Enjeux juridiques de la transformation numérique pour les organismes sans but lucratif

Confidentialité, protection de la vie privée et cybersécurité

Assemblée de la francophonie de l'Ontario

Table des matières

Assemblée de la francophonie de l'Ontario

AVERTISSEMENT

Le contenu de cette présentation ne doit pas être interprétée comme constituant un conseil ou un avis juridique.

Il est fortement recommandé d'obtenir un avis juridique pour votre organisation

Assemblée de la francophonie de l'Ontario

Comment la transformation numérique vous affecte-t-elle votre organisation?

Assemblée de la francophonie de l'Ontario

Contexte de la transformation numérique

Assemblée de la francophonie de l'Ontario

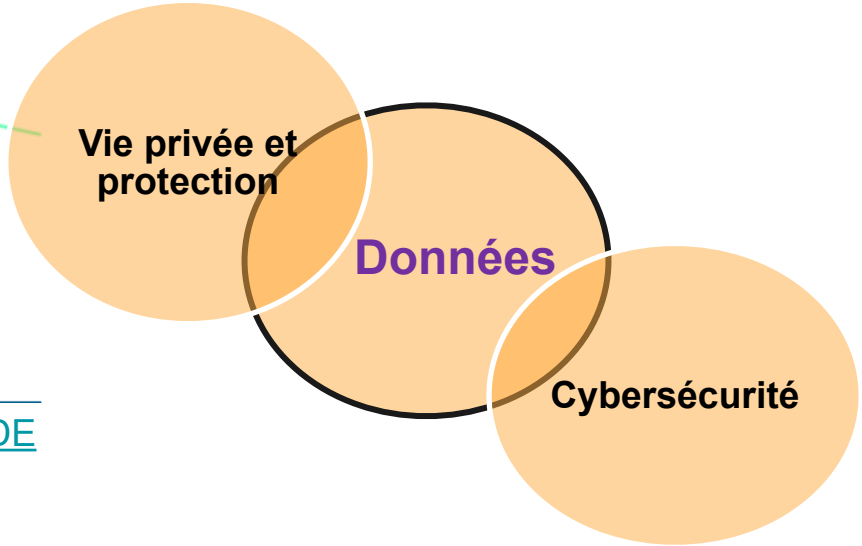
La transformation numérique

- Transformation numérique est un but/destination
  - C’est plutôt un voyage ou un cheminement
- Numérisation de votre organisation
  - Transformation numérique est plutôt stratégique que technologique
- Perturbation de votre organisation
  - Pragmatique, flexible, tester et d’améliorer

Contexte de la transformation numérique

Source et en savoir plus : [Site de l'OCDE]

- # Services infonuagiques
- # Sécurité des données
- # Améliorer l'accès et la gestion des données
- # Plus grande efficacité et transparence
- # Meilleure collaboration et communications



Assemblée de la francophonie de l'Ontario

Pertinence pour les OSBL

« Les **grands volumes de données que détient le secteur sans but lucratif en Ontario** ne sont pas à l'abri des vulnérabilités en matière de protection de la vie privée et de sécurité [...] ils restent largement non protégés par les dispositions fédérales sur la protection de la vie privée, dont la portée est limitée par la Constitution. La pandémie n'a fait qu'exacerber les cybermenaces qui pèsent sur le secteur non commercial. Comme bien d'autres secteurs, les organisations sans but lucratif ont de plus en plus recours au télétravail, ce qui accroît l'exposition aux risques pour la vie privée et la sécurité [...] les organismes sans but lucratif peuvent avoir moins de ressources à consacrer aux activités de conformité en matière de protection de la vie privée.[...]

Aucune loi sur la protection de la vie privée ne s'applique de manière générale aux organismes sans but lucratif de l'Ontario, et la responsabilité à l'égard de ce secteur n'incombe à aucun organisme de réglementation. »

Commentaires de la Commissaire à l'information et à la protection de la vie privée en Ontario suite au livre blanc publié par le ministère des Services gouvernementaux et des Services aux consommateurs

Partie 1 – Protection de la vie privée et des renseignement personnels

Assemblée de la francophonie de l'Ontario

Objectifs du cadre juridique

- Établir les règles pour déterminer quels renseignements personnels peuvent être collectés par les organisations et par quels moyens
- Énoncer les règles régissant le traitement, la gestion et le partage des renseignements personnels entre les institutions et organisations
- Établir les procédures d'accès aux renseignements personnels par les personnes concernées

Cadre juridique : Fédéral

- Loi sur la protection des renseignements personnels
  - *Privacy Act*
  - Applique aux organisations du secteur public

- *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)

  - *Personal Information Protection and Electronic Documents Act* (“PIPEDA”)
  - Applique aux organisations du secteur privé
  - Renseignements personnels qu’ils collectionne, utilise et divulguent dans le cours de leurs activités commerciales
  - S’applique aux renseignements sur les employés dans le contexte fédéral comme les banques, compagnies aériennes

Cadre juridique : provincial

- Certaines lois sont considérées **substantiellement similaires** à LPRPDE
  - S'appliquent aux renseignements sur les employés sauf dans le contexte fédéral
  - **Québec** : *Loi sur la protection des renseignements personnels dans le secteur privé*
  - **Alberta** : *Personal Information Protection Act*
  - **Colombie-Britannique** : *Personal Information Protection Act*
- Les autres provinces ont des lois qui touchent certains aspects ou offrent des protections additionnelles.
- **Importantes à considérer si votre organisme offre des services dans d'autres provinces.**

Cadre juridique : Ontario

- *Loi sur l'accès à l'information et la protection de la vie privée (PAIPVP)*
  - S'applique au gouvernement provincial, aux universités, aux collèges, aux hôpitaux et organismes désignés
- *Loi de 2004 sur la protection des renseignements personnels sur la **santé***
  - **IMPORTANTE (non abordée ici) pour les organisations qui collaborent dans le cercle des soins médicaux pour protéger** les renseignements qui touchent la santé physique ou mentale du particulier, fournisseurs de soins de santé, programmes et services, numéro de la carte Santé, identifier un mandataire spécial, règles de garde des dépositaires.
- *Loi sur l'accès à l'information **municipale** et la protection de la vie privée*
  - S'applique au institutions municipales, conseils scolaires, services de polices et autres entités administratives

Assemblée de la francophonie de l'Ontario

Cadre juridique (clin d'œil international)

Union Européenne (UE)

- Règlement général sur la protection des données (RGPD)
  - General Data Protection Regulation (GDPR)
  - harmonise les lois nationales de protection des données (UE)
  - renforce la protection (confidentialité des données personnelles) de tous les résidents de l'UE
  - s'applique à toutes les entreprises qui traitent les données personnelles de résidents de l'UE, y compris les entreprises établies à l'extérieur de l'UE

Laquelle s'applique à vous?

- Aucune spécifique pour les OSBL, **MAIS**
  - Les OSBL ne sont pas systématiquement exclus
  - Particularité de vos activités
  - Certains secteurs qui traitent des renseignements sensibles (exemple: santé)
  - Lieu de prestation de vos services
  - Protection des renseignements au sujet de vos employé(e)s

- **A qui vous adresser en cas de problème lié à la protection de la vie privée?**
  - Ressource utile: https://www.priv.gc.ca/fr/signaler-un-probleme/leg_info_201405/

Concept clé : renseignement personnel

« [t]out renseignement concernant un individu **identifiable** ».

Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), paragraphe 2(1)

- Pour en savoir plus (site du Commissariat à la protection de la vie privée du Canada)

Assemblée de la francophonie de l'Ontario

Exemples de renseignements personnels

- le nom;
- l'adresse personnelle;
- l'adresse de courriel personnelle;
- le numéro de téléphone personnel;
- la race;
- l'origine nationale;
- l'origine ethnique;
- la couleur;
- la religion;
- l'âge;
- la date de naissance;
- le sexe;
- l'orientation sexuelle;
- l'état matrimonial;
- l'état familial;
- l'éducation;
- les antécédents médicaux;
- les antécédents professionnels;
- les opérations financières auxquelles une personne a participé;
- le numéro d'identification;
- un symbole individuel attribué à une personne;
- la photographie d'une personne;
- un autre signe particulier permettant d'identifier une personne;
- les empreintes digitales;
- le groupe sanguin;
- la correspondance adressée par une personne à une institution, de caractère personnel ou confidentiel, soit implicitement, soit explicitement, ou des réponses à cette correspondance qui révèleraient le contenu de la première correspondance;
- les opinions ou les points de vue d'une personne, sauf s'ils sont au sujet d'une autre personne;
- les opinions ou les points de vue d'une autre personne au sujet de la personne en question.

Source : https://www.ontario.ca/fr/document/manuel-sur-lacces-linformation-et-la-protection-de-la-vie-privee/chapitre-7-principes-fondamentaux-de-la-protection-de-la-vie-privee

Concept clé : activités

activité commerciale Toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds. (commercial activity)

LPRPDE, art 2 (1)

Principes importants

1. Responsabilité
2. Détermination des fins de la collecte des renseignements
3. Consentement
4. Limitation de la collecte
5. Limitation de l'utilisation, de la communication et de la conservation
6. Exactitude
7. Mesures de sécurité
8. Transparence
9. Accès aux renseignements personnels
10. Possibilité de porter plainte à l'égard du non-respect des principes

Concept clé : consentement valable

- collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire
- forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements
- les attentes raisonnables de la personne sont aussi pertinentes
- Pour quelles fins ou utilisations? Réviser en cas de changements
- Avec qui ces renseignements seront partagés

En savoir plus: Infographie : Obtenir un consentement valable

Concept clé : consentement valable

Consentement peut être

- **express**
  - Important pour les renseignements sensibles : positif « Je peux donner la permission… »
- **implicite**
  - Par exemple : on donne les informations pour obtenir le service
  - **Et si le renseignement est public ?**
    - Renseignements sur les coordonnées de travail
    - Renseignement auquel les gens ont accès publiquement car la personne l'a partagé (journal, artistique, littéraire)
  - **Et si on est en contexte d'impartition ? (tierces parties)**

Obligations à considérer

- Protéger les données dont vous disposez, particulièrement celles qui sont sensibles
  - Mesures physiques : des classeurs verrouillés et un accès restreint aux bureaux
  - Mesures organisationnelles : accès limités « au besoin de savoir », formations des personnes, etc.
  - Mesures technologiques : utilisation de mots de passe et le cryptage

En cas d'atteintes aux mesures de sécurité

Les organisations assujetties à la LPRPDE doivent :

- déclarer au commissaire à la protection de la vie privée du Canada les atteintes aux mesures de sécurité concernant des renseignements personnels présentant un risque réel de préjudice grave à des individus;
- aviser les intéressés au sujet de ces atteintes;
- conserver un registre de toutes les atteintes

Plus d'information : Site du Commissariat à la protection de la vie privée

Rôles des Commissaires

Commissaire à la protection de la vie privée (fédéral)
• enquêter sur les plaintes, mener des vérifications et intenter des poursuites judiciaires en vertu de deux lois fédérales; • publier de l'information sur les pratiques relatives au traitement des renseignements personnels d'organisations des secteurs public et privé; • appuyer, entreprendre et publier des travaux de recherche sur les enjeux liés à la protection de la vie privée; • sensibiliser la population aux enjeux concernant la protection de la vie privée et les lui faire comprendre.
Commissaire à l'information et à la protection de la vie privée (Ontario)
• présenter des commentaires sur l'incidence des programmes proposés des institutions sur la protection de la vie privée • après avoir entendu la personne responsable, à enjoindre à une institution de renoncer à certains modes de collecte de renseignements et à disposer des fiches de renseignements personnels qui contreviennent à la Loi • d'entreprendre des recherches sur les questions qui ont une incidence sur la réalisation des objets de la Loi, d'instituer à l'intention du public des programmes d'information relatifs à la Loi ainsi qu'au rôle et aux activités du commissaire, et de recevoir les observations du public

Retour aux principes importants

1. Responsabilité
2. Détermination des fins de la collecte des renseignements
3. Consentement
4. Limitation de la collecte
5. Limitation de l'utilisation, de la communication et de la conservation
6. Exactitude
7. Mesures de sécurité
8. Transparence
9. Accès aux renseignements personnels
10. Possibilité de porter plainte à l'égard du non-respect des principes

Partie 2 – La cybersécurité

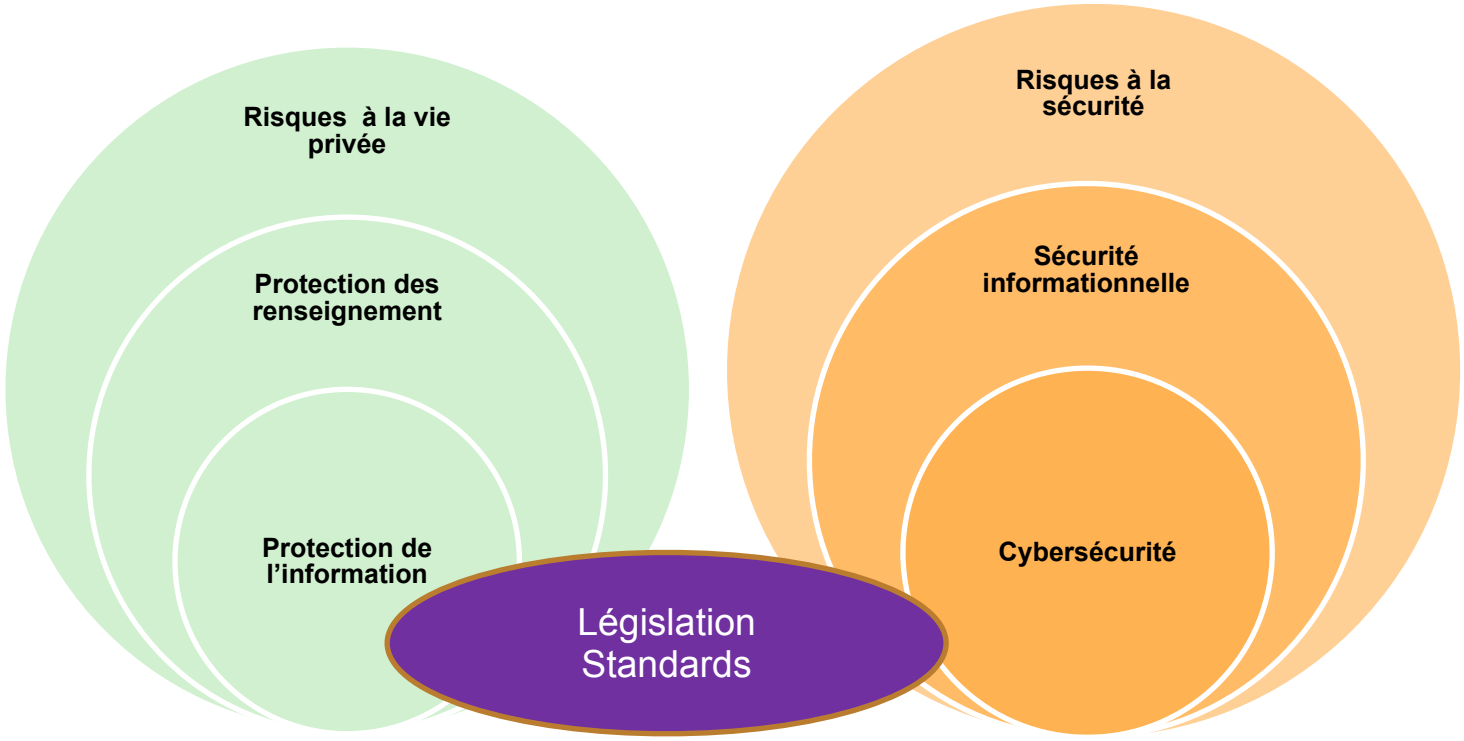
Assemblée de la francophonie de l'Ontario

Définition

Ensemble des technologies, des processus, des pratiques et des mesures d'atténuation et d'intervention conçus pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés afin d'assurer la confidentialité, l'intégrité et la disponibilité.

Source : Termium Plus

Relation entre vie privée et cybersécurité



Assemblée de la francophonie de l'Ontario

Exemples de menaces

- Logiciels malveillants (Malware)
- Rançongiciels (Ransomware)
- Brèche ou atteinte à la protection des données (Threats against data)
- Ingénierie sociale (Social Engineering threats)
  - Hameçonnage, harponnage, appât
- Disinformation/Misinformation
- Disponibilité de services (Threasts against availability)
- Domaines de premier niveau (Top-Level Domain)

Concept clé : anonymisation

- **Anonymisation** : supprimer tout caractère identifiant à un ensemble de données (irréversible)

- **Pseudonymisation** : remplace les identifiants privés par de faux identifiants ou des pseudonymes (réversible)

Plusieurs techniques:

- Masquage des données
- Brouillage des données
- Cryptage des données
- Échange des données
- Données synthétiques
- Substitution des données

Mesures de protection raisonnables

- Quelle est la sensibilité des renseignements personnels en question?
- Est-ce que le risque pour la sécurité des données est prévisible ?
- Quelle est la probabilité que des dommages se produisent?
- Quelle est la gravité du préjudice?
- Quel est le coût des mesures atténuantes?
- Quels sont les standards ou les exigences dans votre domaine?

Questions de discussion –

Quels risques à la confidentialité ou à la sécurité pouvez-vous identifier ?

Assemblée de la francophonie de l'Ontario

Mise en situation 1

- Alex, qui travaille chez ABC En Aide, un OSBL qui aide à l'éducation et l'intégration des nouveaux arrivants en Ontario.
- Un jour, Alex reçoit un courriel publicitaire qui ressemble beaucoup à ceux que l'équipe reçoit habituellement de leurs fournisseurs, accompagné d'un fichier. Alex le sauvegarde comme d’habitude sur son ordinateur et l'ouvre ensuite.
- Quelques semaines plus tard, la direction d’ABC En Aide apprend que des renseignements personnels ont été compromis à cause d’un virus.

Mise en situation 2

- Un(e) employé(e) marche vers sa voiture pour y déposer des dossiers contenant des renseignements confidentiels sur les donateurs. Un coup de vent s'amène et de nombreux papiers s'envolent, sans que l'employé(e) ne puisse les rattraper.

- Variante : l'employé(e) perd un clé USB qui contient un fichier Excel avec les informations sur les donateurs.

Mise en situation 3

- Un(e) employé(e) consulte les dossiers de certains de ses collègues et bénévoles, sans toutefois avoir l'autorisation pour le faire.

Mise en situation 4

- Un(e) employé(e) d'un OSBL qui aime être productif et utilise les technologies pour y arriver.
- L'employé(e) utilise une application appelée ChatGPT pour préparer une stratégie de communication aux donateurs et pour comparer des documents. Les documents contiennent des renseignements au sujet des clients et des donateurs ainsi que des informations au sujet des différentes sources de financement de l'OSBL.

Surveillance des employés

- Depuis le 11 octobre 2022, employeurs d'au moins de 25 employés doivent avoir une politique indiquant s'ils surveillent leurs employés et les méthodes utilisées

- Pour en savoir plus : *Loi sur les normes d'emploi et Politique écrite sur la surveillance électronique des employés*

Changements à considérer

- **Fédéral** : Projet de loi C-27 *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*
  - *Obligations de conformité, amendes, considérations sur des technologies comme l'intelligence artificielle*

- **Québec** : *Projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*
  - *Changements sur 3 ans (2022-2023-2024)*
  - *Se rapproche de la RPDE*

Changements éventuels à considérer

- **Ontario**:
  - Gouvernement de l'Ontario, Services gouvernementaux et Services aux consommateurs: Consultation et publication d'un livre blanc (2021). Voir *Renforcer les mesures de protection de la vie privée pour l'avenir numérique de l'Ontario*
  - **N'est pas en vigueur, mais pourrait s'appliquer aux OSBL et organismes de charité**
  - **Emphase sur : le consentement et droits à la vie privée, la transparence, la suppression des données, droit à l'oubli et de la portabilité des données**
  - **Des pouvoirs additionnels aux Commissaire ainsi que des pénalités de 10M$ ou 3% (administrative) ou 25M$ ou 5% (pénale) des revenus annuels bruts de l'an passé.**
  - **Ajout de l'exigence de l'anonymisation des renseignements personnels**

Meilleures pratiques à adopter pour gérer les risques juridiques

- Rédiger une Politique de confidentialité et de protection des renseignements personnels
  - Distinguer les renseignements liés au service à la clientèle
- Considérer l'impact des lois d'autres juridictions sur vous, selon vos activités (au Québec par exemple) et les informations que vous collectez.
- S'assurer qu'une personne soit responsable de la protection des renseignements personnels
- Former le personnel

Meilleures pratiques à adopter (suite)

- Effectuer un inventaire des données susceptibles d'être touchées
    - Effectuer un inventaire des données disponibles
    - Quelles données collectionne-t-on (sur les gens)?
    - Comment les utilise-t-on?
    - Où on sauvegarde ces données?
    - Qui en est responsable?
    - Comment ces données sont-elles protégées?
- Mettre en place des mesures pour prévenir ou limiter les conséquences d'un incident de confidentialité
- Connaître les obligations d'aviser en cas de brèches
- Répondre aux demandes d'accès aux renseignements

Conclusions

- Être conscients que les lois peuvent s’appliquer, peu importe votre statut/
- Adopter les meilleures pratiques
- Communiquer clairement avec vos parties prenantes. Ces dernières sont plus exigeantes et ont plus d’attentes
- Demander un avis sur le cadre applicable spécifiquement à votre OSBL

Ressources utiles

- Commissariat à la protection de la vie privée du Canada : https://www.priv.gc.ca/fr/
  - Application de la LPRPDE aux organisations caritatives et à but non lucratif
  - Lignes directrices pour l'obtention d'un consentement valable
  - 10 conseils de protection de la vie privée pour les entreprises
- Commissaire à l'information et à la protection de la vie privée de l'Ontario : https://www.cipvp.ca/
- Moderniser la vie privée en Ontario : https://www.ontariocanada.com/registry/view.do?language=fr&postingId=37468
- Centre canadien pour la résilience numérique des organismes sans but lucratif: https://ccndr.ca/?lang=fr
- Centre canadien pour la cybersécurité : https://www.cyber.gc.ca/fr
- Consortium national pour la cybersécurité: https://ncc-cnc.ca/fr/consortium-national-pour-la-cybersecurite/

Ressources utiles (suite)

- Webinaire sur Charity Village : CYBERSECURITY AWARENESS FOR CANADIAN NONPROFITS AND CHARITIES : https://charityvillage.com/cybersecurity-awareness-for-canadian-nonprofits-and-charities/
- Hackers for Change : https://www.hackersforchange.com/
- CANON | Canadian Anonymization Network : https://deidentify.ca/
- Commissaire à l'information et à la protection de la vie privée de l'Ontario, « De-Identification Guidelines for Structured Data » : https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf
- Liste de vérification (Alberta) par Charity Central: http://www.charitycentral.ca/wp-content/uploads/privacy-en.pdf

Avez-vous des questions?

ChristianeSaad

Assemblée de la francophonie de l'Ontario