Cadre de confiance pancanadien respect de la vie privée

Statut du document : Recommandation finale version 1.0

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

Ce document a été préparé par le Comité d'experts du Cadre de confiance pancanadien du CCIAN avec l'apport du public recueilli et traité par le biais d'un processus d'examen ouvert mené par des 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 au moyen 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). Les changements apportés à ce document qui pourraient se répercuter sur l'état des certifications et des marques de confiance seront définis dans la composante « Évaluation » du CCP.

Table des matières

1 Introduction au profil de conformité en matière de 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 l'aperçu du 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

- 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 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.

1.1 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 que même s'il peut y avoir des raisons valables dans des circonstances particulières pour ignorer l'exigence, toutes les implications devraient être comprises et considérées avec soin avant de décider de ne pas respecter les critères de conformité ou de choisir une autre option tel que spécifié par les critères de conformité.
- **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 apparaissent en caractères **gras** et en MAJUSCULES dans ce profil de conformité.

2 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 pour assurer la conformité aux lois applicables, notamment la mise en œuvre de politiques, de pratiques, de contrôles et d'outils d'évaluation en matière de respect de la vie privée.
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 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).
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** auditer ou examiner périodiquement leurs pratiques de gestion des renseignements personnels (y compris leurs pratiques de gestion des avis et consentements), à intervalles ne dépassant pas trois ans, 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	L'organe de gouvernance **DOIT** s'assurer que les organisations menant des activités à l'intérieur de l'écosystème de l'identité numérique se conforment aux critères de conformité énumérés pour les principes 1 à 10.
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 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 nº 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 les entités chargées du traitement des avis et consentements **DOIVENT** s'assurer que l'utilisateur sait clairement qui (p. ex. désignation, coordonnées) est responsable du respect de la vie privée dans leurs organisations respectives.
2	Les organisations divulgatrices et requérantes, les fournisseurs de réseau les entités chargées du traitement des avis et consentements **DOIVENT** mettre à la disposition de l'utilisateur le nom ou le titre de la personne responsable du respect de la vie privée dans leurs organisations respectives et lui donner les moyens de communiquer avec cette personne.
3	L'organisation divulgatrice **DOIT** avoir un programme de gestion du respect de la vie privée qui inclut : • le cas échéant, des restrictions basées sur le type d'organisations avec lesquelles des renseignements personnels spécifiques au sujet seront partagés, ou des restrictions basées sur le but dans lequel ces renseignements sont recueillis. Il peut s'agir, entre autres, de restrictions basées sur le secteur ou l'environnement réglementaire (p. ex., santé, services financiers); • le cas échéant, la spécification des exigences que les participants pertinents à l'écosystème de l'identité numérique doivent remplir en ce

	qui concerne le traitement des renseignements personnels spécifiques au sujet; • le cas échéant, des restrictions sur le processus de partage des renseignements personnels spécifiques au sujet; les processus à suivre lorsque les renseignements personnels spécifiques au sujet sont partagés; • les processus à suivre lorsque les renseignements personnels spécifiques au sujet ayant déjà été partagés sont mis à jour, supprimés ou expirés; • des consignes précises à l'intention des utilisateurs sur le partage de renseignements personnels qui leur sont spécifiques pour les aider à savoir avec quelle partie ils devraient communiquer compte tenu de la nature de leur demande; • des contrôles de la protection des données; et • une évaluation de l'incidence sur le respect de la vie privée, qui couvre explicitement le partage de renseignements personnels spécifiques au sujet par le biais de l'écosystème de l'identité numérique.
4	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DOIVENT** s'assurer que les responsabilités de leur représentant désigné incluent le pouvoir d'intervenir dans les questions de protection de la vie privée spécifiquement reliées au rôle de l'organisation en tant qu'organisation divulgatrice ou requérante ou encore entité chargée du traitement des avis et consentements. Ce pouvoir peut être délégué, mais l'entité de traitement initiale demeure imputable. Cela assurera une approche holistique et uniforme du respect de la vie privée du sujet.
5	L'organisation requérante **DOIT** avoir un programme de gestion du respect de la vie privée qui inclut : • le cas échéant, des restrictions basées sur le genre d'organisations auprès desquelles les renseignements personnels spécifiques au sujet seront obtenus ou sur la raison pour laquelle les renseignements sont recueillis. Par exemple, il peut y avoir des restrictions basées sur le secteur ou l'environnement réglementaire (p. ex., santé, services financiers); • le cas échéant, les processus à suivre quand l'organisation divulgatrice précise à l'organisation requérante des exigences spécifiques concernant le traitement des renseignements personnels spécifiques au sujet; • le cas échéant, des restrictions sur le processus pour obtenir les renseignements personnels spécifiques au sujet; • les processus à suivre lorsque les renseignements personnels spécifiques au sujet sont obtenus par le biais du système d'identité numérique; • les processus à suivre quand les renseignements personnels spécifiques au sujet préalablement obtenus sont mis à jour, supprimés ou expirés;

	• des consignes précises à l'intention des sujets sur le partage des données pour les aider à savoir avec quelle partie ils devraient communiquer compte tenu de leur demande de renseignements; • des contrôles de la protection des données; et • une évaluation de l'incidence sur la protection de la vie privée, qui couvre explicitement l'utilisation des renseignements personnels spécifiques au sujet obtenus par le biais de l'écosystème de l'identité numérique. Suggérer de limiter la responsabilité de l'entité chargée du traitement des avis et consentements aux changements qui affectent l'état des consignes de consentement du sujet ayant été enregistrées. Suggérer d'apporter le changement suivant : « préalablement partagés sont mis à jour, supprimés ou expirés. L'entité chargée du traitement des avis et consentements doit avoir des processus en place pour gérer les changements qui affectent les consignes de consentement du sujet ayant été enregistrées, spécifiquement l'état des consignes de consentement. »
6	L'entité chargée du traitement des avis et consentements **DOIT** avoir un programme de gestion du respect de la vie privée qui inclut : • des restrictions sur l'utilisation des renseignements personnels stipulant que l'entité chargée du traitement des avis et consentements est un simple facilitateur, p. ex. l'entité chargée du traitement des avis et consentements ne devrait jamais être en possession des renseignements personnels spécifiques au sujet ni les stocker; • le cas échéant, les processus à suivre quand l'organisation divulgatrice impose des exigences spécifiques à l'entité chargée du traitement des avis et consentements relativement au traitement des renseignements personnels spécifiques au sujet; • les processus à suivre pour faciliter le partage des renseignements personnels spécifiques au sujet; • les processus à suivre pour la gestion du consentement par le sujet; • les processus à suivre lorsque les renseignements personnels spécifiques au sujet préalablement partagés sont mis à jour, supprimés ou expirés; • des consignes précises à l'intention des sujets sur le partage des renseignements personnels spécifiques au sujet pour les aider à savoir avec quelle partie ils devraient communiquer compte tenu de la nature de leur demande; • des contrôles sur la protection des données; et • une évaluation de l'incidence sur la protection de la vie privée qui couvre explicitement le rôle de la facilitation, en cherchant surtout à réduire (voire à éliminer) l'accès aux renseignements personnels spécifiques au sujet ou au service ou encore leur visibilité.

7	Le fournisseur de réseau **DOIT** avoir un programme de gestion du respect de la vie privée qui inclut : • des restrictions sur l'utilisation des renseignements personnels stipulant que le fournisseur de réseau n'est qu'un fournisseur, par exemple éventuellement que le fournisseur de réseau ne doit jamais être en possession des renseignements personnels spécifiques au sujet ni les stocker; • le cas échéant, les processus à suivre pour faciliter le partage des renseignements personnels spécifiques au sujet; les processus à suivre lorsque les renseignements personnels spécifiques au sujet préalablement partagés sont mis à jour, supprimés ou expirés; • des consignes précises à l'intention des sujets sur le partage des renseignements personnels spécifiques au sujet pour les aider à savoir avec quelle partie ils devraient communiquer compte tenu de la nature de leur demande; • des contrôles sur la protection des données; et une évaluation de l'incidence sur la protection de la vie privée qui couvre explicitement le rôle de la facilitation, en cherchant surtout à réduire (voire à éliminer) l'accès aux renseignements personnels spécifiques au sujet ou au service ou encore leur visibilité.
8	L'organe de gouvernance **DOIT :** • assurer l'imputabilité des organisations menant des activités dans l'écosystème de l'identité numérique; • le cas échéant, faire en sorte que les participants pertinents à l'écosystème de l'identité numérique satisfont aux exigences spécifiquement définies par une organisation en ce qui concerne les renseignements personnels spécifiques au sujet; • inclure des règles en matière de normes et d'interopérabilité faisant en sorte que toutes les parties qui interviennent 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; • inclure des procédures pour enquêter sur les atteintes à la vie privée et les gérer, notamment en évaluant le risque pour les personnes, et en signalant les cas aux organismes de réglementation et aux personnes; et • faciliter 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	L'organisation divulgatrice **DOIT** avoir l'assurance que le principe nº 2 est suivi par les organisations requérantes et les entités chargées du traitement des

	avis et consentements avant de leur communiquer des renseignements personnels.
2	L'organisation divulgatrice **DOIT** maintenir et préserver un calendrier relatif aux documents récupérables pour les dossiers de demande de renseignements et communications. Le calendrier peut consister en un seul événement (« demande et communication ponctuelles ») ou plusieurs événements compte tenu des circonstances de l'échange.
3	L'organisation requérante **DOIT** clairement indiquer le motif pour lequel les renseignements personnels du sujet sont obtenus par le biais 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 trois ans, 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 sont clairs, dépourvus de toute ambiguïté et pas trop généraux.
7	Avant que des renseignements personnels ne soient obtenus ou lorsqu'ils sont recueillis, l'entité chargée du traitement des avis et consentements **DOIT** expliquer par écrit 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.
9	L'organe de gouvernance **DOIT** s'assurer que les organisations qui mènent des activités à l'intérieur de l'écosystème de l'identité numérique satisfont aux critères de conformité du principe nº 2, et la preuve de la conformité des organisations requérantes peut être fournie aux organisations divulgatrices.
10	L'organe de gouvernance **DOIT** inclure des procédures pour enquêter sur les écarts par rapport au principe nº 2.
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 la demande d'avis et de consentement est claire et compréhensible, et qu'elle signifie quelque chose pour le sujet.
2	Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DEVRAIENT** s'assurer que le processus de consentement fournit assez, et non trop, de renseignements au sujet. Dans tous les cas, un moyen direct **DEVRAIT** être fourni au sujet pour lui permettre d'obtenir des renseignements supplémentaires, au besoin.
3	L'organisation divulgatrice **DOIT** s'assurer que l'entité chargée du traitement des avis et consentements s'acquitte de ses fonctions consistant à donner un avis et à enregistrer ou gérer le consentement d'une manière appropriée avant de divulguer les renseignements personnels spécifiques au sujet.
4	L'organisation divulgatrice **DOIT** s'assurer que des preuves suffisantes de l'avis et du consentement sont obtenues de l'entité chargée du traitement des avis et consentements, puis enregistrées d'une manière appropriée.
5	L'organisation divulgatrice **DOIT** confirmer que l'avis et le consentement ne sont ni expirés ni 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** être responsable de définir, 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-5 dans la composante « Avis et consentement » du CCP.
8	L'organisation requérante, dont émane la demande de consentement, **DOIT** être avant tout responsable de définir, dans le contenu de l'avis, la nature de la demande de partage. Remarque : La nature du partage dépend selon que la demande vaut pour une communication ponctuelle ou continue des renseignements personnels.
9	L'organisation requérante **DOIT** s'assurer que la demande est conforme au principe de la divulgation minimale.

10	L'organisation requérante **DOIT** s'assurer que l'entité chargée du traitement des avis et consentements remplit d'une façon appropriée sa fonction consistant à fournir et à enregistrer ou gérer le consentement avant de recevoir les renseignements personnels spécifiques au sujet.
11	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 d'une manière appropriée.
12	Quand l'organisation requérante est informée que le consentement n'est plus valide, elle **DOIT** cesser de recueillir d'autres renseignements personnels spécifiques au sujet qui sont basés sur ce consentement invalidé.
13	L'entité chargée du traitement des avis et consentements **DOIT** être responsable de fournir un avis au sujet à l'intérieur de l'écosystème de l'identité numérique.
14	L'entité chargée du traitement des avis et consentements **DOIT** s'assurer que l'avis reflète clairement la nature du partage à l'intérieur de l'écosystème de l'identité numérique. Remarque : La nature du partage dépend selon que la demande vaut pour une communication ponctuelle ou continue des renseignements personnels.
15	L'entité chargée du traitement des avis et consentements **DOIT** s'assurer ou se faire confirmer que le sujet est authentifié avant d'afficher des renseignements personnels spécifiques au sujet dans un avis adressé au sujet en validant son identité.
16	L'organisation divulgatrice **DOIT** déterminer la sensibilité des renseignements partagés et instaurer des règles (p. ex., politiques de masquage) pour l'affichage de renseignements sensibles dans l'avis.
17	L'entité chargée du traitement des avis et consentements **DOIT** être capable d'afficher des renseignements personnels dans l'avis conformément à n'importe quelles règles (p. ex., politiques de masquage) établies par l'organisation divulgatrice.
18	L'entité chargée du traitement des avis et consentements **DOIT** fournir un moyen de recueillir le consentement et de le communiquer aux autres parties intervenant dans la transaction sur l'identité numérique (organisations divulgatrice et requérante).
19	L'entité chargée du traitement des avis et consentements **DOIT** enregistrer le consentement et donner au sujet les moyens d'examiner et de gérer les consentements accordés.
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 toutes les limites organisationnelles sont maintenues et/ou préservées.

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.
22	Le fournisseur de réseau **PEUT** intervenir pour déterminer ou découvrir quelles organisations divulgatrices sont des sources potentielles des renseignements personnels demandés. Remarque : Comme alternative, par exemple, les organisations requérantes peuvent spécifier directement la source requise.
23	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.
24	L'organe de gouvernance **DOIT** fournir 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.
25	L'organe de gouvernance **DOIT** inclure des procédures pour enquêter sur les écarts par rapport au principe nº 3 et les gérer, qui consistent notamment à évaluer le risque pour les sujets et à signaler les violations aux organismes de réglementation et aux sujets.
26	L'organe de gouvernance **DOIT** inclure des dispositions qui font en sorte 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** avoir l'assurance que l'organisation requérante a une raison valable et suffisante d'obtenir les renseignements personnels demandés.
2	L'organisation requérante **DOIT** dissocier clairement les activités liées à l'obtention de renseignements par le biais de l'écosystème de l'identité numérique de ses autres activités.
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 dans le but spécifique d'utiliser l'écosystème de l'identité

	numérique, p. ex., pour permettre aux utilisateurs d'accéder aux services ou de prouver leur admissibilité.
4	L'organisation requérante **DOIT** documenter publiquement, ou rendre disponible, la nature des renseignements personnels recueillis et à quelle fin ils sont recueillis.
5	L'organisation requérante **DOIT** s'assurer d'indiquer aux employés applicables le genre de renseignements personnels recueillis et dans quel but afin de répondre avec exactitude aux demandes d'information de tierces parties.
6	L'organisation requérante **DOIT** indiquer d'une façon claire, non ambiguë et transparente la raison pour laquelle elle recueille des renseignements personnels dans toutes les formes de communication.
7	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.
8	Le fournisseur de réseau **DOIT** faciliter le partage des renseignements personnels.
9	L'organe de gouvernance **DOIT** avoir l'assurance que l'organisation requérante a une raison valable et suffisante de recueillir les renseignements personnels demandés.
10	L'organe de gouvernance **DOIT** définir des règles et 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.
11	L'organe de gouvernance **DOIT** inclure des procédures pour enquêter sur les écarts par rapport au principe n° 4 et les gérer, notamment en évaluant le risque pour les sujets et en signalant les violations aux organismes de réglementation et aux sujets.
LIMU	**Principe n° 5 – Limitation de l'utilisation, 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 communication dans l'écosystème de l'identité numérique.
3	S'il y a une politique définie sur la rétention minimale et maximale des données qui est spécifiée pour l'écosystème de l'identité numérique, l'organisation

	divulgatrice **DOIT** tenir compte de cette politique 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** limiter la communication des renseignements personnels du sujet à ceux qu'elle sait être exacts et à jour.
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.
8	L'organisation requérante **NE DOIT PAS** utiliser ou conserver, sans avoir obtenu le consentement approprié, les renseignements personnels spécifiques au sujet (reçus par le biais de l'écosystème de l'identité numérique) à des fins autres que celles qui sont spécifiées par le biais de l'entité chargée du traitement des avis et consentements au moment où ils sont recueillis.
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 nouveau de fournir des avis et d'obtenir des consentements dans l'écosystème de l'identité numérique. Idéalement, l'entité chargée du traitement des avis et consentements ne verra pas les renseignements personnels, ce qui 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	L'entité chargée du traitement des avis et consentements **DOIT** se débarrasser des renseignements personnels qui ne sont plus nécessaires pour les besoins reliés à l'identité numérique pour lesquels ils étaient conservés.
12	Le fournisseur de réseau **DOIT** faciliter l'établissement de systèmes pour partager les renseignements personnels.

13	L'autorité qui certifie **DOIT** définir les règles d'utilisation, de divulgation et de rétention de bout en bout des renseignements personnels créés en tant que produit dérivé de l'utilisation de l'écosystème de l'identité numérique.
14	L'autorité qui certifie **DOIT** définir et mettre en place des processus pour surveiller et faire appliquer les exigences relatives à l'utilisation, la communication et la rétention des renseignements personnels créés en tant que produit dérivé 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 qu'il existe un processus qu'un sujet doit suivre pour mettre à jour des renseignements personnels inexacts dans l'écosystème de l'identité numérique, et que ce processus établisse clairement les responsabilités de chaque partie à l'intérieur de l'écosystème de l'identité numérique, notamment celle de l'utilisateur.
2	L'organisation divulgatrice **DOIT** instaurer des politiques, procédures et systèmes pour repérer, corriger et gérer les renseignements personnels désuets (p. ex., en mettant à jour les dossiers du sujet). 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. Le profil « Personne vérifiée », en particulier la section Maintenance des identifiants, contient des 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 au sujet : 1. la possibilité d'examiner ses renseignements personnels spécifiques au sujet qui sont partagés; et 2. des instructions ou les moyens de mettre à jour les renseignements personnels spécifiques au sujet.
5	Lorsqu'on partage les renseignements concernant les services fournis à un sujet avec une organisation requérante, l'organisation divulgatrice ou l'entité chargée du traitement des avis et consentements **PEUT** donner au sujet :

	1. la possibilité d'examiner ses renseignements personnels spécifiques au sujet devant être partagés; et 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 au sujet la possibilité d'examiner un résumé ou une description des renseignements communiqués.
7	Lorsque les renseignements personnels obtenus de l'écosystème de l'identité numérique ne correspondent pas à ceux que l'organisation requérante possède, celle-ci **DOIT** résoudre la question en interne.
8	L'entité chargée du traitement des avis et consentements **DOIT** conserver une piste d'audit des renseignements sur les avis et consentements. 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 et instaurer des règles sur la façon dont l'exactitude des renseignements personnels peut être soutenue par l'écosystème de l'identité numérique. Cela peut inclure, par exemple, des services qui permettent (avec le consentement du sujet) de transmettre des mises à jour aux organisations requérantes abonnées.
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** s'assurer que des mesures de sécurité visant à protéger les renseignements personnels sont en place et communiquées au sujet (le cas échéant), et que des mesures de protection sont en place au cas où quelque chose irait mal.
2	L'organisation divulgatrice **DOIT** développer et mettre en place une politique de sécurité visant à protéger les renseignements personnels, 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 en cause.
3	L'organisation divulgatrice **DOIT** mettre en place des mesures de sécurité appropriées, conformément aux risques de préjudice identifiés dans l'évaluation des risques (évaluation des risques de menace et/ou de l'impact sur le respect de la vie privée, selon le cas), pour protéger l'accès aux renseignements personnels au repos et en transit.
4	L'organisation divulgatrice **DOIT** employer des mesures de sécurité, conformément aux risques de préjudice identifiés dans l'évaluation

	des risques (évaluation des risques de menace et/ou de l'impact sur le respect de la vie privée, selon le cas), appropriées à la sensibilité des renseignements personnels du sujet et au risque de fraude ou d'utilisation malveillante.
5	L'organisation divulgatrice **DOIT** examiner et mettre à jour régulièrement les mesures de sécurité reliées à l'écosystème de l'identité numérique.
6	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 des systèmes d'identité numérique en cause.
7	L'organisation requérante **DOIT** mettre en place des mesures de sécurité appropriées pour protéger l'accès aux renseignements personnels, au repos et en transit.
8	L'organisation requérante **DOIT** employer des mesures de sécurité appropriées à la sensibilité des renseignements personnels du sujet et au risque de fraude ou d'utilisation malveillante.
9	L'organisation requérante **DOIT** examiner et mettre à jour régulièrement les mesures de sécurité reliées à l'écosystème de l'identité numérique.
10	L'entité chargée du traitement des avis et consentements **DOIT** développer et mettre en place une politique de sécurité pour protéger les renseignements personnels, qui inclut spécifiquement les mesures de protection employées dans les processus d'avis et de consentement.
11	L'entité chargée du traitement des avis et consentements **DOIT** mettre en place des mesures de sécurité appropriées.
12	L'entité chargée du traitement des avis et consentements **DOIT** employer des mesures de sécurité appropriées à la sensibilité des renseignements personnels présentés au sujet dans l'avis sur la protection de la vie privée et au risque de fraude ou d'utilisation malveillante.
13	L'entité chargée du traitement des avis et consentements **DOIT** examiner et mettre à jour régulièrement les mesures de sécurité reliées à l'écosystème de l'identité numérique.
14	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 qu'il donne aux renseignements personnels.
15	Le fournisseur de réseau **DOIT** mettre en place des mesures de sécurité appropriées.
16	Le fournisseur de réseau **DOIT** examiner et mettre à jour régulièrement les mesures de sécurité reliées à l'écosystème de l'identité numérique.

17	L'organe de gouvernance **DOIT** 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.
18	Les participants à l'écosystème de l'identité numérique **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 n° 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 sur-le-champ des renseignements clairs et compréhensibles sur l'écosystème de l'identité numérique, la façon dont la vie privée du sujet est protégée, l'endroit où il peut obtenir de plus amples renseignements et 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** fournir de l'aide et des conseils lorsqu'un sujet fait une demande d'accès concernant une partie différente de l'écosystème de l'identité numérique. Cela peut consister pour le sujet 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	L'organisation divulgatrice **DOIT** fournir aux utilisateurs des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance.
4	L'organisation divulgatrice **DOIT** s'assurer que les renseignements sur son rôle sont clairement dissociés des autres services et fonctions qu'elle fournit (qui ne font pas partie de l'écosystème de l'identité numérique en soi).
5	L'organisation requérante **DOIT** fournir aux utilisateurs des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance.
6	L'organisation requérante **DOIT** s'assurer que les renseignements sur son rôle sont clairement dissociés des autres services et fonctions qu'elle fournit (qui ne font pas partie de l'écosystème de l'identité numérique en soi).
7	L'entité chargée du traitement des avis et consentements **DOIT** fournir aux utilisateurs des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance.
8	L'entité chargée du traitement des avis et consentements **DOIT** s'assurer que les renseignements sur son rôle sont clairement dissociés des autres services

	et fonctions qu'elle fournit (qui ne font pas partie de l'écosystème de l'identité numérique en soi).
9	Le fournisseur de réseau **DOIT** fournir aux utilisateurs des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance.
10	Le fournisseur de réseau **DOIT** s'assurer que les renseignements sur son rôle sont clairement dissociés des autres services et fonctions qu'il fournit (qui ne font pas partie de l'écosystème de l'identité numérique en soi).
11	L'organe de gouvernance **DOIT** s'assurer que les politiques et pratiques de gestion des renseignements personnels utilisées par l'écosystème de l'identité numérique sont claires, uniformes et complètes.
12	L'organe de gouvernance **DOIT** collaborer avec les participants à l'écosystème pour s'assurer que les renseignements sur les politiques et pratiques en matière de protection de la vie privée exigées par le critère 8 sur l'ouverture sont présentés d'une manière uniforme afin d'éviter des messages conflictuels ou qui portent à confusion.
13	L'organe de gouvernance **DOIT** fournir à tous les participants des lignes directrices sur la conformité aux exigences énoncées plus haut dans cette section et examiner la conformité des participants afin de s'assurer qu'ils suivent les lignes directrices.
14	L'organe de gouvernance **DOIT** s'assurer qu'il y a des processus en place pour répondre à une demande d'information de la part 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	Les participants à l'écosystème de l'identité numérique fourniront souvent des fonctionnalités intégrées qui renseignent automatiquement le sujet sur l'existence, l'utilisation et la communication de ses renseignements personnels dans l'écosystème de l'identité numérique. Lorsque de telles fonctionnalités existent, les organisations divulgatrices et requérantes ainsi que les entités chargées du traitement des avis et consentements **DOIVENT** s'assurer que le principe de l'accès individuel (tel que décrit dans la LPRPDE) est respecté. Lorsque les participants à l'écosystème de l'identité numérique ne fournissent pas des fonctionnalités intégrées procurant à l'utilisateur de l'information sur l'existence, l'utilisation et la communication de ses renseignements personnels, le processus pour obtenir une telle information **DOIT** être clair, direct et conforme à la LPRPDE ou toute autre loi pertinente.
2	L'organisation divulgatrice **DOIT** fournir à l'utilisateur des moyens clairs d'obtenir de l'information sur l'existence, l'utilisation et la communication de

	ses renseignements personnels ayant trait au traitement des renseignements dans le contexte de l'écosystème de l'identité numérique.
3	L'organisation requérante **DOIT** fournir au sujet des moyens clairs d'obtenir de l'information sur l'existence et l'utilisation de ses renseignements personnels par le biais de l'écosystème de l'identité numérique.
4	Si l'organisation requérante détermine que les renseignements personnels qu'elle reçoit de l'écosystème de l'identité numérique sont inexacts ou incomplets, il **PEUT** exister des processus pour aviser l'organisation communicante pertinente du problème.
5	L'entité chargée du traitement des avis et consentements **DOIT** fournir à l'utilisateur des moyens clairs pour obtenir auprès d'elle de l'information sur l'existence, l'utilisation et la communication de ses renseignements personnels. Étant donné que l'entité chargée du traitement des avis et consentements est là pour faciliter le partage des renseignements personnels mais qu'elle ne les utilise pas ensuite, l'« accès individuel » risque de se limiter à voir la piste d'audit des activités d'avis et de consentement reliées au sujet.
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 au principe de l'« accès individuel » de la LPRPDE.
7	Les mesures de gouvernance prises par l'organe de gouvernance **DOIVENT** faire en sorte que les processus et les lignes directrices concernant l'« accès individuel » sont fournis 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 simples et disponibles.
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 : • dissocie d'une façon claire et simple l'implication dans l'écosystème de l'identité numérique des autres activités de l'organisation; et

	• 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** mettre en place des processus pour trier et transmettre les plaintes de sorte que le sujet reçoive le soutien nécessaire du bon participant, d'une manière aussi efficace et claire que possible.
4	L'organe de gouvernance **DOIT** inclure des procédures sur la façon d'aviser les plaignants, de leur répondre sans délai, et de consigner les décisions et les mesures afin d'assurer une uniformité avec le profil de conformité au respect de la vie privée et de protéger les participants à l'écosystème de l'identité numérique.

3 Historique des révisions

Numéro de version	Date de publication	Auteurs	Description
0.01	2018-10-31	Consult Hyperion	Ébauche de travail initiale
0.02	2017-03-26	CCIAN	Changement de termes utilisés pour les rôles • « Réseau » remplacé par « fournisseur de réseau » • « Écosystème » remplacé par « 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 du 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	Intégration des commentaires résultant de l'examen par le TFEC de l'ébauche de discussion
0.06	2019-10-31	Équipes de conception « Respect de la vie privée » et de rédaction du CCP	Révision du contenu basée sur les commentaires découlant de l'examen ouvert de l'ébauche de discussion
0.07	2019-11-22	Équipe de rédaction du CCP	Application de la présentation standard pour l'aperçu du CCP, qui consolide 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 à la suite de l'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 pour examiner les commentaires du TFEC
1.0	2020-02-12	Équipe de rédaction du CCP	Approbation de l'ébauche de recommandations V1.0
1.1	2020-05-20	Équipe de rédaction du CCP	« Organe de gouvernance » changé pour « autorité qui certifie » pour concorder avec la composante « Évaluation »

1.2	2020-05-28	Équipe de rédaction du CCP	Ébauche mise à jour conformément aux commentaires et résolutions de l'examen ouvert
1.0	2020-07-02	Équipe de rédaction du CCP	Recommandation finale V1.0