Ébauche de recommandations pour le profil de conformité en matière de respect de la vie privée du Cadre de confiance pancanadien V1.0

Cette ébauche de recommandations a été préparée par le Comité d'experts du Cadre de confiance (TFEC) du Conseil canadien de l'identification et de l'authentification numériques (CCIAN). Le TFEC est régi par les politiques du CCIAN en matière de contrôle. Les commentaires soumis par le public sont assujettis à l'entente de contributeur du CCIAN.

Le CCIAN prévoit modifier et améliorer cette ébauche de recommandations en fonction des commentaires du public. Les commentaires ouverts ont pour but d'assurer la transparence de l'élaboration et la diversité d'un apport véritablement pancanadien. Les commentaires effectués pendant l'examen seront pris en considération en vue d'être incorporés dans la prochaine ébauche. Le CCIAN va regrouper les commentaires afin de montrer d'une façon transparente comment chacun a été traité.

Les prochaines versions du Cadre de confiance pancanadien vont étoffer, clarifier et peaufiner le contenu de ce document.

Table des matières

1 Introduction au profil de conformité en matière de respect de la vie privée du Cadre de confiance pancanadien 2

1.1 Mots clés des critères de conformité 2

2 Critères de conformité de la composante « Respect de la vie privée » 2

---

1 Introduction au profil de conformité en matière de respect de la vie privée du Cadre de confiance pancanadien

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

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 n° 1 des critères de conformité de base »).

Référence	Critères de conformité
BASE	**Critère de base** **Remarque :** Les exigences pour les cas où le sujet agit comme l'organisation communicante ne sont pas abordées dans cette version des critères de conformité de base.
1	Les organisations communicantes 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 communicantes 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 communicantes 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.

72	4	Les organisations communicantes 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.
73	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.
74	6	Dans le cadre de leurs programmes de gestion du respect de la vie privée, les organisations communicantes 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, ce qui inclut les étapes d'évaluation des dommages ou torts, de signalement, de confinement, de correction et de prévention.
75	7	L'organe de gouvernance **DOIT** définir et gérer d'une manière claire les limites de l'écosystème de l'identité numérique.
76	**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.*
77	1	Les organisations communicantes et requérantes, les entités chargées du traitement des avis et consentements, les fournisseurs de réseau et l'organe de gouvernance **DOIVENT** s'assurer que le sujet sait clairement qui est responsable du respect de la vie privée dans leurs organisations respectives.
78	2	Les organisations communicantes et requérantes, les entités chargées du traitement des avis et consentements, les fournisseurs de réseau et l'organe de gouvernance **DOIVENT** mettre à la disposition du sujet le nom ou le titre de la personne responsable du respect de la vie privée et lui donner les moyens de communiquer avec cette personne.

79	3	L'organisation communicante **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 sujets 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.
80	4	Les organisations communicantes et requérantes, et les entités chargées du traitement des avis et consentements **DOIVENT** s'assurer que leur responsable désigné du respect de la vie privée a notamment le pouvoir d'intervenir dans les questions de protection de la vie privée spécifiquement reliées au rôle de l'organisation en tant qu'organisation communicante 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 assure une approche holistique et uniforme du respect de la vie privée du sujet.

81	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 communicante 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.

82	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 communicante 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.
83	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.

84	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.
85	**IDEN**	**Principe n° 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.*
86	1	L'organisation communicante **DOIT** avoir l'assurance que le principe n° 2 est suivi par les organisations requérantes et les entités chargées du traitement des avis et consentements avant de leur communiquer des renseignements personnels.
87	2	L'organisation communicante **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.
88	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.
89	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.
90	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.
91	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.

92	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.
93	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.
94	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 se conforment aux critères de performance énumérés pour le principe nº 2, et la preuve de la conformité des organisations requérantes peut être fournie aux organisations communicantes.
95	10	L'organe de gouvernance **DOIT** inclure des procédures pour enquêter sur les écarts par rapport au principe nº 2.
96	**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.*
97	1	Les organisations communicantes 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.
98	2	Les organisations communicantes 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.
99	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.
100	4	L'organisation communicante **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 stockées d'une manière appropriée.
101	5	L'organisation divulgatrice **DOIT** confirmer que le consentement n'est ni expiré ni révoqué 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 n'est pas valide.

102	6	L'organisation communicante **DOIT** s'assurer que le sujet comprend la nature, le but et les risques associés à l'utilisation ou la divulgation de ses 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 Cadre de confiance pancanadien.
103	7	L'organisation requérante est à l'origine de la demande de consentement et **DOIT** donc être avant tout 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 Cadre de confiance pancanadien.
104	8	L'organisation requérante est à l'origine de la demande de consentement et **DOIT** donc 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.
105	9	L'organisation requérante **DOIT** s'assurer que la demande est conforme au principe de la divulgation minimale.
106	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.
107	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.
108	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.
109	13	L'entité chargée du traitement des avis et consentements **DOIT** être responsable de fournir un avis au sujet dans l'écosystème de l'identité numérique.
110	14	L'entité chargée du traitement des avis et consentements **DOIT** s'assurer que l'avis reflète clairement la nature du partage dans 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.
111	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.
112	16	L'organisation communicante **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.

113	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 communicante.
114	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 communicante et requérante).
115	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.
116	20	Pour les transactions liées à l'identité où le consentement est géré entre plusieurs organisations requérantes et communicantes, l'entité chargée du traitement des avis et consentements **DOIT** s'assurer que toutes les limites organisationnelles sont maintenues et/ou préservées.
117	21	L'entité chargée du traitement des avis et consentements **DOIT** avoir des processus en place pour soutenir la révocation du consentement. Cela pourrait émaner du sujet ou être, par exemple, une réponse à une fraude décelée.
118	22	Le fournisseur de réseau **PEUT** intervenir pour déterminer ou découvrir quelles organisations communicantes sont des sources potentielles des renseignements personnels demandés. Remarque : Comme alternative, par exemple, les organisations requérantes peuvent spécifier directement la source requise.
119	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.
120	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.
121	25	L'organe de gouvernance **DOIT** inclure des procédures pour enquêter sur les écarts par rapport au principe n° 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.
122	26	L'organe de gouvernance **DOIT** inclure des provisions qui font en sorte que la révocation du consentement par un sujet devient rapidement effective dans tout l'écosystème de l'identité numérique.
123	**LIMC**	**Principe n° 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.*

124	1	L'organisation communicante **DOIT** avoir l'assurance que l'organisation requérante une raison valable et suffisante d'obtenir les renseignements personnels demandés.
125	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 des autres activités de l'organisation requérante.
126	3	L'organisation requérante **DOIT** limiter les renseignements personnels obtenus par le biais de l'écosystème de l'identité numérique à ce qui est nécessaire pour l'utilisation spécifique de ce dernier, p. ex., pour permettre aux sujets d'accéder à des services ou de prouver leur admissibilité.
127	4	L'organisation requérante **DOIT** documenter publiquement, ou rendre disponible, le genre de renseignements personnels recueillis et dans quel but.
128	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.
129	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.
130	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.
131	8	Le fournisseur de réseau **DOIT** faciliter le partage des renseignements personnels.
132	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.
133	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.
134	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.
135	**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.*
136	1	L'organisation communicante **DOIT** avoir des politiques internes et d'autres documents pour limiter l'utilisation, la divulgation et la rétention des renseignements personnels spécifiques au sujet.

137	2	L'organisation communicante **DOIT** documenter l'utilisation des renseignements personnels du sujet pour les besoins de la communication dans l'écosystème de l'identité numérique.
138	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 communicante **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.
139	4	À moins que la loi ne permette ou n'exige autre chose, l'organisation communicante **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.
140	5	L'organisation communicante **DOIT** limiter la communication des renseignements personnels du sujet à ceux qu'elle sait être exacts et à jour.
141	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.
142	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.
143	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.
144	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.
145	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.
146	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.
147	12	Le fournisseur de réseau **DOIT** faciliter l'établissement de systèmes pour partager les renseignements personnels.

148	13	L'organe de gouvernance **DOIT** définir les règles d'utilisation, de communication 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.
149	14	L'organe de gouvernance **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.
150	**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.*
151	1	Les organisations communicantes 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 soit clair et direct.
152	2	L'organisation communicante **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.
153	3	L'organisation communicante **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.
154	4	Lorsqu'elle partage les renseignements personnels d'un sujet avec une organisation requérante, l'organisation communicante **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.
155	5	Lorsqu'on partage les renseignements concernant les services fournis à un sujet avec une organisation requérante, l'organisation communicante 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.

156	6	Pour vérifier l'exactitude des renseignements personnels reçus de l'organisation communicante, l'organisation requérante **DEVRAIT** donner au sujet la possibilité d'examiner un résumé ou une description des renseignements communiqués.
157	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.
158	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.
159	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.
160	**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.*
161	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.
162	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.
163	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.
164	4	L'organisation communicante **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.
165	5	L'organisation communicante **DOIT** examiner et mettre à jour régulièrement les mesures de sécurité reliées à l'écosystème de l'identité numérique.

166	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.
167	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.
168	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.
169	9	L'organisation requérante **DOIT** examiner et mettre à jour régulièrement les mesures de sécurité reliées à l'écosystème de l'identité numérique.
170	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.
171	11	L'entité chargée du traitement des avis et consentements **DOIT** mettre en place des mesures de sécurité appropriées.
172	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.
173	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.
174	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.
175	15	Le fournisseur de réseau **DOIT** mettre en place des mesures de sécurité appropriées.
176	16	Le fournisseur de réseau **DOIT** examiner et mettre à jour régulièrement les mesures de sécurité reliées à l'écosystème de l'identité numérique.
177	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 des normes de sécurité minimales.
178	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.

179	**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.*
180	1	Les organisations communicantes 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.
181	2	Les organisations communicantes 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.
182	3	L'organisation communicante **DOIT** fournir aux sujets des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance.
183	4	L'organisation communicante **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).
184	5	L'organisation requérante **DOIT** fournir aux sujets des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance.
185	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).
186	7	L'entité chargée du traitement des avis et consentements **DOIT** fournir aux sujets des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance.
187	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).
188	9	Le fournisseur de réseau **DOIT** fournir aux sujets des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance.
189	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).
190	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.

191	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.
192	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.
193	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 du sujet.
194	**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.*
195	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 communicantes 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 au sujet 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.
196	2	L'organisation requérante **DOIT** fournir au sujet 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.
197	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.
198	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.

199	5	L'entité chargée du traitement des avis et consentements **DOIT** fournir au sujet des moyens clairs pour obtenir de l'information sur l'existence, l'utilisation et la communication de ses renseignements personnels auprès de l'entité chargée du traitement des avis et consentements. 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.
200	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.
201	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.
202	**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.*
203	1	Le nom ou le titre de la personne responsable de la conformité au sein de l'organisation communicante, 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 eux **DOIVENT** être simples et disponibles.
204	2	Les organisations communicantes 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 le sujet à obtenir le soutien voulu, même si la plainte doit être adressée à un autre participant dans l'écosystème de l'identité numérique.
205	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.
206	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.

Tableau 1. Critères de conformité de la composante « Respect de la vie privée » du Cadre de confiance pancanadien