisé l'accomplissement de l'acte ou de l'omission qui constitue l'infraction.

Pour une personne morale comme un OBNL, l'amende possible se situe entre 15 000\$ et 25 000 000\$.

Critères guidant la détermination de la sanction :

- La nature, la gravité, le caractère répétitif et la durée de l'infraction;
- La sensibilité des renseignements personnels concernés;
- Le fait que l'organisme ait agi intentionnellement ou fait preuve de négligence ou d'insouciance;
- La prévisibilité de l'infraction;
- Les tentatives de dissimulation ou le défaut de tenter d'atténuer les conséquences;
- L'omission de prendre des mesures raisonnables pour empêcher l'infraction;
- Le fait que cette infraction ait augmenté les revenus ou réduit les dépenses de l'organisme;
- Le nombre de personne concernée par l'infraction;
- Le risque de préjudice.