GUIDE DE BONNES PRATIQUES CONCERNANT LA CRÉATION DE POLITIQUES DE CONFIDENTIALITÉ DANS LE SECTEUR DE LA CULTURE[i]

IVADO

SYNAPSE C

Septembre 2019

Table des matières

Termes du mandat

Dans le cadre du « Programme de démarrage de projets de recherche collaborative avec les membres industriels d'IVADO », Synapse C, organisme à but non lucratif qui vise à développer et à mettre en commun l'expertise en valorisation de données pour les arts et la culture au Québec et au Canada, ainsi qu'IVADO, organisme ayant vocation à regrouper professionnels de l'industrie et chercheurs académiques afin de développer une expertise de pointe dans les domaines de la science des données, de l'optimisation et de l'intelligence artificielle, ont contacté le Laboratoire de cyberjustice, centre de recherche en droit des technologies de la Faculté de droit de l'Université de Montréal, pour participer à un projet de recherche collaborative.

L'objectif étant de mener une étude sur la collecte de données dans le domaine des arts et de la culture au Canada, notamment par la mise en place de politiques types de confidentialité reflétant les meilleures pratique dans le domaine en date de ce Guide. Plus précisément, Synapse C a mandaté le Laboratoire de cyberjustice pour :

- Effectuer une analyse du droit québécois et fédéral de la protection des données personnelles,
- Rédiger un guide de bonnes pratiques sur les politiques de confidentialité pour les organismes québécois et canadiens qui souhaiteraient faire mutualiser et valoriser leurs données par des tiers, tels que Synapse C, afin que ces tiers puissent récolter les données de ces organismes dans le respect des droits des individus.

L'approche de ce guide de bonnes pratiques sera double. Pour ce faire, nous comptons effectuer une analyse en droit québécois et fédéral, afin que Synapse C puisse fournir des recommandations standardisées pour les acteurs du secteur de la culture tant québécois que canadiens, ces organismes souhaitant avoir une meilleure compréhension des enjeux entourant les renseignements personnels, plus particulièrement en ce qui a trait aux politiques de confidentialité. Il est cependant important de noter que l'analyse effectuée ne vise pas la législation applicable aux autres provinces dans le secteur privé, plus particulièrement le *Personal Information Protection Act* de la Colombie-Britannique[1] ainsi que le *Personal Information*

[1] *Personal Information Protection Act,* S.B.C. 2004, ch. 63.

Protection Act d'Alberta[2]. Il est également important de considérer l'évolution rapide des technologies et de la législation applicable, ce Guide et les politiques de confidentialité étant limités à la situation prévalant en date de leur rédaction.

Introduction

« *The world's most valuable resource is no longer oil, but data* ». Depuis la parution de cet article dans le journal *The Economist* en 2017, rares sont ceux qui demeurent encore sceptiques face à l'ampleur de la transformation sociétale provoquée par l'avènement de l'ère du Big data ou des données massives. En effet, l'utilisation des données, combinée à leur traitement, peut générer une réelle valeur ajoutée sociale et économique, mais soulève une variété de questions quant aux risques et à l'encadrement de celles-ci.

D'une part, elle peut contribuer à stimuler la productivité ainsi qu'à améliorer ou promouvoir de nouveaux produits, processus, méthodes d'organisation et marchés, ce que l'Organisation de Coopération et Développement Économique (OCDE) appelle « l'innovation fondée sur les données » (Data Driven Innovation)[3]. Mais, d'autre part, on ne peut occulter le fait que ces données sont émises par des personnes physiques, sujets de droits, et que le traitement de celles-ci conduit à la révélation d'informations personnelles, voire sensibles selon le contexte. La protection des données doit donc aller de pair avec leur usage.

On assiste ainsi à une prise de conscience citoyenne en matière de protection des données, tandis que les entreprises souhaitent en obtenir et en conserver un maximum pour leurs processus, leurs services, etc. Comment combiner ces deux exigences, plus particulièrement dans le domaine de la culture où de nombreuses entreprises, OSBL ou organismes publics cohabitent et souhaiteraient parfois échanger ou mettre en commun leurs données pour des actions conjointes ou pour améliorer l'expérience du public ?

[2] *Personal Information Protection Act,* S.A. 2003, ch. P-6.5.
[3] Des études sur les entreprises suggèrent que l'utilisation des données et leurs analyses augmentent la productivité plus rapidement que dans les entreprises non utilisatrices d'environ 5-10%.

1 - Définitions et concepts

Afin d'appréhender au mieux la protection des renseignements personnels, il est primordial de s'intéresser à la définition de l'objet premier de la protection, c'est-à-dire les données.

Qu'est-ce qu'une donnée?

De manière technique, la discipline informatique définit la donnée comme étant une représentation d'une information dans un programme que cela soit dans le texte même du programme, appelé "code source", ou dans l'exécution de celui-ci. Ces données, principalement codées, représentent alors des éléments du logiciel qui peuvent être des interactions, des transactions ou autres.

Lorsqu'on cherche ensuite à définir les données dans un cadre non plus technique, mais juridique, il devient alors important de différencier les notions d'information et de donnée. En effet, les données sont des éléments bruts qui doivent être interprétés pour que l'on puisse en tirer une information et ne recouvrent donc pas le même champ sémantique. Cette distinction est essentielle puisqu'elle justifie la création d'un droit spécifique à la protection des données, distinct du droit à la protection de l'information, qui inclut notamment les droits de propriété intellectuelle et de confidentialité.

Néanmoins, il ne faut pas oublier que certaines données sont plus aisées à interpréter que d'autres et qu'elles donnent alors accès à des informations, parfois sensibles, sur les individus. C'est pourquoi, toujours dans le but de mettre en place une protection adéquate des données concernant les individus, aussi appelées renseignements personnels, il faut s'intéresser aux méthodes de classification afin de pouvoir adapter ses actions aux divers types de données collectées. En effet, l'application des principes juridiques et obligations légales, qu'ils proviennent du législateur québécois ou fédéral, change en fonction du type de données.

Comment classifier les données ?

Bien qu'il n'existe pas véritablement d'unanimité sur la façon de classifier des données, on peut néanmoins avancer certains critères de classification essentiels à l'élaboration d'une protection de la vie privée des individus.

Les renseignements personnels :

Dans ce sens, le critère essentiel de classification est celui du caractère personnel des données.

Au Québec, est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier[4]. La *Loi sur la protection des renseignements personnels et les documents électroniques* (ci-après « Loi fédérale sur le secteur privé ») définit les renseignements personnels comme étant des renseignements concernant un individu identifiable[5]. Voici quelques exemples :

- « *l'âge, le nom, un numéro d'identification, le revenu, l'origine ethnique ou le groupe sanguin;*
- *une opinion, une évaluation, un commentaire, le statut social ou une mesure disciplinaire;*
- *le dossier d'un employé, un dossier de crédit ou de prêt, un dossier médical, l'existence d'un différend entre un consommateur et un commerçant ou le projet d'une personne (par exemple, l'intention d'acquérir des biens ou des services ou de changer d'emploi).* »[6]

En règle générale, les renseignements seront donc réputés concerner un « individu identifiable » lorsqu'il est raisonnablement possible d'identifier un individu grâce à l'utilisation de ces renseignements, seuls ou en combinaison avec d'autres.

---

[4] Art. 2 de la *Loi sur la protection des renseignements personnels dans le secteur privé*
[5] Art. 3 de la *Loi sur la protection des renseignements personnels et les documents électroniques*
[6] Commissariat à la protection de la vie privée du Canada, *Survol de la LPRPDE,* 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/lprpde_survol/, Mai 2019

La sensibilité des données :

En droit québécois, la sensibilité des données n'est pas juridiquement définie en tant que telle. En revanche, l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après, « Loi québécoise sur le secteur privé ») ainsi que l'article 63.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* énoncent de la même façon qu'un organisme public ou une entreprise : "*doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support*".

En droit fédéral, le caractère sensible des données n'est pas directement défini non plus. La Loi fédérale sur le secteur privé se contente de rappeler que toute information peut être considérée comme sensible en fonction du contexte dans lequel elle se situe et que les mesures de sécurité à prendre pour protéger les renseignements personnels dépendent de la sensibilité de ceux-ci[7].

Les échanges d'information susceptibles de contenir des renseignements personnels :

Une approche pertinente pour l'élaboration des politiques de confidentialité consiste à distinguer les parties impliquées dans les flux de données et à permettre une évaluation immédiate du caractère personnel des renseignements échangés entre celles-ci.
Le tableau ci-dessous, tiré du rapport de l'OCDE, *Data in the Digital Age*, permet d'illustrer, sur une échelle de 1 à 10, le taux de renseignements personnels lors d'un échange de données, où 1 équivaut à un faible taux de renseignements personnels et 10 à un taux important de renseignements personnels.

[7] Article 7.2 (1) et (2) et article 10.1 (8) de la Loi fédérale sur le secteur privé et articles 4.3.4 et 4.7.2 de l'Annexe 1 de la Loi fédérale sur le secteur privé.

Type de données	*Présence de données personnelles*									
Échange entre entreprises (B2B)	1	2	3	4	5	6	7	8	9	10
Chaîne de valeur globale (production)		X								
Ingénierie (M2M)				X						
Objets connectés (M2M)					X					
Finance / Ressources humaines								X		
Échange entre entreprises et particuliers (B2C)										
Médias							X			
Consommateur								X		
Services basiques (i.e. location, vente, etc.)								X		
Services personnalisés (i.e. santé, finance, etc.)										X
Échange entre gouvernements et citoyens (G2C)										
Services (i.e. santé, impôts, social, etc.)										X
Objets connectés (i.e. transports, surveillance, etc.)										X
Échange entre citoyens (C2C)										
Média sociaux										X
Communications (i.e. courriels, textos, téléphone)										X

Qu’est-ce que le traitement des données ?

Le traitement n'est pas expressément défini dans les lois fédérales sur la protection des renseignements personnels, mais, en pratique, il comprend la collecte, l'utilisation, l’analyse, la modification, le stockage, la communication ou la destruction de renseignements personnels.

Un traitement de données personnelles n’est pas nécessairement informatisé : les fichiers papier et autres supports de communication sont également concernés et doivent être protégés dans les mêmes conditions. Un traitement de données doit avoir une finalité déterminée préalablement au recueil des données et à leur exploitation.

Qu’est-ce qu’une politique de confidentialité ?

Une politique de confidentialité est un document comprenant les différentes mesures et règles adoptées par un organisme ou une entreprise, afin de garantir la sécurité et une utilisation appropriée des données recueillies dans le cadre de la relation entre ledit organisme ou entreprise et une personne physique utilisant ses services. La politique de confidentialité

comprend notamment des informations sur la manière dont les données sont collectées, stockées et utilisées par l'organisme ou l'entreprise en question et comment elles sont transmises à des tiers, le cas échéant.

2 - État du droit des données dans le contexte québécois et fédéral

Le droit canadien de la protection des renseignements personnels au Canada est pluriel, car les provinces et le fédéral ont légiféré en la matière. Dans le secteur privé on retrouve les lois suivantes :

- *Loi sur la protection des renseignements personnels et les documents électroniques* (Fédéral)
- *Loi sur la protection des renseignements personnels dans le secteur privé* (Québec)
- *Personal Information Protection Act* (Alberta)
- *Personal Information Protection Act* (Colombie-Britannique)
- mais aussi des lois plus générales qui contiennent des dispositions spécifiques à la protection données par exemple en droit de la santé.

Tandis que les lois suivantes concernent plutôt le secteur public :

- *Loi sur la protection des renseignements personnels (Fédéral)*
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Québec)
- *Freedom of Information and Protection of Privacy Act* (Alberta)
- *Freedom of Information and Protection of Privacy Act* (Colombie-Britannique)
- *Loi sur l'accès à l'information et la protection de la vie privée* (Ontario)
- *Loi sur le droit à l'information et la protection de la vie privée* (Nouveau-Brunswick)
- *Access to Information and Protection of Privacy Act* (Terre-Neuve et Labrador)

- *Freedom of Information and Protection of Privacy Act* (Saskatchewan)
- *Loi sur l'accès à l'information et la protection de la vie privée* (Manitoba)
- *Freedom of Information and Protection of Privacy Act* (Nouvelle-Écosse)
- *Freedom of Information and Protection of Privacy Act* (Île-du-Prince-Édouard)

Afin de présenter ce cadre légal de manière utile à l'élaboration de politiques de confidentialité, nous avons donc fait le choix de détailler les principes juridiques fondateurs de la protection des renseignements personnels ainsi que les droits individuels qui en découlent en étudiant principalement la Loi québécoise sur le secteur privé, ainsi que la Loi fédérale sur le secteur privé. En effet, il existe des invariants normatifs, à savoir des principes équivalents qui produisent les mêmes effets, dans toute cette législation et ceux-ci seront identifiés dans le cadre de l'élaboration des politiques de confidentialité.

Application du droit :

Les lois québécoises en matière de protection des renseignements personnels sont plus anciennes et plus complètes que la loi fédérale. À quelques exceptions près, la Loi québécoise sur le secteur privé a préséance sur la Loi fédérale sur le secteur privé au Québec[8]. Au cours de notre analyse, nous n'avons pas étudié les lois de l'Alberta et de la Colombie-Britannique, qui elles aussi ont préséance sur la loi fédérale, en raison des invariants dans toutes ces législations et de leur qualification de lois essentiellement similaires à la Loi fédérale sur le secteur privé par le Commissariat à la protection de la vie privée du Canada.

Québec

La Loi québécoise sur le secteur privé est une loi qui a vocation à s'appliquer à l'égard des renseignements personnels qu'une entreprise privée, dont les activités se déroulent entièrement au Québec, recueille, détient, utilise ou communique à des tiers, et ce, quelle que soit la nature du support et la forme sous laquelle ils sont accessibles : écrite, graphique, sonore, visuelle, informatisée ou autre. Toutefois elle ne s'applique pas à la collecte, la détention, l'utilisation ou la

[8] Décret d'exclusion visant des organisations de la province de Québec (DORS/2003-374)

communication de matériel journalistique, historique ou généalogique à une fin d'information légitime du public.

Concernant les organismes à but non lucratif (OBNL), la Loi québécoise sur le secteur privé s'applique[9], en ce sens qu'ils exercent une « *activité économique organisée, qu'elle soit ou non à caractère commercial* »[10].

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « Loi québécoise sur le secteur public ») est une loi qui a vocation à s'appliquer aux documents détenus par un organisme public québécois dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public ou par un tiers. Elle s'applique quelle que soit la forme de ces documents : écrite, graphique, sonore, visuelle, informatisée ou autre.

Fédéral

La Loi fédérale sur le secteur privé est une loi qui a vocation à s'appliquer à toute organisation qui recueille, utilise ou communique des renseignements personnels dans le cadre de ses activités commerciales à l'exclusion des institutions fédérales sujettes à la *Loi sur la protection des renseignements personnels* (ci-après « Loi fédérale sur le secteur public »). Les organisations dont le traitement des données s'effectue au Québec en Alberta ou en Colombie-Britannique sont exemptées d'appliquer la Loi fédérale sur le secteur privé car des lois provinciales s'y substituent. Par ailleurs, celle-ci ne s'applique pas aux renseignements personnels recueillis, utilisés ou communiqués par une organisation à des fins strictement journalistiques, artistiques ou littéraires.

La Loi fédérale sur le secteur public a vocation à s'appliquer aux organismes publics fédéraux et régit la collecte, l'utilisation et la communication des renseignements personnels par le gouvernement dans le cadre de la prestation de services. Toutefois cette loi ne concerne ni Synapse C, ni les organismes dont elle souhaite mutualiser et valoriser les données.

[9] Loi québécoise sur le secteur privé, Art. 1
[10] CCQ, Art. 1525

En principe les organismes à but non lucratif ne sont pas assujettis à la Loi fédérale sur le secteur privé, toutefois la loi fédérale s'applique aux OBNL, à l'exception des OBNL des provinces du Québec, de l'Alberta et de la Colombie-Britannique, qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales. À la lecture des informations transmises par Synapse C, les OBNL provinciales, à l'exception des OBNL des provinces du Québec, de l'Alberta et de la Colombie-Britannique, dont les données seront mutualisées et valorisées, récoltent principalement des renseignements personnels dans le cadre de leurs activités commerciales, ce qui ne les dispense pas des obligations issues de la Loi fédérale sur le secteur privé. En effet, selon la Loi, une activité commerciale comprend : « *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* ».

Tout au long de la rédaction de ce guide de bonnes pratiques, nous avons pris le parti de nous fonder principalement sur la loi québécoise dont les obligations sont plus complètes que la loi fédérale, ce qui implique que tout organisme canadien[11] se conformant aux obligations de la loi québécoise sera en règle avec la loi fédérale. En effet, en raison de l'invariance des principes et obligations touchant à la protection des renseignements personnels, la loi québécoise a été jugée comme essentiellement similaire[12] par le Commissariat à la protection de la vie privée du Canada.

Les principes clés qui doivent s'appliquer à tout traitement de renseignements personnels :

- **La transparence** : En vertu du principe de transparence, les lois sur la protection des renseignements personnels exigent que les organisations documentent et mettent à la disposition des personnes, sous une forme globalement compréhensible, des renseignements précis sur leurs politiques et pratiques en matière de gestion des

[11] À l'exception des organismes des provinces de l'Alberta et de la Colombie-Britannique dont nous n'avons pas étudié les lois

[12] Les lois essentiellement similaires fournissent un mécanisme de protection des renseignements personnels conforme et équivalent à celui de la Loi fédérale sur le secteur privé, intègrent les dix principes de l'annexe 1 de la Loi fédérale sur le secteur privé, fournissent un mécanisme indépendant et efficace de surveillance et de recours ainsi que des pouvoirs d'enquête et restreignent la collecte, l'utilisation et la communication des renseignements personnels à des fins appropriées et légitimes.

renseignements personnels. Les lois québécoises viennent quant à elles préciser quelles sont les informations qui doivent être fournies dans le cadre de la récolte de renseignements personnels par un organisme public[13] ainsi que dans le cadre de la constitution d'un dossier sur une personne dans le secteur privé[14].

- **La base légale de tout traitement des renseignements personnels** : Les organisations doivent obtenir le consentement des personnes concernées pour la collecte, l'utilisation et la communication de renseignements personnels, sous réserve d'exceptions limitées. Pour que le consentement soit valide, il doit être manifeste, libre et éclairé et être donné à des fins spécifiques[15]. Il doit donc être raisonnablement attendu que les personnes concernées comprennent la nature, le but et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquels elles ont consenti. Une organisation n'exige pas, comme condition de la fourniture d'un produit ou d'un service, un consentement autre que celui qui est nécessaire à la réalisation d'un objectif explicitement spécifié et légitime. La forme du consentement (explicite ou implicite) peut varier selon la nature des renseignements et les attentes raisonnables de la personne. Les personnes peuvent retirer leur consentement en tout temps, sous réserve de restrictions légales ou contractuelles et d'un préavis raisonnable. La loi fédérale prévoit une obligation générale selon laquelle les renseignements personnels doivent être recueillis par des moyens justes et licites : le consentement ne doit pas être obtenu par tromperie, coercition ou pratiques trompeuses. Même avec un consentement valide, les organisations sont assujetties à une exigence juridique générale selon laquelle les renseignements personnels ne peuvent être recueillis, utilisés et communiqués qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

- **La limitation de l'objet** : Les organisations sont généralement tenues de préciser les fins auxquelles les renseignements personnels sont recueillis au moment même de la récolte ou antérieurement à celle-ci[16]. Les organisations doivent également documenter ces fins conformément au principe de transparence.

[13] Loi québécoise sur le secteur public, Art. 65.
[14] Loi québécoise sur le secteur privé, Art. 8.
[15] Loi québécoise sur le secteur privé, Art. 14.
[16] Loi québécoise sur le secteur privé, Art. 4 et 5, Loi québécoise sur le secteur public, Art. 65.

L'obligation d'identifier les raisons qui conduisent à une collecte de renseignements personnels permettra par la suite :

- de délimiter le type et le nombre de renseignements personnels à recueillir;
- d'informer la personne concernée des raisons qui justifient la collecte de renseignements;
- de déterminer les mesures de sécurité à adopter pour assurer la protection des renseignements personnels;
- de déterminer la fréquence de leur mise à jour;
- de limiter leur utilisation;
- de fixer, à terme, le moment de leur destruction

Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles pour lesquelles ils ont été recueillis, sauf avec le consentement de la personne concernée ou si la loi l'exige.

- **Le principe de nécessité ou minimisation des renseignements personnels :** Les lois québécoises[17] sur la protection des renseignements personnels exigent généralement que la collecte, l'utilisation et la communication des renseignements personnels soient limitées (tant par leur nature que par leur volume) dans la mesure où elles sont nécessaires pour réaliser les fins déterminées par l'organisation. Les renseignements personnels ne doivent pas être conservés plus longtemps que nécessaire pour réaliser ces fins.

- **Le principe de proportionnalité :** Les lois québécoises sur la protection de la vie privée énoncent généralement l'obligation primordiale selon laquelle les organisations ne peuvent recueillir, utiliser et communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. Le principe de proportionnalité est également intégré dans certains des autres principes. Par exemple, l'obligation de conservation imposée aux organisations est proportionnelle au niveau de sensibilité du renseignement personnel, plus ce dernier est sensible, plus le niveau de protection requis sera élevé[18]. De même, la mesure dans laquelle les

[17] Loi québécoise sur le secteur privé, Art. 5., Loi québécoise sur le secteur public, Art. 64.
[18] Loi québécoise sur le secteur privé, Art. 10, Loi québécoise sur le secteur public, Art. 63.1

renseignements personnels doivent être exacts, complets et à jour dépendra de l'utilisation qui en sera faite, compte tenu des intérêts de l'individu.

- **La conservation des renseignements personnels :** Conformément au principe de nécessité, les lois québécoises[19] sur la protection des renseignements personnels exigent généralement que les organisations ne conservent les renseignements personnels qu'aussi longtemps que nécessaire pour atteindre les fins pour lesquelles ils ont été recueillis, sous réserve d'une exigence légale valide.

  Les renseignements personnels qui ne sont plus nécessaires aux fins déterminées devraient être détruits, effacés ou rendus anonymes.

  Les organisations devraient élaborer des lignes directrices et mettre en œuvre des procédures pour la conservation des données à caractère personnel, y compris des périodes minimales et maximales de conservation et des procédures régissant la destruction des données.

- **La responsabilisation :** Les lois[20] sur la protection des renseignements personnels reflètent le principe clé de la responsabilisation. Les organisations sont responsables de la protection des renseignements personnels sous leur contrôle, y compris les renseignements personnels qu'elles transfèrent à des tiers pour traitement, pour lesquels elles doivent assurer un niveau comparable de protection par des moyens contractuels ou autres.

  Les organisations doivent désigner et identifier une personne responsable de la conformité de l'organisation aux autres principes de protection de la vie privée et doivent mettre en œuvre des politiques et des pratiques pour donner effet à ces principes.

- **La protection** : Chacune des lois québécoises[21] et fédérales[22] sur la protection des renseignements personnels contient des dispositions particulières relatives à la protection de ces derniers. Essentiellement, ces dispositions exigent que les organisations mettent

[19] Loi québécoise sur le secteur privé, Art. 12 et 36. Loi québécoise sur le secteur public, Art. 52.1.
[20] Loi québécoise sur le secteur public, Art. 8. Loi québécoise sur le secteur privé, Art. 91.
[21] Loi québécoise sur le secteur privé, Art. 10. Loi québécoise sur le secteur public, Art. 63.1.
[22] Loi fédérale sur le secteur privé, Art 5.

en œuvre des mesures techniques, physiques et administratives raisonnables pour protéger les renseignements personnels contre la perte ou le vol, ainsi que contre l'accès, la divulgation, la copie, l'utilisation, la modification ou la destruction non autorisés. Notamment au Québec, chaque organisme a la responsabilité d'assurer le caractère confidentiel des renseignements personnels qu'il détient. À cette fin, il doit désigner un responsable de l'accès aux documents et de la protection des renseignements personnels, dont l'identité devra être divulguée à la Commission d'Accès à l'Information.

- **L'exactitude :** Les organisations sont tenues de s'assurer que les renseignements personnels contenus dans leurs dossiers sont exacts, complets et à jour, en particulier lorsque les renseignements sont utilisés pour prendre une décision concernant la personne à qui ils se rapportent ou sont susceptibles d'être communiqués à une autre organisation[23].

Les droits individuels à garantir dans le cadre d'un traitement de renseignements personnels :

Il va sans dire que l'organisation collectant des renseignements personnels a l'obligation d'informer adéquatement la personne concernée avant qu'elle les fournisse. Lorsque cette obligation d'information est remplie par l'organisme, celui-ci peut se trouver confronté à divers droits que la personne souhaiterait exercer :

- **Droit d'accès aux données/copies de renseignements personnels :** Les organisations doivent, sur demande et sous réserve d'exceptions limitées, informer les personnes de l'existence, de l'utilisation et de la divulgation de leurs renseignements personnels et leur donner accès à ces renseignements, y compris une liste des organisations tierces auxquelles les renseignements ont été communiqués[24].

  Le droit d'accès n'oblige pas une organisation à fournir des copies des dossiers de renseignements personnels ; il exige plutôt la fourniture d'accès, ce qui peut inclure la

[23] Loi québécoise sur le secteur privé, Art. 11. Loi québécoise sur le secteur public, Art. 72.
[24] Loi québécoise sur le secteur privé, Art. 27 et 35. Loi québécoise sur le secteur public, Art. 9 et 92.

consultation des dossiers dans les bureaux de l'organisation. En général, la demande d'une personne doit être suffisamment précise pour permettre à une organisation d'identifier les documents pertinents. L'organisation doit répondre dans un délai prescrit ou dans un délai raisonnable, selon le cas, à un coût minime ou nul pour l'individu, et doit rendre l'information disponible sous une forme généralement compréhensible. Les exceptions au droit d'accès varient d'une loi à l'autre et doivent être examinées avec soin. Voici des exemples d'exemptions prévues par la loi : les renseignements protégés par le secret professionnel de l'avocat ou le privilège relatif au litige, les renseignements commerciaux confidentiels, les renseignements concernant une autre personne, les renseignements relatifs à des questions de sécurité nationale et les renseignements obtenus dans le cadre d'un processus officiel de règlement des différends.

- **Droit de rectification des erreurs :** La Loi québécoise sur le secteur privé[25] et la Loi fédérale sur le secteur privé[26] exigent généralement que lorsqu'une personne démontre l'inexactitude ou le caractère incomplet des renseignements personnels détenus par une organisation, celle-ci doit corriger les inexactitudes et/ou ajouter une note aux renseignements, le cas échéant.

- **Droit d'opposition au traitement :** Bien que la Loi fédérale sur le secteur privé ne prévoit pas de droit spécifique de s'opposer au traitement, la Loi québécoise sur le secteur privé[27] interdit aux organisations d'exiger, comme condition à la fourniture d'un produit ou d'un service, que les personnes donnent leur consentement à la collecte, à l'utilisation ou à la communication de leurs renseignements personnels au-delà de ce qui est nécessaire pour atteindre le but légitime et explicitement spécifié. De plus, une personne doit pouvoir retirer son consentement en tout temps, sous réserve de restrictions légales ou contractuelles et d'un préavis raisonnable. Dès réception de tout retrait, les personnes doivent être informées des conséquences d'un tel retrait.

[25] Loi québécoise sur le secteur privé Art. 8, Art. Loi québécoise sur le secteur public, Art. 89.
[26] Loi fédérale sur le secteur privé, Annexe, Neuvième principe
[27] Loi québécoise sur le secteur privé, Art. 9.

- **Droit de retirer son consentement :** Une personne doit pouvoir retirer son consentement en tout temps, sous réserve de restrictions légales ou contractuelles et d'un préavis raisonnable. Les personnes doivent être informées des conséquences d'un tel retrait.

- **Droit de s'opposer à la commercialisation :** Le consentement est requis pour la collecte, l'utilisation ou la communication de renseignements personnels à des fins de marketing. La forme de consentement requise variera selon les circonstances, la sensibilité des renseignements et les attentes raisonnables de la personne. Dans les cas où le consentement négatif est approprié, les personnes doivent être informées des fins de commercialisation au moment de la collecte ou avant, et d'une manière claire et compréhensible. Les personnes doivent pouvoir se retirer facilement de la pratique ; le retrait doit prendre effet immédiatement et être persistant ; et les renseignements recueillis et utilisés doivent être détruits ou effectivement dépersonnalisés dès que possible par la suite.

- **Droit de porter plainte auprès de l'autorité ou des autorités compétentes en matière de protection des renseignements personnels :** Les personnes ont le droit de déposer une plainte auprès de l'autorité compétente en matière de protection des renseignements personnels. Auparavant, les personnes doivent être en mesure d'aborder les questions de protection des renseignements personnels avec la personne désignée au sein de l'organisation qui est responsable de la conformité de l'organisation. Les organisations doivent disposer de procédures faciles d'accès et d'utilisation pour répondre aux plaintes ou aux demandes de renseignements et doivent prendre des mesures pour traiter efficacement les plaintes en conséquence.

3 - Transmission d'information à des tiers

Dans sa mission de support, Synapse C est amenée à valoriser des données des organismes qu'elle supporte du secteur de la culture au Canada, notamment via la mutualisation ou par le biais d'analyse diverses. Ces données contiennent probablement des renseignements personnels. À cette fin, il est important pour les organismes de prévoir dans leurs politiques de confidentialité la possibilité de transmettre les renseignements personnels à Synapse C à des fins définies par l'organisme, avec l'aide de Synapse C.

En matière de protection des renseignements personnels, Synapse C sera considéré comme un tiers. Pour que les traitements, effectués par Synapse C pour le compte des organismes culturels, soient légaux, il est primordial que la transmission d'informations contenant des renseignements personnels suive les obligations contenues dans la loi.

Il semble pertinent de rappeler ici que toute transmission d'information à l'extérieur du Québec ou provenant de l'extérieur du Québec assujettit la transmission au droit fédéral.

Au Québec, il est possible de transférer des renseignements personnels à des tiers, à condition d'obtenir le consentement de la personne concernée ou que la loi l'autorise[28]. La loi sur le secteur privé donne quelques exceptions à la nécessité d'obtenir le consentement de la personne concernée avant transmission à un tiers[29].

Par ailleurs si les renseignements personnels sont communiqués à une personne ou organisme à l'extérieur du Québec ou qu'ils lui sont confiés pour la détention, l'utilisation ou la communication, l'organisme qui transmet ceux-ci doit préalablement s'assurer :

- que les renseignements ne seront pas utilisés à des fins non pertinentes à l'objet du dossier ni communiqués à des tiers sans le consentement des personnes concernées[30] ;
- dans le cas de listes nominatives, que les personnes concernées aient une occasion valable de refuser l'utilisation des renseignements personnels les concernant à des fins

[28] Loi québécoise sur le secteur privé Art. 13 et 17
[29] Loi québécoise sur le secteur privé Art. 18, 18.1, 22, 23
[30] A l'exception des cas prévus aux articles 18 et 23 de la Loi québécoise sur le secteur privé

de prospection commerciale ou philanthropique et de faire retrancher, le cas échéant, ces renseignements de la liste.

Si l'une des deux conditions n'est pas remplie, l'organisme doit refuser de transmettre les renseignements personnels.

Au fédéral, les organisations qui communiquent des informations contenant des renseignements personnels à des tiers pour fin de traitement, restent responsables de ceux-ci. Par ailleurs, elles doivent s'assurer que le tiers offre un degré de protection comparable à celui de l'organisme[31].

Par ailleurs, les organisations doivent aviser les consommateurs, au moment de la collecte, que leurs renseignements personnels pourraient être traités dans un pays étranger[32].

4 - Vers une protection maximale

Les entreprises québécoises et canadiennes du secteur de la culture, par leurs clientèles, leurs potentiels sous-traitants ou le traitement de données de personnes résidant en UE ou en Californie, peuvent se voir assujetties au *Règlement Général sur la Protection des Données de l'Union Européenne*[33] (ci-après « Règlement européen ») ou encore à la *Loi californienne sur la protection des données personnelles*[34]. C'est pourquoi il est important de prendre en compte certains principes issus de ces lois, afin de s'assurer une meilleure protection des données personnelles et une tranquillité d'esprit, notamment lorsque sont traitées les données personnelles de résidents européens ou californiens. De plus, bien que non explicitement énoncés dans les lois québécoise et fédérale aujourd'hui, certains droits garantis par le Règlement européen et la loi californienne pourraient se voir intégrés au droit québécois et/ou fédéral à l'avenir, car les principes qui les fondent sont similaires, voire parfois identiques.

[31] Loi fédérale sur le secteur privé, Article 4.1.3
[32] Lignes directrices sur le Traitement transfrontalier des données personnelles
[33] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, L 119/1, 4 mai 2016.
[34] *California Consumer Protection Act of 2018*, No. 17-0039.

C’est le cas par exemple du droit à la portabilité des données ou encore du droit à l’oubli, tous deux consacrés par le Règlement européen. L’objectif affiché par le législateur européen sur ces questions est de rendre aux individus la “maîtrise” de leurs données.

Droit à la portabilité des données : Bien que les lois québécoise et fédérale sur le secteur privé prévoient un droit d'accès aux renseignements personnels, elles ne prévoient pas le droit à la transférabilité des données. Le droit à la portabilité offre aux personnes la possibilité de récupérer une partie de leurs données dans un format ouvert et lisible par machine. Elles peuvent ainsi les stocker ou les transmettre facilement d’un système d’information à un autre, en vue de leur réutilisation à des fins personnelles.

Droit à l'effacement / droit à l'oubli : Bien que les lois accordent aux individus le droit de retirer leur consentement et de contester l'exactitude, l'intégralité et l'actualité de leurs données personnelles, elles n'accordent pas un droit spécifique d'exiger des organisations qu'elles "effacent" ou suppriment leurs renseignements personnels *en soi*.

La réutilisation des données :

Les données sont une forme de capital qui ne peut être épuisé et qui peut être réutilisé à des fins théoriquement illimitées. Sa réutilisation dans l'ensemble de l'économie a des retombées bénéfiques, les données pouvant potentiellement être réutilisées pour ouvrir d'importantes possibilités de croissance ou pour générer des avantages d'une manière qui n'était pas prévisible lorsque les données ont été créées. Cela souligne le rôle des données en tant qu’infrastructure clé pour les économies du savoir du XXIe siècle, une infrastructure à laquelle l'accès sera une question de politique sociale et économique cruciale.

Malgré des preuves croissantes de ses avantages économiques et sociaux, la réutilisation des données entre les organisations, les secteurs et les pays reste en deçà de son potentiel, car les individus, les entreprises et les gouvernements sont souvent confrontés à des obstacles à la réutilisation des données qui peuvent être aggravés par la réticence à partager. Les risques sociaux et économiques associés à la révélation éventuelle d'informations confidentielles (c'est-

à-dire de certaines données personnelles et de secrets commerciaux) sont souvent indiqués comme la principale raison de cette réticence à partager.

L'amélioration de l'accès aux données est considérée comme un moyen efficace de maximiser la valeur sociale et économique des données, tout en relevant les risques et les défis liés à l'accès aux données et à leur réutilisation. C'est pourquoi il est important que les organisations qui mettent en place des politiques de confidentialité et qui souhaiteraient que des société tierces telles que Synapse C puissent analyser ces données afin d'améliorer l'efficacité et les synergies dans le secteur de la culture à Montréal, au Québec et au Canada, doivent prévoir autoriser le transfert de données vers ces tiers dans leurs politiques de confidentialité.

5 - Recommandations

Il est recommandé aux organismes, dont des sociétés tierces telles que Synapse C souhaiteraient traiter les données aux fins d'amélioration de la collecte et de l'analyse des données dans le secteur de la culture canadien, de suivre les recommandations suivantes lors de la collecte, de l'utilisation et de la communication des renseignements personnels, mais également lors des demandes d'accès à ces derniers.

Tel que mentionné précédemment, la plupart de ces recommandations sont tirées de la Loi québécoise sur le secteur privé qui est plus protectrice des renseignements personnels que la loi fédérale, par ailleurs jugée essentiellement similaire à la Loi québécoise sur le secteur privé. Il semblerait qu'il existe toutefois une exception intéressant Synapse C, relativement à la transmission d'information à des tiers[35].

[35] Si Synapse C reçoit des informations provenant de tiers d'autres provinces, ces organismes seront aussi responsable que Synapse C des renseignements personnels et doivent s'assurer que Synapse C offre une protection au moins égale aux organismes. Lorsque les informations contenant des renseignements personnels seront envoyées par Synapse C à des tiers hors du Québec, Synapse C devra également s'assurer que la protection des renseignements personnels effectuée par les tiers soit au moins comparable à celle offerte par Synapse C, qui restera par ailleurs responsable des renseignements personnels transmis aux tiers.

De plus, avant la lecture des diverses recommandations, nous souhaiterions attirer l'attention des lecteurs de ce guide de bonnes pratiques sur le fait qu'il soit fortement recommandé de ne pas utiliser ou communiquer des renseignements personnels précédemment collectés au risque d'être en contravention des diverses lois de protection des renseignements personnels. Les seuls cas où les organisations pourraient continuer leurs traitements de données personnelles collectées par le passé seraient les cas où les politiques de confidentialité antérieures le permettaient déjà.

Voici dix principes tirés de l'annexe I de la Loi fédérale sur le secteur privé, repris et distillés au sein des lois québécoises, qui permettront aux organismes et aux fournisseurs tels que Synapse C d'avoir une compréhension plus large de leurs **obligations concernant les renseignements personnels** qu'ils seraient amenés à collecter au cours de leurs activités :

1. L'organisme est responsable des renseignements personnels qu'il gère. Il doit nommer une personne en charge de la conformité.

2. Détermination des fins (objectifs) de la collecte des renseignements préalablement à leur collecte et tout au long de celle-ci. Il ne faut pas collecter des renseignements personnels autrement que pour ces fins.

3. Obtenir le consentement de toute personne pour la collecte, l'utilisation et/ou communication de renseignements personnels qui la concernent.

4. La collecte doit procéder de façon honnête et licite.

5. Limitation de l'utilisation, de la communication et de la conservation des renseignements personnels.

6. Les renseignements personnels collectés doivent être aussi exacts et à jour que possible.

7. Les renseignements personnels collectés doivent être sécurisés selon leur degré de sensibilité.

8. Les informations sur les politiques et les pratiques de l'organisme concernant sa gestion des renseignements personnels doivent être facilement accessibles au public.

9. L'accès à ses renseignements personnels doit être offert à toute personne qui en fait la demande. Doivent aussi être divulgués l'usage qui en est fait et s'ils ont été communiqués à des tiers. La personne doit pouvoir contester l'exactitude et l'intégralité des renseignements qui la concernent et y faire apporter les corrections appropriées.

10. Toute personne doit pouvoir se plaindre du non-respect par une organisation des principes énoncés ci-dessus. La plainte doit être adressée au responsable de la conformité (c.f. Principe 1).

En ce qui concerne le sujet qui nous intéresse plus précisément, la Commission d'accès à l'information du Québec a publié un *Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information*[36] dans lequel elle a donné plusieurs conseils afin **d'améliorer les politiques de confidentialité en ligne et la transparence des pratiques en matière de collecte des renseignements personnels et de protection de la vie privée** pour les organismes qui sont assujettis à la québécoise. En outre, le Commissariat de Protection de la Vie Privée du Canada a lui aussi émis des recommandations similaires. À notre avis, ces conseils ont vocation à s'appliquer plus largement aux diverses entités collectant des données à caractère personnel dans le secteur de la culture. Par ailleurs, nous encourageons les organisations à envisager l'adoption de politiques de confidentialité normalisées, faciles à comprendre par tous.

1. Avoir une politique de confidentialité adaptée aux activités du secteur culturel :
    a. Bien que les politiques de confidentialité d'autres organisations puissent être utiles comme référence, il faut éviter de copier/coller des modèles existants d'entreprises pratiquant dans un secteur d'activité différent.
    b. Décrire le type de renseignements personnels collectés par l'entité

[36] Gouvernement du Québec, 2002, mis à jour en 2015, en ligne : http://www.cai.gouv.qc.ca/documents/CAI_G_dev_syst_info_pub.pdf

2. Être précis et transmettre des informations utiles :
    a. Pas de superflus ou termes vagues
    b. Indiquer clairement les renseignements personnels qui sont recueillis et à quelle fin
    c. Indiquer clairement si les renseignements personnels recueillis sont transmis à des tiers, quels sont ces tiers et quels sont les services qu'ils fournissent nécessitant la transmission des renseignements personnels

3. Ne pas se contenter de préciser que l'on utilise des témoins (cookies)
    a. Expliquer comment les témoins fonctionnent (données recueillies) et quelle est leur utilisation / communication à des tiers
    b. Renseigner aussi sur les pratiques en magasin

4. Présenter les options offertes aux clients, utilisateurs ou autres personnes concernées en matière de protection de la vie privée
    a. Renseigner les clients, utilisateurs ou autres personnes concernées sur les options offertes par l'entité concernant la collecte, l'utilisation ou la communication de leurs renseignements (p. ex. refus que leurs renseignements personnels soient utilisés à des fins de marketing)
    b. Expliquer clairement comment ils peuvent exercer les choix qui leur sont offerts

5. Expliquer les modalités d'accès aux renseignements personnels détenus
    a. Permettre aux clients, utilisateurs ou autres personnes concernées de demander la correction ou la suppression de ces renseignements

6. Mettre à jour régulièrement l'information concernant la protection des renseignements personnels
    a. S'assurer que la politique de confidentialité et les autres avis reflètent les pratiques actuelles de gestion de la vie privée de l'entité, surtout lorsque de nouveaux traitements ont lieu ou que de nouvelles données sont collectées
    b. S'assurer de bien mettre à jour l'information dès qu'un changement intervient

   c. Indiquer la date de la dernière mise à jour/modification de la politique de confidentialité
   d. Archiver les versions précédentes de la politique de confidentialité

7. Fournir les coordonnées de l'entité
   a. Faciliter la communication avec l'entité, à minima par le biais d'une adresse courriel
   b. Proposer plusieurs façons d'entrer en contact avec l'entité relativement à la protection de la vie privée / protection des renseignements personnels
   c. Rendre ces informations accessibles à d'autres endroits que la seule politique de confidentialité

8. S'assurer que l'information sur la protection des renseignements personnels est visible et facile d'accès
   a. Placer un lien d'accès à la politique de confidentialité à un endroit en évidence sur la page d'accueil
   b. Proposer des points d'informations complémentaires lorsqu'un client doit prendre une décision qui aura un impact sur sa vie privée / renseignements personnels
   c. Mettre en évidence les informations clés de la politique de confidentialité

9. Utiliser un langage clair

10. Structurer la politique de confidentialité de manière à faciliter la consultation par les utilisateurs

Bien que cela puisse parfois sembler logique, il semble bon d'insister sur le fait que les collectes, **les traitements et les transferts de renseignements personnels effectués aux fins suivantes sont interdits** :

- recueillir, utiliser ou communiquer des renseignements personnels de manière illégale ou en commettant des actes illégaux;
- faire du profilage (classement/tri) de personnes de manière à permettre un traitement inéquitable, non éthique ou discriminatoire;

- recueillir, utiliser ou communiquer des renseignements personnels qui laisseraient paraître l'intention ou permettraient de causer des préjudices graves pour une personne;
- publier des renseignements personnels avec l'intention de faire pression sur la personne par la suite;

Pour conclure, Synapse C a fait part au Laboratoire de cyberjustice de sa volonté d'avoir un consentement éclairé de la part des utilisateurs ou clients des organismes. En effet, le consentement est essentiel lors de la collecte de renseignements personnels d'individus. En principe, **le consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel** doit être manifeste, libre, éclairé et être donné à des fins spécifiques[37]. C'est une valeur phare des lois québécoises et fédérales portant sur le sujet.

Voici sept principes, produits conjointement par le Commissariat à la protection de la vie privée du Canada et les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, afin que les organisations s'assurent d'obtenir un consentement valable durant la collecte, l'utilisation et la transmission des renseignements personnels :

1. Mettre l'accent sur les éléments clés de la collecte, l'utilisation et de la communication à des tiers des renseignements personnels. L'information doit être claire, facilement accessible et ne pas être en surabondance, ce qui risquerait de perdre l'utilisateur. La personne qui donne son consentement doit comprendre la nature, les fins et les conséquences de ce à quoi elle consent.

   Pour que le consentement soit considéré comme valable, les organisations doivent informer les personnes de leurs pratiques de protection de la vie privée et de gestion des renseignements personnels de manière détaillée et en des termes faciles à comprendre. les organisations doivent permettre aux individus d'examiner rapidement les éléments clés qui auront une incidence sur leur décision en matière de protection des renseignements personnels au départ lorsqu'ils envisagent d'utiliser le produit ou le service offert, de faire un achat, de télécharger une application, etc.

   Voici des éléments clés que les organismes doivent communiquer aux personnes :

[37] Loi québécoise sur le secteur privé, Art. 14

- Les renseignements personnels recueillis ou susceptibles de l'être de manière précise
- Les tiers auxquels les renseignements personnels seront communiqués
- Les fins auxquelles les renseignements personnels seront recueillis, utilisés ou communiqués
- Les risques de préjudice et autres conséquences négatives que pourrait avoir la collecte

2. L'information doit être communiquée aux individus de façons gérables et facilement accessibles (possiblement en entonnoir par le biais d'hyperliens apportant une information de plus en plus précise), et ceux-ci devraient avoir la possibilité de déterminer à quel point et quand ils souhaitent obtenir de l'information détaillée.

3. On ne peut pas exiger des individus qu'ils consentent à la collecte, à l'utilisation ou à la communication de renseignements personnels au-delà de ce qui est nécessaire pour fournir le produit ou le service. Ils doivent avoir le choix de consentir ou de ne pas consentir. Ces choix doivent être expliqués clairement, et être facilement accessibles.
   La collecte, l'utilisation et la communication de renseignements personnels sur lesquels un individu n'exerce aucun contrôle (si ce n'est de renoncer à utiliser un produit ou un service) sont appelées « conditions de service ». Pour que la collecte, l'utilisation ou la communication constitue une condition de service valide, elle doit être essentielle à la fourniture de ce produit ou ce service, c'est-à-dire qu'elle est nécessaire pour réaliser les fins légitimes précisées explicitement. Si le lien entre la collecte et la fourniture du service semble faible, l'organisme doit pouvoir l'expliquer.

4. Lorsqu'elles demandent le consentement d'une personne en ligne, les organismes ne doivent pas se contenter de transposer en format numérique les politiques imprimées qu'elles utilisent hors ligne. L'environnement numérique est dynamique par nature et il faut en tirer parti. Les organismes devraient utiliser diverses stratégies de communication concernant la collecte, l'utilisation et la communication des renseignements personnels. Notamment des bulles d'information précisant pourquoi le renseignement personnel est

requis, lorsque l'on doit le saisir en ligne ou encore des hyperliens menant à la section pertinente de la politique de confidentialité ou de gestion des données.

5. Avoir une interface utilisateur graphique afin que la réception de l'information soit simple et compréhensible. Il est notamment peu recommandé de trop segmenter l'information, résultant en un labyrinthe informationnel innavigable pour l'internaute.

6. Faire du consentement un processus dynamique et continu en s'en assurant à plusieurs moments dans le temps. Notamment par le biais d'une foire aux questions mise à jour régulièrement, par le biais de rappels périodiques aux individus ou encore en utilisant de nouvelles technologies de type *chatbot*.

7. Faire preuve de responsabilité en se tenant prêt à démontrer en tout temps sa conformité quant à la validité du consentement d'un utilisateur.

Par ailleurs, Synapse C devra veiller à ce que les organisations dont elle aimerait récolter les données indiquent clairement, dans leurs politiques de confidentialité, quels types de données contenant des renseignements personnels seront communiquées à Synapse C et à quelles fins.

Pour conclure, la création d'une politique de confidentialité n'est qu'une première étape visant à la mise en conformité des organisations culturelles face aux diverses lois de protection des renseignements personnels, ainsi qu'à la possibilité de transfert de données de culture à Synapse C. Dans un second temps, il sera nécessaire que ces organisations se dotent de politiques additionnelles, notamment de sécurité des données et d'archivage.

Si Synapse C en ressent le besoin et qu'IVADO y trouve un certain intérêt, le Laboratoire de cyberjustice est par ailleurs compétent pour rédiger des guides de bonnes pratiques relativement à la sécurité des données et à leur archivage.

[i] Le présent Guide est un instrument d'information uniquement et ne constitue, en aucun cas, un avis ou une opinion juridique. Vous pouvez communiquer avec l'équipe du Laboratoire de cyberjustice pour toutes informations ou questions additionnelles ou pour obtenir des conseils personnalisés.