« Respect de la vie privée » du CCP

Statut du document : Recommandation finale V1.2

Conformément aux procédures opérationnelles du CCIAN, une recommandation finale est un livrable qui représente les conclusions d'un comité d'experts du CCIAN ayant été approuvées par un comité d'experts et ratifiées par un vote des membres bienfaiteurs du CCIAN.

Ce document a été élaboré par le comité d'experts du cadre de confiance du CCIAN avec les commentaires du public recueillis et traités dans le cadre d'un processus ouvert d'examen par les pairs. On s'attend à ce que le contenu de ce document soit examiné et mis à jour régulièrement afin de donner suite à la rétroaction reliée à la mise en œuvre opérationnelle, aux progrès technologiques, et aux changements de lois, règlements et politiques. Les avis concernant les changements apportés à ce document seront partagés sous la forme de communications électroniques, notamment le courriel et les réseaux sociaux. Les notifications seront également consignées dans le programme de travail du Cadre de confiance pancanadien (CCP).

Table des matières

1. Introduction à la composante « Respect de la vie privée » du CCP

Le contenu ici présent concerne un sujet spécifique au domaine de ce composant du Cadre de confiance pancanadien (CPP). La section d'aperçu fournit des informations nécessaires pour une interprétation cohérente des critères de conformité inclus. Pour une introduction générale au CPP, veuillez consulter l'Aperçu du CPP, qui décrit le contexte, le but, la portée, les principes et les objectifs du cadre.

1.1. Raison d’être et avantages anticipés

Le respect de la vie privée est une exigence fondamentale des interactions liées à l’identité numérique. Étant donné cela, tous les participants au Cadre de confiance pancanadien (CCP) sont tenus de suivre des pratiques qui respectent la vie privée. Ces pratiques se fient au principe selon lequel les personnes connaissent et comprennent les détails et éventuels avantages, risques nuisibles et conséquences associés à la gestion de leurs renseignements personnels, et peuvent prendre des mesures en fonction de ces renseignements.

La composante « Respect de la vie privée » du Cadre de confiance pancanadien porte sur le traitement des données personnelles pour les besoins de l’identité numérique. Elle a pour objectif d’assurer l’intégrité permanente des processus, politiques et contrôles des organisations en matière de confidentialité dans un écosystème de l’identité numérique grâce à des critères de conformité uniformisés qui sont utilisés pour l’évaluation et la certification par rapport au Cadre de confiance pancanadien. Les critères de conformité pour la composante « Respect de la vie privée » spécifient les tests qui peuvent être faits pour s’assurer qu’une organisation assume le rôle des organisations divulgatrices et requérantes, des entités chargées du traitement des avis et consentements, des fournisseurs de réseau et l’organe de gouvernance. Les critères de conformité sont conçus pour démontrer que les participants traient les renseignements d’identité numérique conformément aux 10 principes définis à l’annexe 1 de la *Loi sur la protection des renseignements personnels et des documents électroniques* (LPRPDE). La LPRPDE s’applique aux organisations qui traitent des renseignements personnels dans le cadre d’activités commerciales.

Remarque : La série actuelle de critères de conformité est organisée selon les 10 principes de la protection des renseignements personnels figurant dans l’annexe 1 de la LPRPDE[1]; toutefois, ils visent à être appliqués à grande échelle dans les organisations des secteurs privé et public. Il se pourrait que les versions futures de cette composante incorporent des critères de conformité pertinents à d’autres consignes sur la protection de la vie privée (p. ex., respect de la vie privée dès la

conception, modernisation de la LPRPDE) et cadres réglementaires (p. ex., lois fédérales et provinciales sur la protection de la vie privée).

Ces critères de conformité ne remplacent pas les règlements existants; on s'attend à ce que les organisations se conforment aux lois, politiques et règlements pertinents sur la protection de la vie privée dans leur province ou territoire.)

La figure 1 donne un aperçu conceptuel et une organisation logique de la composante « Respect de la vie privée ».

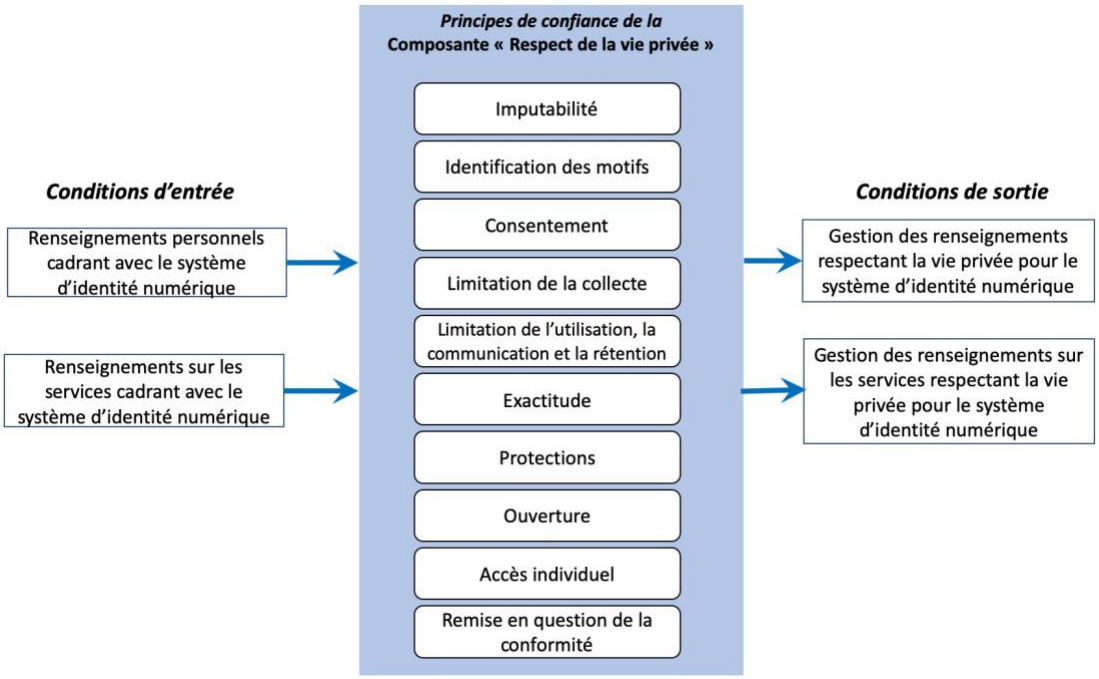

Figure 1. Composante « Respect de la vie privée »

La composante « Respect de la vie privée » est constituée des éléments suivants :

- **Principes de confiance** – ensemble de principes auxquels les organisations (p. ex., organisations divulgatrices, organisations requérantes, entités chargées du traitement des avis et consentements, fournisseurs de réseau) sont censées se conformer lorsqu'elles traitent des renseignements personnels spécifiques à un sujet et à un service dans un système d'identité numérique. Chaque principe de confiance est évalué selon un ensemble de critères de conformité associés à ce principe.
- **Intrants** – ce qui est intégré dans les principes de confiance, p. ex., les renseignements personnels exigeant une gestion de la confidentialité pour agir.

- **Extrants** – ce qui résulte de l'application des principes de confiance, p. ex., les politiques et les contrôles en matière de respect de la vie privée appliqués aux renseignements personnels.

1.2. Portée

La figure 2 illustre la portée de la composante « Respect de la vie privée », qui inclut les fonctions accomplies par les organisations divulgatrice et requérante, et l'entité chargée du traitement des avis et consentements, ainsi que les rôles des fournisseurs de réseau et organes de gouvernance tels que décrits dans la section Rôles.

Dans le contexte du CCP, seuls ceux dont les rôles consistent à traiter des renseignements d'identité numérique dans l'écosystème numérique et qui empêcheront l'accès à ces fins auront normalement accès aux renseignements personnels (tels que définis dans la section Termes et définitions). Les participants qui jouent des rôles dans l'écosystème de l'identité numérique pour favoriser, contrôler et mettre en place des règles visant à faciliter le partage des renseignements personnels ne devraient idéalement (p. ex., à moins que ce ne soit exigé par la loi) pas pouvoir voir, lire ou modifier les renseignements ou y être exposés. L'entité chargée du traitement des avis et consentements, qui remplit des fonctions de contrôle, pourrait être exposée à certains renseignements personnels (compte tenu de la façon dont cette entité est présentée), mais cela devrait être minimisé (selon les critères de conformité pour limiter la collecte LIMC-9).

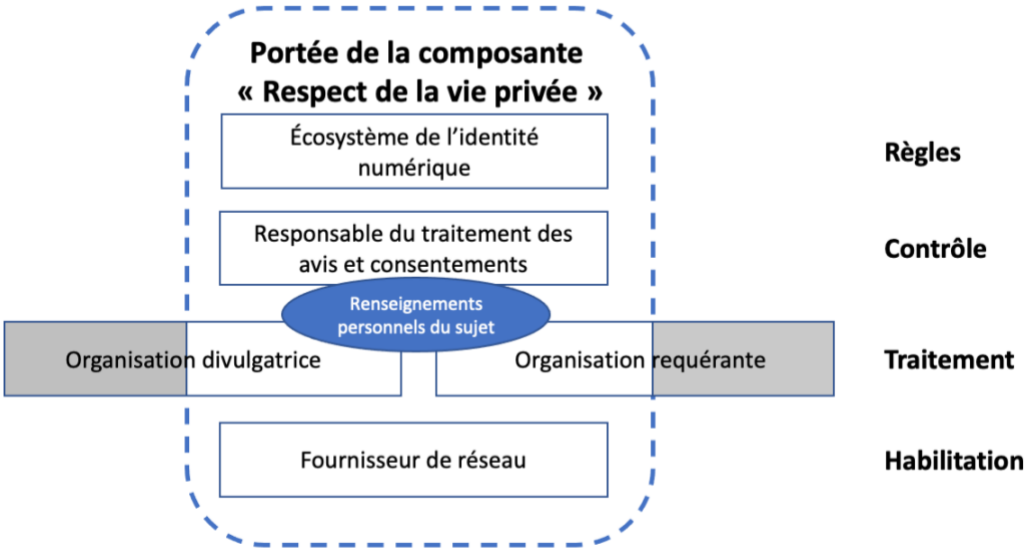

Figure 2. Portée et rôles de la composante « Respect de la vie privée »

1.2.1. Inclus dans la portée

- Dans le contexte du CCP, les exigences en matière de respect de la vie privée s'appliquant aux rôles dans le cadre de l'écosystème de l'identité numérique. Pour voir un aperçu du modèle de CCO et de ses composantes, veuillez vous reporter à l'aperçu du modèle de CCP
- Exigences pour le traitement des renseignements personnels spécifiques au sujet et des renseignements spécifiques aux services associés à l'identité numérique
- Politique et processus reliés à la protection de la vie privée qui s'appliquent à la prestation de l'identité numérique assurée

1.2.2. Exclus de la portée

- Surveillance de la fraude : La composante « Respect de la vie privée » inclut les critères de conformité concernant le signalement des violations de la vie privée et des fraudes pour les rôles spécifiques à la composante « Respect de la vie privée ». Les exigences s'appliquant à une surveillance plus générale et au signalement de la fraude, et les mesures à prendre dans le cadre de l'écosystème de l'identité numérique imposent de poursuivre l'étude et le développement dans le contexte du Cadre de confiance pancanadien. Pour obtenir des références, veuillez consulter les critères suivants :
    - Base - BASE 6
    - Organe de gouvernance - ACCO 2
    - Entité chargée du traitement de l'avis et du consentement - CONS-21
- Exigences connexes spécifiques abordées dans d'autres profils du Cadre de confiance pancanadien (p. ex. autorité déléguée, section « Respect de la vie privée et sécurité » du profil de conformité « Organisation vérifiée », exigence SOUR-01 dans le profil de conformité « Personne vérifiée »)
- Les critères de conformité de base (voir BASE dans le profil de conformité « Respect de la vie privée ») ne couvrent pas les cas d'utilisation où le sujet agit comme organisation divulgatrice
- La variation des critères dépend des niveaux d'assurance : Le CCIAN travaille en ce moment sur les particularités du cadre de niveau d'assurance à appliquer. Le travail est arrivé à une maturité suffisante pour être reflété dans certains profils, mais on a jugé que d'autres détails étaient nécessaires pour définir des variations dans les critères pour la composante « Respect de la vie privée »

1.3. Relation avec le Cadre de confiance pancanadien

Le CCP consiste en une série de composantes modulaires ou fonctionnelles qui peuvent être évaluées et certifiées indépendamment pour être prises en considération en tant de composantes de confiance. Le CCP, qui tire parti d'une approche pancanadienne, permet aux secteurs public et privé de collaborer pour préserver les identités numériques en uniformisant les processus et les pratiques à l'échelle de l'écosystème canadien de l'identité numérique.

La figure 3 illustre les composantes du Cadre de confiance pancanadien. La composante « Respect de la vie privée » englobe toutes les sous-composantes (c.-à-d. les préoccupations reliées au respect de la vie privée s'appliquent aux éléments de tous les profils du CCP).

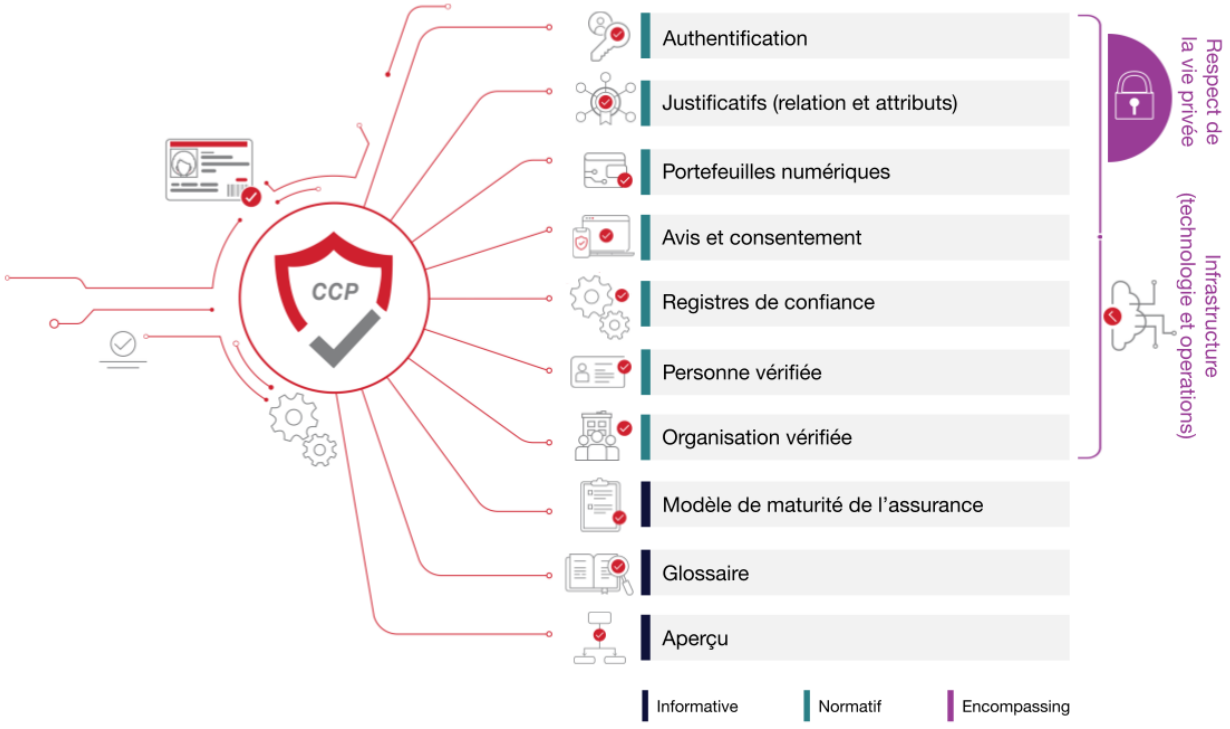

Figure 3. Composantes du Cadre de confiance pancanadien

Les critères de conformité du CCP ne remplacent ou n'annulent pas les règlements existants; on s'attend à ce que les organisations et les particuliers se conforment aux lois, politiques et règlements pertinents dans leur province ou territoire.

2. Conventions de la composante « Respect de la vie privée »

Cette section décrit et définit les principaux termes et notions utilisés dans la composante « Respect de la vie privée » du CCP. Ces renseignements sont fournis pour assurer une utilisation et une interprétation uniformes des termes employés dans cet aperçu et le profil de conformité « Respect de la vie privée » du CCP.

2.1. Termes et définitions

La composante « Respect de la vie privée » fait référence aux termes et définitions figurant dans le glossaire du CCP, et elle utilise spécifiquement les termes et définitions qui suivent :

Sujet

Personne, organisation ou machine qui détient ou est en voie de détenir une représentation numérique dans l'écosystème de l'identité numérique réglementé par le CCP, et qui peut être assujetti aux lois, politiques et règlements à l'intérieur d'un contexte. (Remarque : L'autorité déléguée n'est pas couverte dans le présent document).

Utilisateur

Personne qui est soit le sujet soit autorisée à représenter le sujet et qui accède intentionnellement à un service ou un programme numérique.

Avis

Déclaration qui est formulée pour décrire la collecte, l'utilisation et la divulgation des renseignements personnels, et présentée à un utilisateur. On parle aussi de formulaire de consentement ou de déclaration d'avis.

Consentement

Permission, donnée par un utilisateur autorisé à le faire, de partager des renseignements identitaires et/ou personnels sur un sujet conformément aux modalités définies dans un avis. Dans le contexte du CCP, le consentement équivaut à un « consentement valable » tel que décrit par le Commissariat à la protection de la vie privée du Canada et la LPRPDE. On parle aussi de décision de consentement.

À moins de déclaration explicite, le consentement dans la composante « Respect de la vie privée » fait référence au consentement express ou explicite à partager des renseignements personnels, le sujet devant agir pour donner son consentement. Un consentement implicite, le cas échéant, sera identifié comme tel dans les critères.

Renseignements personnels

En règle générale, les renseignements personnels sont définis comme suit : « Aux termes de la LPRPDE, les renseignements personnels incluent les renseignements factuels ou subjectifs, enregistrés ou non, à propos d'une personne identifiable ». Pour les besoins du présent document, nous définissons deux types de renseignements personnels :

- **Renseignements spécifiques aux services –** Renseignements recueillis ou générés par les participants (organisation divulgatrice, organisation requérante, entité(s) chargée(s) de traiter les avis et consentements, ou fournisseur de réseau) afin d'exploiter et de maintenir le service (p. ex., pseudonymes spécifiques aux services, dossiers de transactions, preuves de transactions incluant le consentement). Dans certains cas, les renseignements spécifiques aux services peuvent être partagés, avec le consentement du sujet.
- **Renseignements personnels spécifiques au sujet –** Renseignements factuels ou subjectifs à propos d'un sujet identifiable qui sont divulgués par une organisation communicante à une organisation requérante (p. ex., nom, adresse de courriel, numéro de téléphone, adresse postale, date de naissance, renseignements sur les comptes).

Écosystème de l'identité numérique

Système interrelié pour l'échange et la vérification des renseignements d'identité numérique, impliquant des organisations des secteurs public et privé (p. ex., entités gouvernementales, commerciales, sans but lucratif et autres) qui se conforment à un cadre de confiance commun pour la gestion et l'utilisation d'identités numériques, et les sujets de ces identités numériques. Dans le contexte de la composante « Respect de la vie privée », l'écosystème de l'identité numérique fait référence à l'écosystème canadien de l'identité numérique conforme au CCP. Les participants à un écosystème de l'identité numérique peuvent inclure l'organisation requérante, l'organisation divulgatrice, l'entité chargée de traiter les avis et consentements, le fournisseur de réseau et l'organe de gouvernance tels qu'identifiés dans la section Portée de ce document.

3. Rôles

Les rôles suivants dans l'écosystème de l'identité numérique sont définis pour couvrir la portée de la composante « Respect de la vie privée ». Selon le cas d'utilisation, des organisations ou personnes distinctes peuvent assumer un ou plusieurs rôles.

- **Organisation divulgatrice –**Rôle que joue une organisation ou une personne pour détenir les renseignements personnels spécifiques au sujet, que l'utilisateur consent à divulguer à une organisation requérante ou que l'organisation divulgatrice peut légalement divulguer en vertu des lois pertinentes. Dans un contexte d'identité numérique, ce sera souvent un fournisseur d'identités ou d'attributs.
- **Organe de gouvernance –** Rôle qu'un participant joue pour s'assurer que les normes, processus et exigences connexes de l'écosystème de l'identité numérique sont mises en place, ce qui inclut la conformité aux lois, règlements et politiques gouvernementales. Ils assurent aussi la conformité des participants à l'écosystème de l'identité numérique à des mesures de protection, conseils, pratiques exemplaires, règles et arrangements commerciaux convenus.
- **Entité chargée du traitement des avis et consentements –** Rôle qu'un participant joue pour donner l'avis à l'utilisateur de la demande de renseignements personnels (émanant de l'organisation requérante), pour obtenir et enregistrer le consentement, et qui donne à l'utilisateur le moyen de gérer le consentement à l'avenir, y compris le retrait du consentement.
- **Fournisseur de réseau –** Rôle qu'un participant joue pour relier les parties dans une transaction sur une identité multipartite. Cette organisation est un participant actif et ajoute de la valeur à la prestation du service d'identité numérique (p. ex., pas un fournisseur de services Internet qui fournit passivement une connectivité Internet). Par exemple, un fournisseur de chaînes de blocs ou un logiciel en tant que service (SaaS) qui facilite le réseau.
- **Organisation requérante –** Rôle que joue une organisation ou personne pour recevoir des renseignements personnels que l'utilisateur consent à divulguer. Dans un contexte d'identité numérique, il s'agira souvent d'un fournisseur de services ou d'une partie dépendante.

Ces rôles aident à isoler les différentes fonctions et responsabilités ayant trait à la protection de la vie privée dans tous les processus de gestion de bout en bout des identités numériques. Ils ne visent pas à impliquer une solution, une architecture ou une mise en œuvre particulière.

Par exemple, dans certains cas, l'avis peut provenir et le consentement peut être obtenu d'une organisation qui facilite l'échange de renseignements personnels entre le sujet, l'organisation divulgatrice et l'organisation requérante. Dans d'autres cas, l'avis peut provenir et le consentement peut être obtenu directement de l'organisation

divulgatrice ou requérante, auquel cas cette organisation serait aussi l'entité chargée du traitement des avis et consentements.

4. Principes clés de la composante « Respect de la vie privée »

4.1. Renseignements personnels

Les pratiques ayant trait au respect de la vie privée reposent sur le principe selon lequel les personnes sont informées des détails ainsi que des éventuels avantages et conséquences associés à la gestion de leurs renseignements personnels, et peuvent agir sur la base de ces renseignements.

Les renseignements personnels, tels que définis pour les besoins de ce profil, incluent les renseignements personnels spécifiques au sujet et les renseignements spécifiques au service. Cela englobe l'information que l'utilisateur consent à communiquer (p. ex., nom, adresse de courriel, numéro de téléphone, adresse postale, date de naissance, renseignements sur le compte, etc.) ainsi que les renseignements nécessaires pour faire fonctionner et maintenir le service (p. ex., pseudonymes d'identification spécifiques aux services, dossiers de transactions).

4.2. Changements apportés aux renseignements personnels à la source (organisation divulgatrice)

Advenant un changement (y compris des corrections) aux renseignements personnels spécifiques au sujet, l'organisation divulgatrice n'est pas tenue, dans le cadre de l'écosystème de l'identité numérique, d'aviser d'une manière proactive une organisation requérante qu'elle a reçu au préalable les renseignements personnels du sujet, ni de signaler qu'un changement a été apporté, sauf si la loi l'exige. Il incombe à une organisation requérante de comparer les nouvelles données qu'elle reçoit avec celles qu'elle a reçues préalablement pour voir s'il y a eu des changements et y donner suite dans la mesure où c'est pertinent pour ses processus opérationnels.

4.3. Traitement en amont et en aval des renseignements personnels

Le traitement des renseignements personnels spécifiques au sujet et des renseignements spécifiques aux services par une organisation divulgatrice est assujetti aux lois et règlements pertinents en matière de protection de la vie privée, et n'est

généralement considéré comme étant visé par la portée du CCP que lorsque ces données sont traitées dans le but d'être partagées par le biais de l'écosystème de l'identité numérique. Il y a toutefois une exception quand une organisation requérante a des exigences spécifiques pour le traitement des renseignements personnels par leur source (l'organisation divulgatrice). Ces exigences feront donc partie de la gouvernance de l'écosystème de l'identité numérique et constitueront les exigences « en amont » auxquelles doit se conformer toute organisation divulgatrice qui dessert cette organisation requérante. De même, le traitement des renseignements personnels spécifiques à un sujet par une organisation requérante est assujetti aux lois et règlements pertinents en matière de protection de la vie privée, et n'est généralement considéré comme étant visé par la portée des exigences du CCP une fois que ces données ont été partagées par le biais de l'écosystème de l'identité numérique. Il y a toutefois une exception quand une organisation divulgatrice a des exigences spécifiques pour le traitement des renseignements personnels par leur destinataire (l'organisation requérante). Ces exigences feront donc partie de la gouvernance de l'écosystème de l'identité numérique et constitueront les exigences « en aval » auxquelles doit se conformer toute organisation requérante qui reçoit des données de l'organisation divulgatrice.

4.4. Respect de la vie privée dès la conception

Le respect de la vie privée dès la conception est un des principes directeurs adoptés par le CCIAN pour un écosystème canadien de l'identité numérique, qui consiste spécifiquement à « mettre en place, protéger et améliorer la protection de la vie privée dès la conception ». Les questions de respect de la vie privée font partie intégrante du développement d'une solution en matière d'identité numérique et devraient être prises en considération à tous les stades de ce développement. Les outils visant à améliorer le respect de la vie privée permettent à une personne de gérer ses renseignements et l'utilisation qui en est faite.

Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) de la Chambre des communes a recommandé que la LPRPDE soit modifiée afin d'inclure les principes du respect de la vie privée dès la conception [2], mais les principes équitables actuels de la LPRPDE ne le couvrent pas explicitement. Par conséquent, les critères de conformité de la composante « Respect de la vie privée » du CCP n'incluent pas des critères pour évaluer la conformité au respect de la vie privée dès la conception.

5. Introduction au profil de conformité de la composante « Respect de la vie privée » du CCP

Ce document spécifie les critères de conformité de la composante « Respect de la vie privée » du Cadre de confiance pancanadien (CCP). Pour avoir une introduction générale du CCP, y compris des renseignements contextuels et les buts et objectifs du CCP, veuillez consulter le modèle de CCP.

Les critères de conformité pour la composante « Respect de la vie privée » spécifient la façon dont les principes de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) du Canada, définis à l'annexe 1 de la Loi, sont pertinents et s'appliquent au traitement des données sur l'identité numérique. La LPRPDE s'applique aux organisations qui traitent des renseignements personnels dans le cadre de leurs activités commerciales.

Remarque : Les critères de conformité du CCP ne remplacent pas les règlements existants; on s'attend à ce que les organisations se conforment aux lois, politiques et règlements pertinents sur le respect de la vie privée qui sont en vigueur dans leur province ou territoire.

Dans les critères de conformité en matière de respect de la vie privée, l'expression « avis et consentement » doit être interprétée comme « avis, ou avis avec consentement » afin de reconnaître les cas où un avis peut être exigé, mais un consentement n'est pas requis ni sollicité.

« Participants » fait référence à chacun des rôles d'organisation divulgatrice, d'organisation requérante, d'entité chargée du traitement des avis et consentements, de fournisseur de réseau et d'organe de gouvernance. Voir l'aperçu de la composante « Respect de la vie privée » pour les définitions de ces rôles. Selon le cas d'utilisation, des organisations ou personnes distinctes peuvent assumer un ou plusieurs rôles. Ils ne sont pas destinés à impliquer une solution, une architecture ou une mise en œuvre particulière.

5.1 Mots clés des critères de conformité

Les mots clés suivants sont utilisés dans les critères de conformité pour indiquer leur priorité et/ou leur rigidité générale, et doivent être interprétés de la façon suivante :

- **DOIT** signifie que l'exigence est impérative en ce qui concerne les critères de conformité.
- **NE DOIT PAS** signifie que l'exigence est une interdiction absolue des critères de conformité.
- **DEVRAIT** signifie qu'on s'attend à ce que l'exigence soit remplie, sauf dans les cas limités où le candidat présente des raisons ou des circonstances valables d'ignorer l'exigence. Toutes les implications d'une telle exception doivent être comprises et considérées avec soin avant de décider de ne pas respecter les critères de conformité comme décrit.
- **NE DEVRAIT PAS** signifie qu'il peut exister une raison valable dans des circonstances particulières pour que l'exigence soit acceptable ou même utile, mais que toutes les implications devraient être comprises et le cas devrait être bien pris en considération avant de choisir de ne pas se conformer aux exigences telles que décrites.
- **PEUT** signifie que l'exigence est discrétionnaire mais recommandée.

Remarque

- Les mots clés ci-dessus sont en **caractères gras** et en MAJUSCULES dans ce profil de conformité.

6. Critères de conformité de la composante « Respect de la vie privée »

Les critères de conformité ci-dessous sont organisés et prévus pour s'aligner sur les principes de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) du Canada, définis à l'annexe 1 de la Loi. Les descriptions des principes qui suivent sont tirées des principes relatifs à l'équité dans le traitement de l'information de la LPRPDE du Commissariat à la protection de la vie privée du Canada. Pour faciliter la consultation, un critère de conformité spécifique peut être mentionné selon sa catégorie et son numéro de référence (p. ex., « BASE-1 » correspond à la « référence nº 1 des critères de conformité de base »).

Référence	Critères de conformité
BASE	**Critères de base** **Remarque :** Les exigences pour les cas où le sujet agit comme l'organisation divulgatrice ne sont pas abordées dans cette version des critères de conformité de base.
1	Les organisations divulgatrices et requérantes, les entités chargées de traiter les avis et consentements, les fournisseurs de réseaux et l'organe de gouvernance **DOIVENT** avoir en place un programme de gestion du respect de la vie privée qui documente les politiques, les pratiques et les procédures afin de se conformer aux lois applicables sur le respect de la vie privée et qui incorpore ce qui suit : • Renseignements recueillis, utilisés, conservés et divulgués, et pourquoi • Évaluation des risques pour la protection de la vie privée • Droits individuels, plaintes et questions • Restrictions pertinentes sur la collecte, l'utilisation, la rétention et la divulgation des renseignements (juridiques, contractuels) • Formation et sensibilisation • Diligence à l'égard des tierces parties (inclut le client, les fournisseurs, les fournisseurs de services, les partenaires) • Mesures de sécurité, et intervention et gestion en cas d'incident • Renseignements à propos de l'échange transfrontalier de renseignements personnels
2	Les organisations divulgatrices et requérantes, les entités chargées de traiter les avis et consentements, les fournisseurs de réseaux et l'organe de gouvernance **DOIVENT** avoir un responsable désigné du respect de la vie privée, qui est chargé de superviser le programme de gestion du respect de la vie privée de même que les audits ou examens internes des pratiques de traitement des renseignements personnels (notamment celles qui ont trait à la communication de l'avis et à l'obtention du consentement), et qui a le pouvoir d'intervenir sur les questions ayant trait au respect de la vie privée spécifiquement reliées au rôle de l'organisation en tant qu'organisation divulgatrice ou requérante, entité chargée de traiter les avis et consentements, fournisseur de réseau ou organe de gouvernance.

3	Les organisations divulgatrices et requérantes, les entités chargées du traitement des avis et consentements, les fournisseurs de réseau et l'organe de gouvernance **DOIVENT** avoir une politique exhaustive en matière de respect de la vie privée qui : • fournit une description de leurs pratiques de traitement des renseignements personnels; et • est facile d'accès, simple à lire et mise à jour au besoin
4	Les organisations divulgatrices et requérantes, les entités chargées du traitement des avis et consentements, les fournisseurs de réseau et l'organe de gouvernance **DOIVENT** effectuer périodiquement un examen interne ou externe indépendant de leurs pratiques de gestion des renseignements personnels (y compris leurs pratiques de gestion des avis et consentements), à intervalles ne dépassant pas un an, pour s'assurer que les renseignements personnels sont traités de la façon décrite dans leur politique en matière de respect de la vie privée.
5	Les participants **DOIVENT** conserver une preuve de conformité aux critères de conformité pour les principes 1 à 10, qui peut être fournie sur demande aux autres participants, notamment l'organe de gouvernance.
6	Dans le cadre de leurs programmes de gestion du respect de la vie privée, les organisations divulgatrices et requérantes, les entités chargées du traitement des avis et consentements, les fournisseurs de réseau et l'organe de gouvernance **DOIVENT** avoir et tester périodiquement des processus pour gérer les vols de renseignements personnels ou la divulgation de renseignements confidentiels, ce qui inclut les étapes d'évaluation des dommages ou torts, de signalement, de confinement, de correction, de notification et de prévention.
7	L'organe de gouvernance **DOIT** définir et gérer d'une manière claire les limites de l'écosystème de l'identité numérique.
ACCO	**Principe 1 - Imputabilité** *Une organisation est responsable des renseignements personnels qu'elle contrôle. Elle doit nommer quelqu'un qui sera chargé de voir à ce qu'elle se conforme à ces principes équitables en matière de traitement de l'information.*

1	Les organisations divulgatrices et requérantes, les fournisseurs de réseau, et les entités chargées du traitement des avis et consentements **DOIVENT** s'assurer que l'utilisateur a facilement accès au nom ou au titre de la personne responsable de la protection de la vie privée dans leurs organisations respectives et lui donner les moyens de communiquer avec cette personne.
2	L'organe de gouvernance **DOIT** définir et documenter des procédures et une politique qui : • enquêtent sur les écarts par rapport aux principes 1 à 10 commis par des organisations qui fonctionnent à l'intérieur de l'écosystème de l'identité numérique et les gère, notamment évaluer le risque pour les sujets et le fait que les infractions sont signalées par les participants aux organismes de réglementation du respect de la vie privée et aux sujets pertinents • le cas échéant, vérifient que les participants pertinents à l'écosystème de l'identité numérique se conforment aux exigences spécifiques définies par une organisation à propos des renseignements personnels spécifiques au sujet • incluent des règles en matière de normes et d'interopérabilité qui font en sorte que toutes les parties intervenant dans le partage des renseignements personnels spécifiques au sujet traitent le sujet et les renseignements personnels spécifiques au sujet d'une manière uniforme et compatible • facilitent la surveillance des risques opérationnels (p. ex., fraude, sécurité des renseignements) à l'échelle de l'écosystème de l'identité numérique.
IDEN	**Principe nº 2 -** Détermination des motifs *Les motifs pour lesquels les renseignements personnels sont recueillis doivent être déterminés par l'organisation avant ou au moment d'être obtenus.* [1]
1	L'organisation divulgatrice **DOIT** pouvoir démontrer aux organisations requérantes et aux entités chargées du traitement des avis et consentements qu'une diligence suffisante a été accomplie pendant l'existence des processus de gouvernance ou de contrôle pertinents, avant de divulguer des renseignements personnels à ces organisations.

2	L'organisation divulgatrice **DOIT** maintenir et préserver un calendrier relatif aux documents récupérables qui inclut les dossiers de demande de renseignements et les cas de divulgation. Le calendrier peut consister en un seul événement (« demande et divulgation ponctuelles ») ou plusieurs événements compte tenu des circonstances de l'échange.
3	L'organisation requérante **DOIT** avoir un motif relié à l'identité qui est clair, défini et justifiable pour recueillir des renseignements personnels spécifiques au sujet par l'intermédiaire de l'entité chargée du traitement des avis et consentements.
4	L'organisation requérante **DOIT** maintenir et préserver un calendrier relatif aux documents récupérables afin d'indiquer pourquoi les renseignements personnels sont nécessaires et de quelle façon ils seront utilisés.
5	L'organisation requérante **DOIT** mener périodiquement, à intervalles d'au plus un an, un examen interne de ses exigences en matière de collecte et d'utilisation des renseignements personnels, et mettre à jour les demandes futures en conséquence.
6	L'organisation requérante **DOIT** s'assurer que les motifs pour recueillir et utiliser les renseignements personnels spécifiques au sujet sont clairs, spécifiques et sans ambiguïté.
7	Avant que des renseignements personnels ne soient obtenus ou lorsqu'ils sont recueillis, l'entité chargée du traitement des avis et consentements **DOIT** indiquer explicitement au sujet pourquoi ils sont nécessaires et de quelle façon ils seront utilisés.
8	L'organe de gouvernance **DOIT** définir clairement la portée de l'écosystème de l'identité numérique à tous les participants et préciser que les motifs d'identification débordant de la portée de l'écosystème de l'identité numérique (qui peuvent exister au sein de chaque organisation participante) ne sont pas couverts.
CONS	**Principe nº 3 - Consentement** *La collecte, l'utilisation et la divulgation des renseignements personnels exigent que la personne soit au courant et donne son consentement, sauf lorsque ce n'est pas approprié.*

1	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DOIVENT** s'assurer que l'avis et la connaissance nécessaires pour la demande de consentement sont clairs et compréhensibles et qu'ils signifient quelque chose pour l'utilisateur, et inclure des détails pour indiquer si le consentement est valable une seule fois ou permanent, et comment l'utilisateur peut révoquer ou reprendre le consentement. Voir aussi les rubriques NOTI 1, 3, 4 et 5, CONS-8 et MANA-2 et 6 dans la composante « Avis et consentement » du CCP.
2	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DEVRAIENT** s'assurer que le processus de consentement est clair en ce qui concerne ce à quoi s'applique le consentement. Dans tous les cas, un moyen direct **DEVRAIT** être fourni à l'utilisateur pour lui permettre d'obtenir des renseignements supplémentaires, au besoin.
3	Les organisations divulgatrices et requérantes **DOIVENT** s'assurer que l'entité chargée du traitement des avis et consentements s'acquitte de ses fonctions consistant à donner un avis et à obtenir, enregistrer et gérer le consentement d'une manière appropriée avant de divulguer les renseignements personnels spécifiques au sujet. Les organisations divulgatrices et requérantes **DOIVENT** s'assurer que le consentement est en place avant de le donner ou le recevoir. Voir aussi la rubrique NOTI-1 dans la composante « Avis et consentement » du CCP.
4	L'organisation divulgatrice **DOIT** s'assurer que l'entité chargée du traitement des avis et consentements obtient la preuve de l'avis et du consentement et qu'elle est ensuite gardée dans un dossier d'avis et de consentements.
5	L'organisation divulgatrice **DOIT** s'assurer que l'avis et le consentement ne sont pas expirés ou révoqués au moment du partage des renseignements personnels spécifiques au sujet. Dans l'éventualité où le consentement n'est ni expiré ni révoqué, l'organisation requérante **DOIT** obtenir une réponse indiquant que le consentement est valide.

6	L'organisation divulgatrice **DOIT** s'assurer que l'utilisateur a accès aux renseignements nécessaires pour comprendre la nature, la raison d'être et les risques associés à l'utilisation ou à la divulgation des renseignements personnels spécifiques au sujet, à l'intérieur de l'écosystème de l'identité numérique, par exemple au moyen de l'avis sur le respect de la vie privée. Voir aussi la rubrique NOTI-5 dans la composante « Avis et consentement » du CCP.
7	L'organisation requérante, dont émane la demande de consentement, **DOIT** indiquer, dans le contenu de l'avis, le but du traitement des renseignements personnels spécifiques au sujet qui ont été demandés. Voir aussi la rubrique NOTI-3 dans la composante « Avis et consentement » du CCP.
8	L'organisation requérante, dont émane la demande de consentement, **DOIT** indiquer, dans le contenu de l'avis, si la demande est pour une divulgation unique des renseignements personnels ou pour permettre une divulgation permanente. Voir aussi la rubrique NOTI-3 dans la composante « Avis et consentement » du CCP.
9	L'organisation requérante **DOIT** s'assurer que la demande de consentement est conforme au principe de divulgation minimale.
10	L'organisation requérante **DOIT** s'assurer qu'une preuve de l'avis et du consentement est obtenue par l'entité chargée du traitement des avis et consentements, puis enregistrée comme un dossier d'avis et de consentement.
11	Quand l'organisation requérante est informée que le consentement n'est plus valide, elle **DOIT** avoir un processus documenté pour cesser de recueillir d'autres renseignements personnels spécifiques au sujet qui sont basés sur ce consentement invalidé. Voir aussi la rubrique MANA-2 dans la composante « Avis et consentement » du CCP.
12	L'entité chargée du traitement des avis et consentements **DOIT** aviser l'utilisateur à l'intérieur de l'écosystème de l'identité numérique.
13	L'entité chargée du traitement des avis et consentements **DOIT** s'assurer que l'avis indique clairement si la demande est pour une divulgation unique des renseignements personnels ou pour permettre une divulgation permanente à l'intérieur de l'écosystème de l'identité numérique.

14	L'entité chargée du traitement des avis et consentements **DOIT** s'assurer ou se faire confirmer que l'utilisateur est authentifié avant d'afficher des renseignements personnels spécifiques au sujet dans un avis adressé à l'utilisateur en validant l'identité de l'utilisateur.
15	L'organisation divulgatrice **DOIT** déterminer la sensibilité des renseignements partagés et stipuler des contrôles (p. ex., politiques de masquage ou autres mesures de précaution) pour l'affichage de renseignements sensibles dans l'avis.
16	Si l'entité chargée du traitement des avis et consentements affiche des renseignements personnels dans l'avis, ces renseignements personnels **DOIVENT** être affichés conformément à n'importe quels contrôles (p. ex., politiques de masquage ou autres mesures de précaution) stipulés par l'organisation divulgatrice. Voir NOTI-3 dans la composante « Avis et consentement » du CCP pour savoir quels types de renseignements peuvent être exigés dans l'avis.
17	L'entité chargée du traitement des avis et consentements **DOIT** avoir un processus documenté pour recueillir le consentement et le communiquer à l'organisation divulgatrice et à l'organisation requérante intervenant dans la transaction sur l'identité numérique. Voir aussi la rubrique RECO 2 dans la composante « Avis et consentement » du CCP.
18	L'entité chargée du traitement des avis et consentements **DOIT** enregistrer le consentement. Voir aussi la rubrique RECO-1 dans la composante « Avis et consentement » du CCP.
19	L'entité chargée du traitement des avis et consentements **DEVRAIT** avoir un processus clair et documenté permettant à l'utilisateur d'examiner et de gérer les consentements donnés. Voir aussi la rubrique MANA 7 dans la composante « Avis et consentement » du CCP.
20	Pour les transactions liées à l'identité où le consentement est géré entre plusieurs organisations requérantes et divulgatrices, l'entité chargée du traitement des avis et consentements **DOIT** s'assurer que le traitement est effectué conformément au motif spécifié dans l'avis et le consentement accordés par l'utilisateur à chaque organisation.

21	L'entité chargée du traitement des avis et consentements **DOIT** avoir des processus en place pour soutenir la révocation du consentement. Par exemple, une mesure pour révoquer un consentement pourrait émaner du sujet ou être une réponse à la détection d'une activité frauduleuse par n'importe laquelle des organisations qui traitent l'identité numérique. Voir aussi les rubriques MANA-3, 4 et 5 dans la composante « Avis et consentement » du CCP.
22	Le fournisseur de réseau **NE DOIT PAS** être en mesure de voir des renseignements personnels non protégés partagés par le biais de l'écosystème de l'identité numérique. Cela inclut spécifiquement les renseignements personnels présentés dans le processus d'avis et de consentement, ainsi que les renseignements personnels transmis par le biais du réseau.
23	L'organe de gouvernance **DOIT** définir des lignes directrices sur la formulation des avis et l'obtention du consentement, de façon à procurer une expérience utilisateur uniforme et optimisée dans tout l'écosystème de l'identité numérique.
24	L'organe de gouvernance **DOIT** s'assurer que la révocation du consentement par un utilisateur devient rapidement effective dans tout l'écosystème de l'identité numérique.
LIMC	**Principe nº 4 – Obtention limitée** *L'obtention de renseignements personnels doit se limiter à ce qui est nécessaire pour les besoins déterminés par l'organisation. Les renseignements doivent être recueillis par des moyens équitables et légaux.*
1	L'organisation divulgatrice **DOIT** établir un processus documenté pour s'assurer que l'organisation requérante a un motif clair, défini et justifiable, relié à l'identité, pour recueillir les renseignements personnels demandés.
2	L'organisation requérante **DOIT** uniquement utiliser, garder et divulguer les renseignements personnels à des fins reliées à l'identité, comme la validation ou la vérification des attributs de l'identité d'un demandeur de service. Elle **NE DOIT PAS** utiliser sans consentement ces renseignements sur l'identité à d'autres fins non reliées, comme le marketing.
3	L'organisation requérante **DOIT** limiter les renseignements personnels qui sont recueillis par le biais de l'écosystème de l'identité numérique à ce qui est nécessaire pour la ou les fins reliées à l'identité indiquées.

4	L'organisation requérante **DOIT** documenter publiquement, ou rendre disponible, dans un langage clair et dépourvu de toute ambiguïté, la nature des renseignements personnels recueillis et à quelle fin.
5	L'organisation requérante **DOIT** indiquer aux employés applicables la nature des renseignements personnels recueillis et à quelle fin afin de répondre avec exactitude aux demandes d'information de tierces parties, le cas échéant.
6	L'entité chargée du traitement des avis et consentements **DOIT** s'assurer que les renseignements personnels nécessaires pour remplir la fonction d'avis et de consentement sont limités uniquement à ce qui est requis pour la fonction.
7	Le fournisseur de réseau **NE DOIT PAS** recueillir des renseignements personnels au-delà de ce qui est nécessaire pour soutenir ses ententes de service, par exemple agir en leur nom comme fournisseur de service.
8	L'organe de gouvernance **DOIT** avoir un processus documenté qui examinerait la raison pour laquelle l'organisation requérante recueille les renseignements personnels demandés et détermine que la collecte est juste et légale.
9	L'organe de gouvernance **DOIT** fournir des lignes directrices sur les façons appropriées de limiter l'obtention des renseignements personnels dans l'écosystème de l'identité numérique et par ceux qui y participent.
LIMU	**Principe nº 5 – Limitation de l'utilisation, de la divulgation et de la rétention** *À moins que la personne n'y consente ou que la loi ne l'exige, les renseignements personnels ne peuvent être utilisés ou divulgués qu'aux fins pour lesquelles ils ont été recueillis. Les renseignements personnels ne doivent être conservés que le temps nécessaire pour servir à ces fins.*
1	L'organisation divulgatrice **DOIT** avoir des politiques internes et d'autres documents pour limiter l'utilisation, la divulgation et la rétention des renseignements personnels spécifiques au sujet.
2	L'organisation divulgatrice **DOIT** documenter l'utilisation des renseignements personnels du sujet pour les besoins de la divulgation dans l'écosystème de l'identité numérique.

3	L'organisation divulgatrice **DOIT** se conformer à la politique définie sur la rétention minimale et maximale des données qui est spécifiée pour l'écosystème de l'identité numérique, en ce qui concerne les renseignements personnels spécifiques au sujet en lien avec l'écosystème de l'identité numérique. Remarque : Sous réserve des restrictions réglementaires.
4	À moins que la loi ne permette ou n'exige autre chose, l'organisation divulgatrice **DOIT** limiter la communication des renseignements personnels spécifiques au sujet uniquement à ce qui est nécessaire pour les fins précises et recherchées qui correspondent au consentement du sujet.
5	L'organisation divulgatrice **DOIT** avoir des processus en place pour s'assurer que les renseignements personnels devant être divulgués sont exacts, complets et le plus à jour possible.
6	L'organisation requérante **DOIT** documenter l'usage des renseignements personnels spécifiques au sujet obtenus par le biais de l'écosystème de l'identité numérique.
7	L'organisation requérante et l'entité chargée du traitement des avis et consentements **DOIVENT** instituer des périodes maximales et minimales valides pour conserver les renseignements personnels spécifiques au sujet qui sont reçus par le biais de l'écosystème de l'identité numérique, et se conformer à la rétention spécifiée dans l'avis. Voir aussi la rubrique NOTI-3 dans la composante « Avis et consentement » du CCP.
8	L'organisation requérante **DOI**T obtenir un consentement approprié pour l'utilisation ou la rétention de renseignements personnels spécifiques au sujet (reçus par le biais de l'écosystème de l'identité numérique) pour des fins débordant de ce qui est spécifié par l'entremise de l'entité chargée du traitement des avis et consentements au moment où ils sont recueillis. Voir l'aperçu de la composante « Respect de la vie privée » du CCP pour consulter la définition du consentement dans le contexte de cette composante.
9	L'entité chargée du traitement des avis et consentements **DOIT** avoir des politiques internes et autres documents pour limiter l'utilisation, la divulgation et la rétention des renseignements personnels.

10	L'entité chargée du traitement des avis et consentements **DOIT** documenter l'utilisation des renseignements personnels spécifiques au sujet dans le but de fournir des avis et d'obtenir des consentements dans l'écosystème de l'identité numérique. Remarque : D'une façon générale, l'entité chargée du traitement des avis et consentements ne verra pas les renseignements personnels. Cela dépend toutefois de la mise en œuvre et de l'obligation de présenter les renseignements personnels spécifiques au sujet dans le cadre du processus de consentement.
11	Les organisations requérantes et les entités chargées du traitement des avis et consentement **DOIVENT** se débarrasser des renseignements personnels à l'expiration de la période de rétention. Voir aussi la rubrique MANA-2 dans la composante « Avis et consentement » du CCP.
12	Le fournisseur de réseau **NE DOIT PAS** utiliser, divulguer ou garder des renseignements personnels plus que le temps nécessaire pour soutenir ses ententes de service, par exemple pour agir pour le compte d'un fournisseur de services.
13	L'organe de gouvernance **DOIT** définir des règles pour l'utilisation, la divulgation et la rétention de bout en bout des renseignements personnels créés comme sous-produit de l'utilisation de l'écosystème de l'identité numérique.
14	L'organe de gouvernance **DOIT** définir et mettre en place des processus pour superviser et faire appliquer les exigences concernant l'utilisation, la divulgation et la rétention des renseignements personnels créés comme un sous-produit de l'utilisation de l'écosystème de l'identité numérique.
ACCU	**Principe nº 6 - Exactitude** *Les renseignements personnels doivent être aussi exacts, complets et à jour que possible afin de servir adéquatement les fins pour lesquelles ils sont destinés à être utilisés.*
1	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DOIVENT** faire en sorte que les utilisateurs puissent mettre à jour des renseignements personnels inexacts que détient le participant respectif de l'écosystème de l'identité numérique. Par exemple, un fournisseur d'identité axé sur le consommateur peut fournir à l'utilisateur la capacité de mettre directement à jour ses renseignements personnels en tout temps.

2	L'organisation divulgatrice **DOIT** instaurer des politiques, procédures et systèmes pour repérer, corriger et gérer les renseignements personnels inexacts ou désuets (p. ex., en mettant à jour les dossiers du sujet). Remarque : D'une façon générale, une organisation saura que les renseignements sont désuets uniquement si elle pose la question à quelqu'un (p. ex., au sujet lors d'une vérification périodique) ou si elle reçoit des notifications poussées de mises à jour. Les options optimales ou disponibles pour maintenir ces renseignements varieront selon les cas d'utilisation et les circonstances spécifiques. Se reporter au profil « Personne vérifiée », en particulier la section Maintenance des identifiants, pour les critères de conformité connexes.
3	L'organisation divulgatrice **NE DOIT PAS** partager des renseignements personnels qui sont connus pour ne pas être valides, comme une adresse pour laquelle le courrier a été retourné à l'organisation.
4	Lorsqu'elle partage les renseignements personnels d'un sujet avec une organisation requérante, l'organisation divulgatrice **DOIT** donner à l'utilisateur : 1. la possibilité d'examiner une description ou un résumé des renseignements personnels spécifiques au sujet devant être partagés; 2. des instructions ou les moyens de mettre à jour les renseignements personnels spécifiques au sujet.
5	Lorsqu'on partage des renseignements d'un sujet spécifiques à des services avec une organisation requérante, l'organisation divulgatrice ou l'entité chargée du traitement des avis et consentements **PEUT** donner à l'utilisateur : 1. la possibilité d'examiner une description ou un résumé de ses renseignements spécifiques aux services devant être partagés; 2. des instructions ou les moyens de mettre à jour ces renseignements spécifiques aux services.
6	Pour vérifier l'exactitude des renseignements personnels reçus de l'organisation divulgatrice, l'organisation requérante **DEVRAIT** donner à l'utilisateur la possibilité d'examiner un résumé ou une description des renseignements divulgués.

7	Lorsque les renseignements personnels obtenus d'autres participants à l'écosystème de l'identité numérique ne correspondent pas à ceux que l'organisation requérante possède, celle-ci **DOIT** avoir une procédure documentée pour résoudre l'anomalie.
8	L'entité chargée du traitement des avis et consentements **DOIT** conserver une piste d'audit des avis présentés et des décisions reçues relativement aux consentements, et quand cela a été fourni. L'intégrité de cette piste d'audit doit être maintenue. La période de rétention pour la piste d'audit sera déterminée par le cadre de gouvernance et la législation et la réglementation applicables.
9	L'organe de gouvernance **DOIT** définir une politique et des lignes directrices afin d'assurer l'exactitude des renseignements personnels dans l'écosystème de l'identité numérique. Cela peut inclure, par exemple, des indications pour mettre en place des services qui permettent (avec le consentement du sujet) de diffuser des mises à jour aux organisations requérantes qui se sont abonnées pour recevoir ces mises à jour.
SAFE	**Principe nº 7 – Mesures de protection** *Les renseignements personnels doivent être protégés par des mesures de sécurité appropriées compte tenu de la sensibilité des renseignements.*
1	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DOIVENT** avoir des politiques, des processus, des contrôles et des mesures de sécurité en place pour protéger les renseignements personnels, et les communiquer à l'utilisateur (le cas échéant).
2	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DOIVENT mettre en place des** politiques, processus et contrôles pour repérer, gérer et atténuer les incidents et atteintes à la sécurité, notamment en rendre compte à l'extérieur à d'autres organisations, aux organismes de réglementation, à l'organe de gouvernance ou aux utilisateurs, si cela est nécessaire, approprié ou exigé par la loi.
3	L'organisation divulgatrice **DOIT** développer et mettre en place une politique de sécurité qui inclut spécifiquement des mesures de protection utilisées dans la divulgation des renseignements personnels spécifiques au sujet dans le contexte des systèmes d'identité numérique.

4	L'organisation divulgatrice et l'organisation requérante **DOIVENT** mettre en place des mesures de sécurité appropriées, conformément aux risques de préjudice et à la sensibilité des renseignements personnels identifiés dans l'évaluation des risques (évaluation des risques de menace et/ou de l'impact sur la protection de la vie privée, selon le cas), pour protéger l'accès aux renseignements personnels.
5	L'organisation divulgatrice et l'organisation requérante **DOIVENT** mettre en place des mesures de sécurité appropriées pour protéger l'accès aux renseignements personnels, au repos et en transit.
6	Les organisations divulgatrices et requérantes, les entités chargées du traitement des avis et consentements, et les fournisseurs de réseau **DOIVENT** examiner et mettre à jour régulièrement leurs mesures de sécurité reliées à l'écosystème de l'identité numérique.
7	L'organisation requérante **DOIT** développer et mettre en place une politique de sécurité pour protéger les renseignements personnels, qui inclut spécifiquement les mesures de protection employées pour la réception des renseignements personnels dans le contexte de l'écosystème de l'identité numérique.
8	L'entité chargée du traitement des avis et consentements et le fournisseur de réseau **DOIVENT** mettre en place des mesures de sécurité spécifiées dans les critères pertinents de la composante « Infrastructure (technologie et opérations) » du CCP.
9	L'entité chargée du traitement des avis et consentements **DOIT** mettre en place des mesures de sécurité appropriées à la sensibilité des renseignements personnels fournis au sujet dans l'avis de protection de la vie privée et au risque d'utilisation malveillante identifié dans l'évaluation du risque (évaluation du risque de menace et/ou de répercussions sur la vie privée, selon ce qui est approprié) pour protéger l'accès aux renseignements personnels.
10	Le fournisseur de réseau **DOIT** développer et mettre en place une politique de sécurité appropriée à la fonction du réseau. Cela consiste normalement à s'assurer que le fournisseur de réseau réduit la visibilité des renseignements personnels.
11	L'organe de gouvernance **DOIT** définir et mettre en place des mesures de gouvernance qui incluent des normes de sécurité minimales, une évaluation des mesures de sécurité des participants (si approprié) et des obligations contractuelles forçant les participants à satisfaire à des normes de sécurité minimales.

12	Les participants **DOIVENT** faire une évaluation des risques (évaluation des risques de menace et/ou évaluation de l'impact sur la protection de la vie privée, selon le cas) afin de confirmer les risques associés à leur traitement des renseignements personnels.
OPEN	**Principe nº 8 - Ouverture** *Une organisation doit faire en sorte que des informations détaillées sur ses politiques et pratiques reliées à la gestion des renseignements personnels soient publiques et immédiatement accessibles.*
1	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DOIVENT** faire en sorte que le sujet soit capable d'obtenir immédiatement des renseignements clairs et compréhensibles sur ce qui suit : • l'écosystème de l'identité numérique (pouvant faire référence aux renseignements conservés par l'organe de gouvernance) • les renseignements personnels recueillis, utilisés, conservés ou divulgués • les fins pour lesquelles les renseignements personnels sont recueillis, utilisés, conservés ou divulgués • les noms ou catégories des destinataires tiers des renseignements personnels • une explication des droits du sujet à la protection de la vie privée et de la façon dont il s'en prévaut • la façon dont les renseignements personnels du sujet sont protégés • l'endroit où obtenir plus de renseignements • à qui s'adresser pour obtenir de l'aide
2	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DOIVENT** avoir un processus documenté pour fournir de l'aide et des conseils quand un utilisateur fait une demande d'accès concernant une partie différente de l'écosystème de l'identité numérique. Cela peut consister pour l'utilisateur à identifier l'organisation requérante à partir de l'historique de l'activité ou d'un reçu de consentement, et/ou en incitant le fournisseur de réseau ou l'organe de gouvernance à soutenir l'identification du participant pertinent.

3	Les organisations divulgatrices et requérantes, les entités chargées du traitement des avis et consentements, et les fournisseurs de réseau **DOIVENT** avoir un processus documenté pour fournir sur demande de l'information aux utilisateurs à propos de leur rôle dans l'écosystème de l'identité numérique selon les lignes directrices de l'organe de gouvernance.
4	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements, et les fournisseurs de réseau **DOIVENT** s'assurer que les renseignements sur leur rôle sont clairement dissociés des autres services et fonctions fournis par l'organisation (qui ne font pas partie de l'écosystème de l'identité numérique en soi), comme le marketing.
5	L'organe de gouvernance **DOIT** développer et maintenir des renseignements clairs et compréhensibles sur la façon générale dont les renseignements personnels sont recueillis, utilisés et divulgués dans l'écosystème de l'identité numérique, et dont les utilisateurs peuvent exercer leurs droits à la protection de la vie privée.
6	L'organe de gouvernance **DOIT** avoir une procédure documentée pour examiner les renseignements sur la politique et les pratiques d'un participant en ce qui concerne la protection de la vie privée, qui sont exigés par les critères du principe nº 8 Ouverture, et faire en sorte que ces renseignements soient présentés d'une manière uniforme pour éviter des messages conflictuels ou prêtant à confusion.
7	L'organe de gouvernance **DOIT** fournir aux participants des lignes directrices sur la conformité avec les énoncés des critères du principe nº 8 Ouverture à l'intérieur de l'écosystème de l'identité numérique.
8	L'organe de gouvernance **DOIT** s'assurer que chaque participant, y compris l'organe de gouvernance, a des processus en place pour répondre à une demande d'information d'un utilisateur.
INDI	**Principe nº 9 – Accès individuel** *Une personne doit être informée, sur demande, de l'existence, l'utilisation et la divulgation de ses renseignements personnels, et obtenir l'accès à ces renseignements. Une personne devra pouvoir remettre en question l'exactitude et l'exhaustivité des renseignements, et les faire modifier le cas échéant.* [1]
1	Les participants à l'écosystème de l'identité numérique **DOIVENT** avoir des politiques appropriées concernant l'existence, l'utilisation et la divulgation des renseignements personnels.

2	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DEVRAIENT** avoir des processus appropriés pour gérer les plaintes et les demandes de droits des utilisateurs, notamment : • établir clairement les responsabilités des autres entités intervenant dans le règlement • former le personnel applicable pour qu'il soit en mesure de répondre aux demandes ou aux plaintes
3	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DEVRAIENT** fournir des fonctionnalités intégrées qui donnent automatiquement à l'utilisateur la capacité d'accéder à leurs renseignements personnels et de les corriger. Remarque : Étant donné que l'entité chargée du traitement des avis et consentements facilite le partage, mais pas l'utilisation, des renseignements personnels, l'« accès individuel » risque de se limiter à voir la piste d'audit des activités d'avis et de consentement reliées au sujet.
4	Si les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements ne fournissent pas des fonctionnalités intégrées, elles **DOIVENT** créer un processus documenté permettant aux utilisateurs d'obtenir des renseignements concernant l'existence, l'utilisation et la divulgation de leurs renseignements personnels, et en informer clairement les utilisateurs. Remarque : Comme l'entité chargée du traitement des avis et consentements facilite le partage des renseignements personnels, mais ne les utilise pas, l'« accès individuel » devrait se limiter à voir la piste d'audit des activités d'avis et de consentement reliées au sujet.
5	Si l'organisation requérante détermine que les renseignements personnels qu'elle reçoit de l'écosystème de l'identité numérique sont inexacts ou incomplets, il **DEVRAIT** y avoir des processus pour aviser l'organisation divulgatrice pertinente du problème.
6	Le fournisseur de réseau **NE DEVRAIT PAS** avoir accès aux renseignements personnels (autres que des identifiants potentiellement anonymes que le réseau ne peut pas relier aux sujets). Si le fournisseur de réseau n'a pas accès aux renseignements personnels, il **DOIT** alors se conformer aux critères INDI 1 à 4.

7	Les mesures de gouvernance prises par l'organe de gouvernance **DOIVENT** inclure une section sur les processus et lignes directrices du principe nº 9 « Accès individuel » qui sont fournis aux participants et appropriés aux renseignements échangés par le biais de l'écosystème de l'identité numérique.
CHAL	**Principe nº 10 – Remise en question de la conformité** *Une personne devra pouvoir remettre en question la conformité d'une organisation aux principes ci-dessus. Cette remise en question devrait être adressée à la personne responsable de la conformité de l'organisation à la LPRPDE, qui est généralement le chef de la protection de la vie privée.*
1	Le nom ou le titre de la personne responsable de la conformité au sein de l'organisation divulgatrice, de l'organisation requérante et de l'entité chargée du traitement des avis et consentements, de même que le moyen d'intenter un recours contre elles **DOIVENT** être clairement disponibles à quiconque les demande.
2	Les organisations divulgatrices et requérantes, les entités chargées du traitement des avis et consentements, et les fournisseurs de réseau **DOIVENT** tous avoir un programme de gestion de la conformité qui, à tout le moins : • dissocie d'une façon claire et simple l'implication dans l'écosystème de l'identité numérique des autres activités de l'organisation; • aide l'utilisateur à obtenir le soutien voulu, même si la plainte doit être adressée à un autre participant dans l'écosystème de l'identité numérique.
3	L'organe de gouvernance **DOIT** fournir aux participants des lignes directrices sur la façon de signaler des plaintes et d'y répondre sans délai, et de consigner les mesures afin que le sujet reçoive le soutien nécessaire de la part du bon participant, d'une manière aussi efficace et claire que possible.

7. Notes et hypothèses

Il peut y avoir plus d'une organisation chargée de mener de bout en bout les processus de confiance en matière de respect de la vie privée. L'implication de plusieurs organisations ou personnes peut introduire de la complexité dans le processus d'évaluation et de certification, mais le cadre de confiance n'empêche pas d'avoir différentes approches pour la mise en œuvre. Trois rôles organisationnels sont définis à l'intérieur du profil de conformité (organisation requérante, organisation communicante, et entité chargée du traitement des avis et consentements). Ces rôles permettent d'isoler les différentes fonctions et responsabilités dans le processus intégral. Ils ne visent toutefois pas à impliquer une solution, une architecture ou une mise en œuvre en particulier.

Les pratiques qui respectent la vie privée dépendent du principe voulant que les personnes connaissent et comprennent les détails et les avantages et conséquences potentiels associés à la gestion de leurs renseignements personnels, et peuvent prendre des mesures basées sur ces renseignements. Le profil « Avis et consentement » du CCP traite des exigences spécifiques pour cela sont traitées dans le profil « Avis et consentement » du CCP.

8. Références

Cette section énumère les normes, directives et autres documents externes auxquels il est fait référence dans la composante « Respect de la vie privée » du CCP.

1. Principes relatifs à l'équité dans le traitement de l'information de la LPRPDE, Commissariat à la protection de la vie privée du Canada, date de modification : mai 2019 et Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), Principes énoncés dans la norme nationale du Canada intitulée Code type sur la protection des renseignements personnels, CAN/CSA-Q830-96
2. Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, février 2018, recommandation 14, p. 52

9. Historique des révisions

Numéro de version	Date de diffusion	Auteur(s)	Brève description
0.01	2018-10-31	Consult Hyperion	Ébauche de travail initiale
0.02	2018-11-22	CCIAN	Changements de termes dans les rôles : • « Réseau » changé pour « fournisseur de réseau » • « Écosystème » changé pour « organe de gouvernance »
0.03	2019-03-20	Équipe de rédaction du CCP	Mises à jour pour l'ébauche de discussion • Suppression du contenu sur l'avis et le consentement • Principes de respect de la vie privée • Description de la raison d'être de la composante « Respect de la vie privée »
0.04	2019-05-09	Équipe de rédaction du CCP	Mise à jour des principales descriptions de la composante « Respect de la vie privée »
0.05	2019-06-26	Équipe de rédaction du CCP	Incorporation des commentaires provenant de l'examen par le TFEC sur l'ébauche de discussion
0.06	2019-10-31	Équipes de rédaction de la protection de la vie privée dès la conception et du CCP	Révision du contenu basée sur les commentaires lors de l'examen ouvert de l'ébauche de discussion

0.07	2019-11-22	Équipe de rédaction du CCP	Application d'une présentation standard pour l'aperçu du CCP, qui regroupe l'information conceptuelle dans l'aperçu
0.08	2019-12-11	Équipe de rédaction du CCP	Mise à jour découlant des réunions de l'équipe de conception « Respect de la vie privée »
0.09	2020-01-02	Équipe de rédaction du CCP	Mise à jour basée sur les changements rédactionnels suggérés lors d'un examen ouvert
0.10	2020-02-12	Équipe de rédaction du CCP	Mise à jour basée sur plusieurs séances de consultation avec l'équipe d'experts du TFEC visant à examiner les commentaires reçus du TFEC
1.0	2020-02-12	Équipe de rédaction du CCP	Approbation comme ébauche de recommandation V1.0
1.1	2021-10-29	Rédacteur du PCTF et équipe de conception de la composante « Respect de la vie privée »	Mise à jour en réponse aux commentaires du public
1.1	2021-11-10	Rédacteur du PCTF et équipe de conception de la composante « Respect de la vie privée »	Approbation du TFEC comme candidat à une recommandation finale V1.1
1.2	2022-02-05	Rédacteur du PCTF et équipe de conception de la composante « Respect de la vie privée »	Mise à jour conformément aux instructions de l'équipe de conception de la composante « Respect de la vie privée », basée sur les commentaires découlant de l'examen public

1.2	2022-03-02	Rédacteur du PCTF et équipe de conception de la composante « Respect de la vie privée »	Approbation du TFEC comme candidat à une recommandation finale V1.2
1.2	2022-03-18	Rédacteur du PCTF et équipe de conception de la composante « Respect de la vie privée »	Approuvé en tant que recommandation finale V1.2 par vote du membre de soutien du CCIAN