Norme nationale du Canada
Proposition de norme

Titre de la norme proposée :
Gouvernance des données dans la prestation des services sociaux et communautaires

Résumé en langage clair de la proposition de norme (200 mots maximum) :
Un cadre de gouvernance des données pour les organisations fournissant des services sociaux et communautaires qui vise à préserver la confidentialité des données de leurs clients et donateurs.

Portée proposée :
La norme proposée vise à établir les exigences minimales régissant la collecte, le stockage, l'utilisation et le partage des renseignements personnels réalisés de manière responsable et respectueuse de la vie privée par les organisations offrant des services sociaux et communautaires. Sont visés les éléments suivants : • des données des clients, des bénéficiaires et des donateurs; • des pratiques de gouvernance et de gestion des données; • des réglementations en matière de confidentialité et des autres lois applicables; • des directives et pratiques éthiques pertinentes; • des exigences pour les fournisseurs de services, les bailleurs de fonds et les fournisseurs de technologies.

Besoin stratégique :
Déterminez le besoin stratégique des principales parties prenantes et la confirmation exprimant le besoin. *Cela demande de tenir compte des éléments suivants :* *a. Le besoin stratégique de la principale prenante (p. ex., le législateur, le secteur, le gouvernement, les consommateurs);* *b. Le type de norme (norme internationale, régionale ou nationale, et le besoin d'harmonisation);* *c. La reconnaissance des normes à jour par rapport aux normes désuètes pour s'assurer que les entreprises ont accès aux plus récentes caractéristiques en matière d'innovation, de technologie et de sécurité;*

d. *Le soutien aux programmes de certification nationaux, régionaux ou internationaux comme objectif de la norme;*
e. *L'existence d'une volonté des parties prenantes d'adopter une norme différente;*
f. *Le type de maintenance (périodique, continue, stabilisée, à durabilité minimale);*
g. *L'utilisation d'un descripteur « CAN ».*

La collecte de données par les fournisseurs de services sociaux et communautaires

Les fournisseurs de services sociaux et communautaires du Canada sont responsables d'offrir des services et du soutien aux personnes vulnérables et à risque. La grande majorité de ces organisations recueillent et utilisent une certaine quantité de données de clients. Certaines de ces données sont sensibles, comme les informations reliées à la participation à un traitement des dépendances, à un diagnostic de santé ou à un témoignage de violences subies.

Au-delà de la collecte d'informations sur les clients, une grande partie de ces organisations recueillent également des dons de la part de particuliers. En effet, ce soutien financier peut être indispensable à leur réussite.

Les risques auxquels sont confrontés les fournisseurs de services sociaux et communautaires

À mesure que les fournisseurs de services sociaux et communautaires adoptent de nouvelles technologies pour la gestion des clients et des donateurs, le nombre de données sous le contrôle des organisations et de leurs fournisseurs se multiplie. Cette multiplication peut, à son tour, entraîner de nouveaux risques graves liés à la confidentialité et à la sécurité qui ne sont pas toujours bien compris.

1. L'utilisation non autorisée des données de clients peut causer un préjudice irréparable à ces clients, sous la forme, entre autres, d'atteinte à la réputation, de traumatisme ou d'une exposition au vol d'identité et à la fraude.
2. Si les données des donateurs sont compromises, cela peut également entraîner la perte de confiance de ces derniers.
3. La réputation de l'organisation, ainsi que celle du secteur des services sociaux et communautaires dans son ensemble, peut elle aussi s'effriter à mesure que les violations de données et autres préjudices s'accumulent.

La vulnérabilité aux risques

Les fournisseurs de services sociaux et communautaires sont particulièrement vulnérables, puisqu'ils sont plus susceptibles d'être confrontés à ces risques.

Premièrement, la **multitude d'exigences en matière de confidentialité et de réglementation imposée au sein du secteur social** peut entraîner une incertitude au sujet des normes de conformité à respecter. Les fournisseurs de services sociaux et communautaires se retrouvent, en effet, à l'intersection de plusieurs réglementations en matière de protection de la vie privée et ne sont pas soumis à un cadre de réglementation unique comme ceux qui régissent d'autres secteurs (p. ex., les services financiers). L'applicabilité d'un cadre de réglementation spécifique dépend en grande partie de l'entité faisant affaire avec le client, des informations en tant que telles (par exemple, si le travail

implique certains postes réglementés en vertu des lois provinciales sur les renseignements médicaux) et de l'entité qui finance le travail. À différents moments au cours des interactions, une même entité peut se voir soumise à des lois provinciales ou fédérales, à des lois associées aux renseignements personnels en général ou aux renseignements médicaux en particulier, et à des lois qui s'appliquent spécifiquement au secteur sans but lucratif, au secteur privé ou au secteur public. Les exigences en matière de financement qui s'appliquent aux diverses entités subventionnaires, y compris le gouvernement, peuvent faire intervenir certaines lois, mais ces dernières ne s'appliqueront pas uniformément à tous les clients ou à tous les programmes. De telles disparités entraînent alors une gestion inégale de la confidentialité au sein d'une même organisation.

Deuxièmement, **l'absence d'un accord global concernant les outils et les processus de gestion des données de clients à utiliser** aggrave la vulnérabilité que présentent ces organisations. Au Canada, des milliards de dollars ont été dépensés afin de soutenir la numérisation dans le secteur de la santé et quelques systèmes centraux ont fait leurs preuves pour la gestion des données. En revanche, de nombreux fournisseurs de services sociaux et communautaires dépendent toujours des renseignements sur papier, des feuilles de calcul ou d'un sous-ensemble de solutions qui ne permettent pas un effort de protection de la vie privée uniforme. Plusieurs organisations font encore usage de fichiers Excel protégés par un mot de passe (avec des mots de passe partagés) ou d'armoires de stockage des données déverrouillées. Même si les exigences en matière de confidentialité étaient clairement indiquées, les fournisseurs de services pourraient ne pas disposer des outils nécessaires pour protéger les informations de leurs clients de manière appropriée.

Troisièmement, **la rareté des fonds d'exploitation de base peut entraîner une capacité interne insuffisante.** Par exemple, de nombreux fournisseurs de services sociaux et communautaires n'ont pas la capacité interne suffisante pour :

1. comprendre pleinement et respecter les exigences légales et réglementaires en matière de gestion et de gouvernance des données;
2. examiner de manière appropriée les fournisseurs de technologie avec qui ils font affaire (p. ex., les logiciels CRM/SGD);
3. construire et maintenir une infrastructure ou des processus informatiques, y compris des systèmes de cybersécurité, conçus pour gérer les cybermenaces courantes de l'ère numérique;
4. former et retenir du personnel capable d'assurer une surveillance constante;

Enfin, les fournisseurs de services sociaux et communautaires peuvent être la cible d'attaques de rançongiciels, car le caractère volumineux des subventions en jeu signifie qu'ils détiennent souvent des sommes importantes dans leurs comptes bancaires.

Les avantages d'une bonne gouvernance des données

Réaliser la collecte, le stockage, l'utilisation et le partage des données des clients, des donateurs et des dons de manière responsable est donc d'autant plus important puisque cela permet de gérer les risques et les vulnérabilités.

Adopter de bonnes pratiques de gouvernance des données peut également contribuer à l'amélioration de l'expérience client, ce qui est important lorsque l'on vise une approche qui tient compte des traumatismes. En effet, une telle approche permet d'éviter les recommandations, les

renvois, les formulaires et les processus de consentement sans fin. Adopter de bonnes pratiques de gouvernance contribue également à la rétention et à l'engagement du personnel.

De plus, une fois les protections appropriées bien en place, les fournisseurs de services sociaux et communautaires peuvent alors mieux utiliser les données à leur disposition afin de remplir leur mission. Par exemple, les fournisseurs ne permettent pas un accès uniforme aux données. Un système de soutien en matière de gestion des fournisseurs serait donc bénéfique pour les organisations. Certains utilisateurs précoces explorent déjà des solutions associées à l'IA afin d'améliorer leurs opérations. Cependant, l'IA n'est pas encore bien comprise au sein du secteur en général et son utilisation peut donc introduire des risques supplémentaires liés à la partialité, au manque de transparence et au manque de responsabilité. Afin de pouvoir pleinement bénéficier de l'efficience que peut permettre l'adoption de l'IA, les fournisseurs de services sociaux et communautaires doivent d'abord mettre en place de solides pratiques de gouvernance des données.

L'insuffisance des normes existantes

Il n'existe actuellement aucune norme reconnue (par exemple, ISO, CEN, BSI ou SA) spécifiquement axée sur les données du secteur social. De plus, les normes plus générales en matière de gouvernance des données ne sont pas adaptées aux besoins de ce dernier, puisque :

1. les fournisseurs de services sociaux et communautaires à but non lucratif opèrent au sein d'un environnement réglementaire unique et les organismes de bienfaisance enregistrés s'occupent de gérer des dons admissibles à un reçu aux fins d'impôt, ce qui implique également l'intérêt public;
2. les fournisseurs de services sociaux et communautaires se distinguent des entités publiques et ne sont pas régis par les lois associées à l'utilisation des données par le gouvernement. Qui plus est, leurs parties prenantes et leurs bénéficiaires les obligent à respecter des normes éthiques plus rigoureuses que celles d'autres organisations. Afin d'assurer la confiance des parties prenantes, ils nécessitent un standard de pratique spécifique qui peut même dépasser les exigences légales minimales;
3. ce secteur a tendance à utiliser une suite commune d'applications logicielles qui sont uniques et non utilisées dans d'autres industries;
4. les composantes des normes de certification en gestion de cas (CARF, CARAF, CAC) qui traitent de certains aspects de la protection de la vie privée sont souvent des composantes mineures du service à la clientèle, et non des éléments autonomes complets qui peuvent être mis à jour rapidement afin de relever les défis en constante évolution du secteur;
5. en ce qui concerne les données des donateurs, il existe des directives éthiques strictes pour les collecteurs de fonds professionnels, telles que la Charte des droits du donateur, créée par l'Association des professionnels en collecte de fonds (AFP), l'Association for Healthcare Philanthropy (AHP), le Council for Advancement and Support of Education (CASE) et le Giving Institute: Leading Consultants to Nonprofits. Ces directives énoncent des principes de haut niveau, tels que le droit « d'être assurés que les informations concernant leurs dons sont traitées avec respect et confidentialité dans la mesure prévue par la loi ». Ces lignes directrices peuvent être développées davantage en (1) se concentrant plus spécifiquement sur les risques et les catalyseurs liés à la technologie et aux données et (2) en fournissant des conseils techniques plus détaillés sur la manière exacte de répondre aux exigences établies par ces cadres éthiques.

Par conséquent, il est nécessaire d'établir une norme capable de définir les exigences minimales en matière de gouvernance des données.

Principales parties prenantes

Les principales parties prenantes comprennent :

- Les organismes sans but lucratif et leurs associations et fédérations (p. ex., CanaDon, Imagine Canada, United Way Centreaide Canada, Bénévoles Canada, Ontario Nonprofit Network et 211)
- Les organismes de prestation de services sociaux à but lucratif
- Les collecteurs de fonds et leurs associations (p. ex., l'Association des professionnels en collecte de fonds [AFP], les CFRE, et le Council for Advancement and Support of Education [CASE])
- Les fondations et les entités philanthropiques et leurs associations (p. ex., Fondations communautaires du Canada et Fondations philanthropiques Canada)
- Les fournisseurs de technologies des organisations caritatives et des fondations (p. ex., FundMetric, FundraiseUp, Blackbaud, HelpSeeker, Salesforce et Benevity)
- Les conseillers en technologie pour les organismes de bienfaisance (p. ex., Technology Helps et Ajah)
- Les avocats spécialisés en droit des organismes de bienfaisance (p. ex., Miller Thomson et Carters)
- L'Agence du revenu du Canada
- CPA Canada

La norme nationale du Canada visée par la présente proposition :

- soutiendra les futurs programmes de certification élaborés à l'échelle nationale, régionale et internationale afin de soutenir les secteurs caritatifs et de la collecte de fonds;
- fera l'objet d'une mise à jour périodique conformément à ce que déterminera le comité technique responsable de son élaboration;
- fera appel au descripteur CAN.

Besoin de disponibilité dans les deux langues officielles du Canada : *Les parties prenantes jugent-elles nécessaire que la norme soit publiée dans les deux langues officielles?* *Les utilisateurs de la norme jugent-ils nécessaire que celle-ci soit publiée dans les deux langues officielles?* *Les autorités compétentes jugent-elles nécessaire que la norme soit publiée dans les deux langues officielles?* *Est-il nécessaire, sur les plans de la santé et la sécurité, que la norme soit publiée dans les deux langues officielles?* *En ce qui concerne les adoptions, la norme régionale ou internationale (ou tout autre produit livrable) est-elle mise à disposition à partir de la source?* *En ce qui concerne les adoptions, existe-t-il une entente avec le comité de la source pour faciliter une traduction officielle?*	O

Considérations liées à la représentation géographique :

Déterminez la représentation géographique canadienne correspondant au domaine concerné par la norme.

La représentation géographique peut tenir compte de facteurs comme :

a. *l'industrie (p. ex., le pétrole dans les provinces productrices de pétrole);*
b. *la référence en réglementation (si la province possède une réglementation);*
c. *les caractéristiques et l'impact social des produits de base (p. ex., le mazout de chauffage pour les climats nordiques).*

Tous les secteurs de l'économie.

Marché :

Indiquez de quelle manière la norme répond aux besoins du marché et contribue à favoriser le commerce dans les contextes géographiques et économiques les plus vastes possibles.

Par exemple :

a. *Faciliter l'innovation canadienne afin qu'elle joue un rôle de premier plan à l'échelle internationale;*
b. *Appuyer les objectifs du principe « Une norme, un essai, acceptés partout »;*
c. *Appuyer les objectifs visant à « Être les premiers à commercialiser »;*
d. *Favoriser l'harmonisation des exigences à l'échelle internationale, régionale et nationale.*

Une norme conçue au Canada facilitera l'innovation canadienne afin qu'elle joue un rôle de premier plan à l'échelle internationale, un avancement qui touchera particulièrement les fournisseurs canadiens axés sur la gestion des données et les outils d'IA utilisés pour les opérations du secteur social. La norme permettra alors d'assurer une confiance dans les technologies canadiennes, ce qui améliorera les perspectives commerciales de ces technologies. La norme prendra en considération et s'alignera sur toutes les normes mondiales, telles que le Code de normes éthiques de l'Association of Professional Fundraisers.

Documents existants pertinents à l'échelle internationale, régionale et nationale :

ISO/IEC 38500, Technologies de l'information – Gouvernance des technologies de l'information pour l'entreprise

ISO/IEC 38505-1, Technologies de l'information – Gouvernance des technologies de l'information – Gouvernance des données – Partie 1 : Application de l'ISO/IEC 38500 à la gouvernance des données

ISO/IEC TR 38505-2, Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données

Série ISO 8000, qualité des données

ISO 27001, sécurité de l'information

Code de normes éthiques de l’Association des professionnels en collecte de fonds

CASE Global Reporting Standards

Charte des droits du donateur

Programme de normes d’Imagine Canada