CAN/DSGI 100-11:2025
NORME NATIONALE DU CANADA

Première édition
2025-05

Gouvernance des données – Partie 11 : Prestation de services communautaires et sociaux

03.100.02; 03.100.40; 35.020; 35.030

Page laissée intentionnellement vierge

Table des matières

Page laissée intentionnellement vierge

Avant-propos

L'Institut des normes de gouvernance numérique (INGN) élabore des normes de gouvernance de la technologie numérique adaptées à une utilisation planétaire. Il collabore avec des experts, avec des partenaires au pays et à l'étranger et avec le public pour établir des normes nationales visant à réduire les risques pour la population et les organisations canadiennes qui adoptent et utilisent des technologies novatrices dans l'économie numérique d'aujourd'hui.

Ses normes sont élaborées conformément aux *Exigences et lignes directrices – Accréditation des organismes d'élaboration de normes* (13 juin 2019) du Conseil canadien des normes (CCN).

Il est à noter que certains éléments de la présente norme peuvent faire l'objet de droits de brevet. L'INGN ne saurait être tenu responsable de ne pas avoir indiqué ces droits. Les droits de propriété intellectuelle identifiés lors de l'élaboration de la présente norme figurent dans l'introduction.

Pour en savoir plus sur l'INGN :

Institut des normes de gouvernance numérique
100, promenade Innovation, bureau 500
Ottawa (Ontario) K2K 3E7
www.dgc-cgn.org/fr

Une Norme nationale du Canada est une norme qui a été élaborée par un organisme d'élaboration de normes (OEN) titulaire de l'accréditation du Conseil canadien des normes (CCN) conformément aux exigences et lignes directrices du CCN. On trouvera des renseignements supplémentaires sur les Normes nationales du Canada à l'adresse : https://ccn-scc.ca/.

Le CCN est une société d'État qui fait partie du portefeuille d'Innovation, Sciences et Développement économique Canada. Dans le but d'améliorer la compétitivité économique du Canada et le bien-être collectif de la population canadienne, l'organisme dirige et facilite l'élaboration et l'utilisation des normes nationales et internationales. Le CCN coordonne aussi la participation du Canada à l'élaboration des normes et définit des stratégies pour promouvoir les efforts de normalisation canadiens.

En outre, il fournit des services d'accréditation à différents clients, parmi lesquels des organismes de certification de produits, des laboratoires d'essais et des organismes d'élaboration de normes. On trouvera la liste des programmes du CCN et des organismes titulaires de son accréditation à l'adresse : https://ccnscc.ca/.

Page laissée intentionnellement vierge

Introduction

Voici la première édition de la norme CAN/DGSI 100-11:2025, *Gouvernance des données – Partie 11 : Prestation de services communautaires et sociaux*.

Cette norme a été élaborée par le Comité technique 1 (TC 1) de l'INGN sur la gouvernance des données, composé de plus de 260 grands penseurs et experts en gouvernance des données et de domaines connexes. Elle a été approuvée par un groupe avec droit de vote formé par le comité technique comprenant 4 producteurs, 3 représentants du secteur public, d'organismes de réglementation ou d'organismes responsables des politiques, 4 utilisateurs et 4 représentants de la collectivité.

Toutes les unités de mesure utilisées sont exprimées conformément au Système international d'unités (SI).

La norme sera soumise à l'examen du Comité technique au plus tard deux ans après sa date de publication, après quoi elle pourra être rééditée, révisée, confirmée ou abandonnée.

Son but premier est énoncé sous la rubrique « Portée ». Il importe de retenir qu'il incombe à l'utilisateur de juger si la norme convient à une application donnée.

La norme est conçue pour être utilisée dans l'évaluation de la conformité.

03.100.02; 03.100.40; 35.020; 35.030

THIS NATIONAL STANDARD OF CANADA IS AVAILABLE IN BOTH FRENCH AND ENGLISH.

Page laissée intentionnellement vierge

Contexte

La présente norme est soutenue par un comité technique bénévole et une équipe de rédaction composée de huit bénévoles experts en la matière qui s'intéressent à ce sujet et qui proviennent d'organismes canadiens à but non lucratif de divers horizons, dont l'Ontario Nonprofit Network (ONN), la Fondation Trillium de l'Ontario (FTO), l'Approche commune de la mesure d'impact, la filiale de Toronto de l'Association canadienne pour la santé mentale (ACSM), l'Institut de recherche, de données et de formation du Nouveau-Brunswick (IRDF-NB) et le Centre canadien pour la résilience numérique des organismes sans but lucratif (CCRNOSBL). La norme a été rédigée par l'équipe de rédaction, puis révisée et commentée par le comité technique avant d'être rendue disponible par l'INGN pour examen public, approbation par comité, ratification et publication.

Elle est conçue pour aider les organisations qui offrent des services communautaires et sociaux, y compris des programmes financés par des tiers, à protéger la confidentialité des données. En pratique, la confidentialité des données ne doit pas être perçue comme une tâche administrative ou opérationnelle, mais plutôt comme une obligation fondamentale, ce qui implique de former les bénévoles selon leurs tâches et leurs responsabilités. Les tiers bailleurs de fonds doivent envisager comment fournir les ressources nécessaires aux organismes sans but lucratif (OSBL) dont le financement est conditionnel à la collecte de renseignements personnels

Gouvernance des données et importance des normes

La gouvernance des données dans les services communautaires et sociaux est utile à bien des égards. Elle est essentielle pour préserver l'utilité, l'accessibilité et la sécurité des données de l'organisation. Elle clarifie qui, au sein de l'organisation, est responsable des données et impose la mise en place de pratiques ou de politiques couvrant toutes les étapes du cycle de vie des données. Elle tient compte du lien entre les données et l'organisation, énonce des principes ou des valeurs conformes à la mission et au mandat de l'organisation et assigne les responsabilités liées aux données aux bonnes personnes (salariées ou bénévoles). La gouvernance est le pilier central de toute stratégie de données.

Les normes de gouvernance des données sont essentielles pour organiser, documenter et représenter (expliquer et classer les métadonnées) les données en vue de faciliter leur utilisation et leur partage. Elles couvrent tant les décisions simples sur la saisie des données que les décisions complexes concernant l'anonymisation d'un jeu de données particulier. Elles se renforcent mutuellement puisqu'elles peuvent contribuer à lancer des discussions cruciales et à clarifier certaines définitions, en particulier lorsque chaque sous-secteur utilise des abréviations qui lui sont propres. L'harmonisation des normes entre les organisations peut aider à comparer les programmes similaires, à relever les pratiques économiques et à relier les différents ensembles de données pour mettre d'autres éléments en lumière.

En tant qu'outil d'apprentissage, la présente norme aplanit les obstacles aux efforts collectifs du secteur. A joué un rôle de premier plan dans son élaboration la compréhension des questions d'équité, en particulier des préjudices passés et présents découlant de la gouvernance, de la collecte, de la consultation, de l'utilisation, du partage et du stockage des données. Le comité technique reconnaît que ces préjudices ont disproportionnellement touché les personnes autochtones, noires et racisées. Il

espère que la création de la présente norme viendra complémenter d'autres initiatives concernant la souveraineté et l'équité en matière de données, comme les *Principes de propriété, de contrôle, d'accès et de possession (PCAP^{MD}) des Premières Nations* et le *Black Community Data Governance Framework* de la Ville de Toronto.

Gouvernance des données et intelligence artificielle

Les cadres robustes de gouvernance des données forment une base solide pour tout programme de gouvernance de l'intelligence artificielle (IA) formulé avant l'utilisation, le développement ou le déploiement de systèmes ou d'outils d'IA. Ils comprennent des politiques, des mesures de contrôle et des procédures clairement définies pour la collecte, la consultation, l'utilisation, le partage et le stockage des renseignements personnels; la mise en place de mesures de sécurité visant à protéger les renseignements personnels, médicaux ou commerciaux confidentiels; et la conformité aux protocoles de cybersécurité. Les organisations doivent également veiller à ce que leurs pratiques de gouvernance des données respectent les lois et la réglementation en vigueur au Canada, dont la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), les lois provinciales régissant la confidentialité des renseignements médicaux, les lois sur la propriété intellectuelle, la *Loi canadienne sur les droits de la personne* et toute autre loi provinciale ou territoriale applicable. Ainsi, elles pourront traiter leurs données de manière éthique, sécurisée et conforme et donc déployer des outils d'IA générative de manière efficace et responsable pour atteindre leurs objectifs et servir la population en toute sécurité.

Monétisation des données

Dans le domaine de la gouvernance des données, la monétisation des données désigne l'utilisation de celles-ci comme actif stratégique pour générer des revenus ou améliorer l'efficacité opérationnelle de sorte à libérer des ressources pouvant ainsi être allouées à la mission principale de l'organisation. Cela se fait au moyen du processus « données-constat-action » (Wixom, Beath et Owens, 2023), au cours duquel les données sont analysées pour produire des constats qui orientent les actions et les décisions stratégiques. Des revenus peuvent être tirés de ces constats ainsi que du partage des données, de l'octroi de licences ou de la vente de jeux de données anonymisés.

Cependant, la monétisation des données ne concerne pas uniquement les gains financiers. Les questions éthiques – les activités de monétisation ne doivent entrer en conflit ni avec la mission, les engagements relatifs à l'équité et les valeurs fondamentales de l'organisation, ni avec les lois et règlements applicables, ni avec le consentement des personnes à qui les données appartiennent, s'il y a lieu – sont au cœur de ce processus. Les investissements en infrastructure et en capacité liées aux données peuvent être coûteux et augmenter les dépenses d'exploitation annuelles, mais ce ne sont pas que des dépenses : ils représentent aussi des décisions stratégiques qui, à long terme, créeront de la valeur pérenne quantifiable.

L'organisation doit déterminer quelle valeur pourrait le plus facilement découler de ses initiatives de données, comme la production de constats exploitables, l'amélioration de l'efficacité opérationnelle ou de la prestation de services, ou un soutien à l'innovation; ainsi, elle pourra se concentrer sur les initiatives ayant le plus de poids stratégique. La gouvernance efficace et éthique des données peut donc

permettre aux organisations de financer plus de programmes, d’améliorer les services et d’établir des partenariats qui renforcent leurs capacités et les aident à servir leur milieu.

Gouvernance des données – Partie 11 : Prestation de services communautaires et sociaux

1 Portée

Le présent document énonce les exigences minimales que les organisations qui offrent des services communautaires et sociaux doivent respecter pour recueillir, consulter, utiliser, partager et stocker des renseignements personnels de manière responsable et dans le respect de la confidentialité. La présente norme est un guide visant d'une part à aider les OSBL et les bailleurs de fonds à utiliser leurs données de manière éthique et équitable, et d'autre part à faire progresser la culture entourant la collecte, la consultation, l'utilisation, le partage et le stockage des données dans le secteur.

Elle s'applique aussi aux OSBL, généralement de petite ou moyenne taille, qui doivent composer avec un effectif limité et dont les employés doivent tous assumer de nombreuses responsabilités.

Elle aborde les points suivants :

- Lignes directrices et pratiques concernant l'équité en matière de données;
- Données des clients ou bénéficiaires et des donateurs;
- Pratiques de gouvernance et de gestion des données;
- Règlements sur la vie privée et autres lois applicables;
- Lignes directrices et pratiques en matière d'éthique;
- Exigences pour les fournisseurs de services, les bailleurs de fonds et les fournisseurs de technologies.

2 Références normatives

La présente norme renvoie aux documents suivants de telle sorte qu'une partie ou la totalité de leur contenu constitue une exigence normative. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, c'est la dernière édition des documents mentionnés qui s'applique (y compris les éventuelles modifications).

Groupe de travail sur l'équité en santé pour les Noirs, *Engagement, gouvernance, accès et protection (EGAP) : Cadre de gouvernance des données pour les données de santé recueillies auprès des communautés Noires*

Ville de Toronto, *Black Community Data Governance Framework*

Centre de gouvernance de l'information des Premières Nations, *Principes de PCAP^{MD} des Premières Nations*

Ontario Nonprofit Network, *A Framework for Nonprofit Data Strategies*

Association nationale des centres d'amitié, *Stratégie nationale en matière de données*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent :

chiffrement
Modification de la forme de l'information pour en cacher le contenu et empêcher l'accès non autorisé.

[SOURCE : Centre canadien pour la cybersécurité]

classification des données
Schéma structurant l'accès aux actifs de données et la protection de ces actifs.

[SOURCE : Association internationale des professionnels de la protection de la vie privée, *Glossary of Privacy Terms*]

collecteur de données
Personne ou entité recueillant des données.

confidentialité
Capacité à protéger les données sensibles contre l'accès non autorisé.

[SOURCE : CAN/DGSI 104:2021/rév. 1 : 2024, version modifiée]

contrôleur de données
Partie qui, seule ou avec d'autres, détermine les objectifs et les procédés de traitement des données personnelles. Le traitement peut être délégué à une autre partie, appelée traiteur de données. Le contrôleur est responsable de la légalité du traitement, de la protection des données et du respect des droits des personnes ou entités concernées. C'est aussi lui qui reçoit les demandes des personnes ou entités concernées voulant se prévaloir de leurs droits.

[SOURCE : Contrôleur européen de la protection des données, *Glossaire*]

cycle de vie des données
Processus englobant toute l'existence des données, de leur création à leur suppression définitive.

[SOURCE : Association internationale des professionnels de la protection de la vie privée, *Glossary of Privacy Terms*]

équité
Élimination des obstacles d'ordre systémique (par exemple, les préjugés inconscients, la discrimination, le racisme, le sexisme, le capacitisme, l'homophobie), permettant à toutes les personnes d'avoir des chances équitables d'accéder à un programme et d'en bénéficier.

[SOURCE : Gouvernement du Canada, *Pratiques exemplaires en matière d'équité, de diversité et d'inclusion en recherche*]

équité en matière de données
Principes et pratiques orientant l'utilisation des données dans une optique de diversité, de justice, d'équité et d'inclusion.

[SOURCE : Ontario Nonprofit Network, *A Framework for Nonprofit Data Strategies*]

fuite de données
Incident de cybersécurité au cours duquel des renseignements confidentiels, protégés ou sensibles sont volés, perdus, ou collectés, utilisés ou divulgués sans autorisation.

[SOURCE : CAN/DGSI 104:2021/rév. 1 : 2024]

gérance des données
Collecte, conservation, utilisation, suppression et diffusion de données; dans ce contexte, action de décider qui a accès aux données, à quelles fins et au profit de qui.

[SOURCE : Open Data Stewards Institute, *Applying new models of data stewardship to health and care data* (contenu adapté)]

groupe racisé
Groupe de personnes classées selon des caractéristiques ethniques ou raciales et, sur ce fondement, soumises à un traitement discriminatoire.

[SOURCE : Gouvernement du Canada, *Guide de la terminologie liée à l'équité, la diversité et l'inclusion*]

personne ou entité concernée
Personne ou entité dont les données sont traitées.

[SOURCE : CAN/DGSI 100-2:2022/rév. 1 : 2024]

propriétaire de données
Personne ou entité responsable de la gouvernance d'un jeu de données de l'organisation.

renseignements personnels
Information sur une personne identifiable.

[SOURCE : CAN/DGSI 103-1:2023 (rév. 2024)]

sécurité des données
Processus, actions, politiques, exigences réglementaires, réponses et procédures appliqués, communiqués, respectés, convenus et surveillés pour protéger la confidentialité et l'intégrité des renseignements.

NOTE : Dans de nombreux cas, l'application de ces mesures de protection exige le respect de lois nationales et internationales.

[SOURCE : CAN/DGSI 100-2:2022/rév. 1 : 2024]

sensibilité des données
Mesure dans laquelle la divulgation ou le mauvais usage des données pourraient être préjudiciables.

[SOURCE : CAN/DGSI 117:2023]

traiteur de données
Personne physique (autre qu'un employé du contrôleur) ou morale, autorité publique, agence ou autre entité traitant des données personnelles au nom du contrôleur. Une organisation peut être simultanément contrôleur et traiteur, selon la fonction qu'elle assure.

[SOURCE : Association internationale des professionnels de la protection de la vie privée, *Glossary of Privacy Terms*]

utilisateur de données
Personne ou entité pouvant utiliser les données ou interagir avec elles.

vie privée
Droit des personnes de choisir elles-mêmes quels renseignements à leur propos peuvent être consultés, utilisés, partagés et stockés.

[SOURCE : Alan F. Westin, *Privacy and Freedom*, New York : Atheneum, 1967]

4 Gouvernance et supervision

4.1 Contexte

4.1.1 Cette section énonce des exigences de base pour les principes de gouvernance des données que les organisations devraient suivre tout au long du cycle de vie des données. Les collecteurs, les contrôleurs, les utilisateurs et les traiteurs de données doivent reconnaître que les données ne sont pas intrinsèquement neutres, c'est-à-dire qu'elles peuvent être biaisées et refléter le point de vue et les valeurs de ceux qui les recueillent, les analysent et les interprètent.

4.2 Responsabilité et surveillance

4.2.1 L'organisation doit élaborer un plan de gouvernance des données.
NOTE : Ce plan peut faire partie d'autres plans de gouvernance existants ou en élaboration.

4.2.2 L'organisation doit désigner un responsable chargé de surveiller le plan de gouvernance des données et d'en assurer le respect.

4.2.3 Des audits réguliers doivent avoir lieu pour surveiller la conformité au plan de gouvernance des données et l'efficacité de ce dernier.

4.3 Consentement éclairé

4.3.1 L'organisation doit veiller à ce que le consentement éclairé, qui doit être obtenu des bénéficiaires des services communautaires et sociaux avant la collecte des données, tienne compte de toutes les étapes possibles du cycle de vie des données.

4.3.2 Le consentement éclairé peut comprendre, sans s'y limiter, les critères suivants :

a) Comment les données seront-elles partagées, et sous quelle forme?
b) Des données identifiables seront-elles partagées?
c) À quelles fins les données seront-elles consultées et utilisées?
d) Quel rôle jouera le propriétaire des données dans tout éventuel partage?
e) La personne ou entité concernée a-t-elle été clairement informée du moment à partir duquel elle peut demander que ses données ne soient plus partagées?

4.3.3 Si on ne peut pas obtenir le consentement éclairé de la personne ou de l'entité concernée, l'organisation doit se reporter aux lois sur la vie privée pertinentes.

4.4 Équité en matière de données

4.4.1 L'organisation doit reconnaître et respecter la souveraineté des données autochtones et la gouvernance des données des personnes noires.

4.4.2 L'organisation doit reconnaître le principe de souveraineté des données voulant que les lois sur les données varient d'une province ou d'un territoire à l'autre et veiller au traitement équitable des données de tous les utilisateurs, en tous lieux. Pour mieux protéger les droits des utilisateurs, le principe d'« autosouveraineté des données dès la conception » sera intégré à tous les aspects de l'élaboration et de la mise en place du produit ou service, comme indiqué à la section 4.4.1.

4.4.3 L'organisation devrait adhérer aux cadres de gouvernance des données relatifs aux Autochtones et aux personnes noires.

NOTE : Ces cadres comprennent notamment, pour la collaboration avec les Autochtones, les *Principes de propriété, de contrôle, d'accès et de possession (PCAP^{MD}) des Premières Nations* et la *Stratégie nationale en matière de données* de l'Association nationale des centres d'amitié, et pour la collaboration avec les personnes noires, le *Black Community Data Governance Framework* de la Ville de Toronto et le *Cadre de gouvernance des données pour les données de santé recueillies auprès des communautés Noires* du Groupe de travail sur l'équité en santé pour les Noirs.

4.4.4 Les collecteurs de données devraient adhérer aux principes d'équité en matière de données et intégrer des stratégies de cet ordre dans leur plan de gouvernance des données. Ces stratégies devraient :

a) tenter de répondre aux besoins des groupes racisés et marginalisés, et particulièrement des personnes noires et des Autochtones, à toutes les étapes du cycle de vie des données;

b) habiliter les groupes racisés et marginalisés à participer aux processus de gouvernance des données;

c) faire en sorte que les pratiques de gouvernance des données de l'organisation ne perpétuent pas de biais et n'entraînent pas de résultats discriminatoires;

d) mobiliser les communautés en fondant les approches de gouvernance des données sur l'équité de manière à bâtir la confiance et à réduire les préjudices;

e) examiner le contexte sociohistorique pour identifier les causes premières des disparités, pour orienter la collecte et l'utilisation des données et pour élaborer des solutions fondées sur des données;

f) faire en sorte que les données visualisées promeuvent l'inclusion et la sensibilisation à des publics cibles de cultures, de langues et de races différentes;

g) chercher à obtenir le consentement de la personne ou de l'entité concernée sur l'interprétation des jeux de données;

h) obliger la ventilation des données pour faciliter l'analyse des disparités et le suivi des progrès ainsi que pour orienter les actions;

i) remettre en question les méthodes et les hypothèses habituelles ainsi que la perspective de la culture dominante en matière de collecte et d'analyse de données, et trianguler les données quantitatives avec d'autres sources (Gonzalez et coll., 2024).

5 Collecte de données

5.1 Contexte

5.1.1 Cette section énonce les principes et exigences en matière de collecte des données, lesquels s'appliquent aux collecteurs, aux contrôleurs, aux administrateurs, aux utilisateurs et aux traiteurs de données, et présente leurs responsabilités à l'égard de la personne ou de l'entité concernée.

5.2 Permission de collecte

5.2.1 L'organisation doit consigner les objectifs précis de la collecte, du traitement et de la rétention des données.

5.2.2 La collecte de données doit être conforme à toutes les lois et à tous les règlements applicables.

5.2.3 L'organisation doit avoir une politique régissant la collecte de données dans le cadre de son plan de gouvernance des données.

5.2.4 L’organisation doit obtenir le consentement volontaire – exprès ou implicite – de toute personne ou entité concernée avant de procéder à la collecte des données, selon les objectifs visés et le type de données recueillies.

5.2.5 Le processus de consentement doit présenter clairement l’objectif, la portée et l’utilisation des données recueillies.

5.2.6 L’organisation doit indiquer clairement à la personne ou à l’entité concernée le processus à suivre pour retirer son consentement à tout moment pendant ou après la collecte, et indiquer à partir de quand il n’est plus possible de retirer les données. Ce processus peut nécessiter la suppression ou la modification des données recueillies.

5.3 Qualité et intégrité des données

5.3.1 L’organisation doit donner des renseignements clairs sur ses pratiques de gouvernance des données et les rendre accessibles à la personne ou à l’entité concernée et à toutes les parties intéressées au moment de la collecte.

5.3.2 L’organisation doit veiller, au meilleur de sa capacité, à ce que les données recueillies remplissent les critères de qualité que sont l’exhaustivité, l’exactitude, la récence, l’actualité et l’intégrité.

5.4 Minimalisation des données

5.4.1 Les contrôleurs de données devraient restreindre la collecte de renseignements personnels à ce qui est directement pertinent et nécessaire pour accomplir l’objectif déclaré de la collecte de données.

5.4.2 Les contrôleurs de données devraient conserver les données seulement aussi longtemps que nécessaire pour accomplir cet objectif.

5.4.3 Les données ne doivent pas être utilisées ou divulguées à des fins autres que celles pour lesquelles elles ont été recueillies, sauf avec le consentement exprès ou si la loi l’exige.

5.4.4 Les périodes de rétention des données doivent être définies selon l’objectif de la collecte des données et les exigences juridiques. Une fois ces périodes échues, les données doivent être supprimées de manière sécurisée.

6 Stockage des données

6.1 Contexte

6.1.1 Cette section énonce les principes et exigences en matière de stockage des données, lesquels s’appliquent aux collecteurs, aux contrôleurs, aux utilisateurs et aux traiteurs de données, et présente leurs responsabilités à l’égard de la personne ou de l’entité concernée. Le stockage adéquat des données est crucial pour préserver l’intégrité, la confidentialité et la disponibilité des renseignements et pour ainsi protéger les données des accès non autorisés, des modifications, des pertes et de la destruction. Cette responsabilité incombe à l’organisation.

6.1.2 L’organisation devrait étudier attentivement et évaluer régulièrement les exigences de résidence des données en tenant compte de l’équilibre entre les avantages potentiels et les

risques possibles, par exemple la vie privée, la sécurité publique, la sécurité intérieure et nationale, l'entrave à l'innovation et la restriction de l'accès aux services.

6.2 Protection sécurité des données

6.2.1 L'organisation doit avoir une politique régissant le stockage des données dans le cadre de son plan de gouvernance des données.

6.2.2 Il doit y avoir des mesures de sécurité techniques, matérielles et organisationnelles proportionnelles à la sensibilité des données.

6.2.3 La personne, le comité ou le groupe de travail responsable de la protection et de la sécurité des données de l'organisation doit tenir sa formation en sécurité des données à jour.

6.3 Stockage des données

6.3.1 L'organisation doit trouver la solution de stockage des données (physique, infonuagique, locale ou hybride) qui protège le mieux les données recueillies.

6.3.2 Les données physiques doivent être stockées dans un emplacement sécurisé à accès restreint.

6.3.3 L'organisation doit, dans le cadre de sa politique de stockage des données, consigner où sont stockées les données localement ou dans le nuage et quelles lois de protection des données s'appliquent dans ces endroits.

6.3.4 Les données doivent être classifiées selon leur niveau de sensibilité.

6.3.5 L'organisation doit définir ce qu'est une utilisation appropriée d'appareils personnels pour l'accès aux données.

6.4 Mesures de sécurité techniques

6.4.1 Les données au repos et en transit doivent être chiffrées selon les protocoles d'usage dans le secteur.

6.4.2 L'accès aux données doit être restreint à certains postes. Seuls les membres du personnel autorisés ayant un besoin opérationnel légitime doivent être autorisés à accéder aux données sensibles.

NOTE : Les données sensibles sont généralement une catégorie d'information pouvant causer des dommages ou des préjudices au-delà d'un certain seuil.

6.4.3 L'authentification multifacteur doit être mise en place pour l'accès aux systèmes de stockage ou de traitement des données sensibles.

6.4.4 L'organisation doit régulièrement mener des audits de sécurité de données et des évaluations des vulnérabilités pour déceler et atténuer les risques potentiels.

6.4.5 L'organisation doit surveiller l'accès aux données et les opérations sur les données et les consigner dans un journal pour détecter toute activité non autorisée et intervenir rapidement.

6.5 Sauvegarde et reprise

6.5.1 L'organisation devrait stocker les données à plusieurs endroits (stockage physique, infonuagique, local ou hybride).

6.5.2 L’organisation doit utiliser une solution de sauvegarde automatisée et la tester régulièrement.

6.5.3 L’organisation doit veiller à ce que ses logiciels soient mis à jour régulièrement.

6.6 Conservation et archivage

6.6.1 L’organisation doit instaurer une politique de conservation des données énonçant la durée pour laquelle chaque type de données sera conservé avant d’être supprimé. Cette politique doit comprendre toute exigence juridique applicable et tout dossier ou certificat de suppression requis.

6.6.2 Les données ne doivent être conservées qu’aussi longtemps que nécessaire pour accomplir ce pour quoi elles ont été recueillies.

7 Accès aux données et utilisation

7.1 Contexte

7.1.1 Cette section énonce les mesures à prendre pour sécuriser l’accès aux données personnelles ou médicales et leur utilisation. Les utilisateurs des données sont responsables de leurs actions relatives à l’accès aux données personnelles et à leur utilisation. La responsabilité peut être rendue explicite grâce à des mesures de protection administratives et à des pratiques exemplaires, comme le recours à des ententes de confidentialité et des attestations de connaissance des politiques de confidentialité.

7.2 Généralités

7.2.1 L’organisation doit avoir une politique régissant l’accès aux données et leur utilisation dans le cadre de son plan de gouvernance des données.

7.2.2 L’organisation doit veiller à la transparence de ses pratiques relatives aux données, par exemple en indiquant comment les données seront utilisées et en signalant toute fuite de données aux propriétaires des données en question.

7.2.3 Les utilisateurs de données doivent recevoir une formation en confidentialité des données avant de recueillir, de consulter, d’utiliser, de partager ou de stocker celles-ci. Cette formation doit être renouvelée périodiquement pour consolider l’application des pratiques exemplaires.

NOTE : Le Commissariat à la protection de la vie privée du Canada propose des outils de formation sur ce sujet.

7.2.4 La formation doit être adaptée aux données et actualisée régulièrement pour maintenir la conformité aux lois et aux pratiques exemplaires.

7.2.5 La formation doit traiter de la détection des fuites et des incidents relatifs aux données ainsi que des mesures d’intervention qui s’imposent.

7.2.6 L’accès doit être limité aux seules données nécessaires afin de réaliser l’objectif pour lequel on y accède. Pour ce faire, on peut avoir recours à une gestion des accès et des permissions d’utilisation basée sur les rôles.

7.2.7 Les données consultées ou utilisées doivent être anonymisées autant que possible pour accomplir une tâche donnée.

7.2.8 L’accès et l’utilisation ne doivent être permis qu’aux fins pour lesquelles les données ont été recueillies avec le consentement des personnes concernées.

7.2.9 Toute autre raison d’accéder aux données ou de les utiliser nécessite le consentement (ou le renouvellement du consentement) des personnes concernées.

7.2.10 Il doit y avoir un mécanisme permettant d’accéder aux données pour les corriger à la demande de la personne concernée.

NOTE : Cela n’est pas toujours possible, par exemple dans le cas d’un sondage anonyme ou dans toute autre situation où une réponse ne peut pas être liée à une personne spécifique.

7.2.11 Il doit y avoir un mécanisme pour permettre un accès sécurisé au cas où il faudrait consulter les données en vertu de la loi.

7.2.12 Les permissions d’accès et d’utilisation doivent être supprimées lorsque les utilisateurs quittent leur poste.

7.2.13 L’organisation doit veiller à ce que ses méthodes d’interprétation des données produisent des résultats exacts, fiables et conformes à ses objectifs de collecte de données.

8 Partage et publication des données

8.1 Contexte

8.1.1 Cette section énonce les principes et exigences en matière de partage des données recueillies par les organisations de services communautaires et sociaux. Le partage de données peut s’avérer nécessaire pour les bénéficiaires et les fournisseurs de services communautaires et sociaux, puisqu’il peut orienter l’offre de services actuelle et future. La présente section a pour fil conducteur le droit des bénéficiaires des services communautaires et sociaux de savoir comment leurs données seront utilisées et partagées et de refuser que leurs données soient partagées à tout moment après la collecte desdites données.

8.2 Généralités

8.2.1 L’organisation doit avoir une politique régissant le partage et la publication des données dans le cadre de son plan de gouvernance des données.

8.2.2 L’organisation doit déterminer les conséquences du partage des données sur les bénéficiaires de ses services communautaires et sociaux.

8.2.3 L’organisation doit réduire le partage des données au minimum requis pour les fins énoncées ci-dessus, dans le respect des attentes de confidentialité des personnes et entités dont les données pourraient être partagées et conformément aux lois, règlements, politiques et lignes directrices applicables.

8.2.4 L’organisation doit indiquer quelles données seront partagées, avec qui, dans quel format et de quelle manière.

8.2.5 L’anonymisation des données doit être la norme lorsque l’on partage les données, sauf indication ou obligation contraire. Si des données identifiables doivent être partagées (par

exemple, pour offrir d'autres services), il faut s'assurer de respecter les lois, règlements, politiques et lignes directrices applicables.

8.2.6 L'organisation doit veiller à ce que les données ne soient partagées que par des canaux de communication sécurisés au moyen de procédés robustes et conformes aux lois, règlements, politiques et lignes directrices régissant la communication des données liées aux services communautaires et sociaux.

8.2.7 L'organisation doit instaurer des protocoles, des formats et une terminologie tels que les données puissent être échangées entre différents systèmes et logiciels et utilisées sur ceux-ci sans en altérer le sens ou la fonction.

8.3 Ententes de partage de données

8.3.1 L'organisation doit identifier les tiers avec qui elle partagera les données.

8.3.2 L'organisation doit conclure une entente de partage de données avec les tierces parties avant tout partage de données.

8.3.3 L'organisation doit s'assurer qu'il y a une personne responsable de veiller à ce que toutes les modalités des ententes de partage de données soient respectées.

8.3.4 Les ententes de partage de données doivent définir les modalités et les conditions du partage de données ainsi que les fins pour lesquelles les données peuvent être utilisées ou partagées à d'autres.

8.3.5 Les ententes de partage de données doivent énoncer les mesures prises pour préserver la vie privée des propriétaires des données et pour conserver les données de manière sécurisées. Elles doivent aussi énoncer les conditions sous lesquelles les données peuvent être partagées à d'autres.

8.3.6 Les ententes de partage de données doivent indiquer où, comment et pendant combien de temps les données partagées seront stockées par les tiers.

8.3.7 Les ententes de partage de données doivent énoncer quand les données seront détruites et toutes les exigences relatives aux certificats de destruction.

Bibliographie

[1] Association internationale des professionnels de la protection de la vie privée (2024). *Glossary of Privacy Terms.* Consulté le 19 juillet 2024 à l'adresse https://iapp.org/resources/glossary/.

[2] Centre de gouvernance de l'information des Premières Nations (25 juillet 2023). *Les principes de PCAP[MD] des Premières Nations*. Consulté le 20 avril 2024 à l'adresse https://fnigc.ca/fr/les-principes-de-pcap-des-premieres-nations/.

[3] Commissariat à la protection de la vie privée du Canada (31 mai 2019). *Principes relatifs à l'équité dans le traitement de l'information de la LPRPDE.* Consulté le 20 avril 2024 à l'adresse https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/p_principle/.

[4] Contrôleur européen de la protection des données (2024). *Glossaire*. Consulté le 20 avril 2024, à l'adresse https://www.edps.europa.eu/data-protection/data-protection/glossary_fr.

[5] Gonzalez, Naihobe, et coll. (20 avril 2024). *Education-to-Workforce Indicator Framework: Using Data to Promote Equity and Economic Security for all.* Consulté le 19 juillet 2024 à l'adresse https://www.mathematica.org/publications/education-to-workforce-indicator-framework-using-data-to-promote-equity-and-economic-security.

[6] Law for Non-Profits (2024). *Top Tips for Maintaining Data Privacy*. Consulté le 19 juillet 2024 à l'adresse https://lawfornonprofits.ca/blog/top-tips-maintaining-data-privacy.

[7] NTEN (2021). *Data Policies Your Nonprofit Needs.* Consulté le 19 juillet 2024 à l'adresse https://word.nten.org/wp-content/uploads/2021/10/Data-Policies-Your-Nonprofit-Needs.pdf.

[8] Ontario Nonprofit Network (ONN) (2023). *A framework for nonprofit data strategies.* Consulté le 20 avril 2024 à l'adresse https://theonn.ca/publication/deal-framework/.

[9] Own Company (18 août 2023). *What Every Nonprofit's Data Protection Solution Should Include*. Consulté le 19 juillet 2024 à l'adresse https://www.owndata.com/blog/what-every-nonprofits-data-protection-solution-should-include.

[10] Wixom, B. H., Beath, C. M. et Owens, L. (2023). *Data Is Everybody's Business: The Fundamentals of Data Monetization.* Cambridge, Massachusetts, États-Unis : The MIT Press. Consulté le 12 mai 2024.