# Document de travail sur le profil de conformité en matière de respect de la vie privée
# Version 0.12

Ce document de travail a été préparé par le Comité d'experts du cadre de confiance (TFEC) du Digital ID & Authentication Council of Canada (DIACC). Le TFEC est régi par les politiques du DIACC en matière de contrôle. Les commentaires soumis par le public sont assujettis à l'entente de contributeur du DIACC.

Le DIACC prévoit modifier et améliorer ce document de travail 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 DIACC 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. L'auditoire ciblé inclut des décideurs qui peuvent être ou non des experts dans la technologie des domaines.

---

En examinant cette ébauche, veuillez tenir compte de ce qui suit :

1. La structure générale et le ton couvrent-ils d'une façon appropriée le respect de la vie privée dans le contexte de l'identité numérique?
2. Les documents réussissent-ils à formuler des exigences en matière de respect de la vie privée pour l'identité numérique alignées sur les principes de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) sans toutefois répéter ce que la LPRPDE dit?
3. Les critères de conformité sont-ils suffisamment clairs et sans ambiguïté pour s'appliquer à votre contexte?
4. La distinction entre les renseignements personnels du sujet et l'information sur les services est-elle censée et/ou s'applique-t-elle dans votre contexte?

Remarques :

- La gouvernance du respect de la vie privée et des autres composantes du cadre de confiance pancanadien fait partie de discussions permanentes. Les commentaires découlant de cet examen de la gouvernance seront transmis à l'équipe de conception de la gouvernance du cadre de confiance pancanadien.
- Les exigences concernant le respect de la vie privée qui sont spécifiques aux processus d'avis et de consentement sont détaillées dans la composante « Avis et consentement » du cadre de confiance pancanadien.

# Table des matières



# 1 Introduction au profil de conformité en matière de respect de la vie privée

Les critères de conformité pour la composante « Respect de la vie privée » spécifient la façon dont les principes relatifs à l'équité dans le traitement de l'information de la LPRPDE, définis par le Commissariat à la protection de la vie privée du Canada, sont pertinents ou s'appliquent au traitement des données sur l'identité numérique (remarque : ils ne visent pas à remplacer des règlements existants; on s'attend à ce que les organismes se conforment aux règlements sur le respect de la vie privée qui sont en vigueur dans leur territoire de compétence).

## 1.1 Relation avec le cadre de confiance pancanadien

Le cadre de confiance pancanadien consiste en une série de composantes modulaires ou fonctionnelles pouvant être évaluées et certifiées indépendamment pour être considérées comme des éléments de confiance. Le cadre de confiance pancanadien, qui mise sur une approche pancanadienne, permet au public et au secteur privé de collaborer pour préserver les identités numériques en uniformisant les processus et les pratiques dans tout l'écosystème numérique canadien.

La figure 1 illustre l'ébauche visuelle du modèle de cadre de confiance pancanadien. La composante « Respect de la vie privée » s'applique à toutes les sous-composantes.

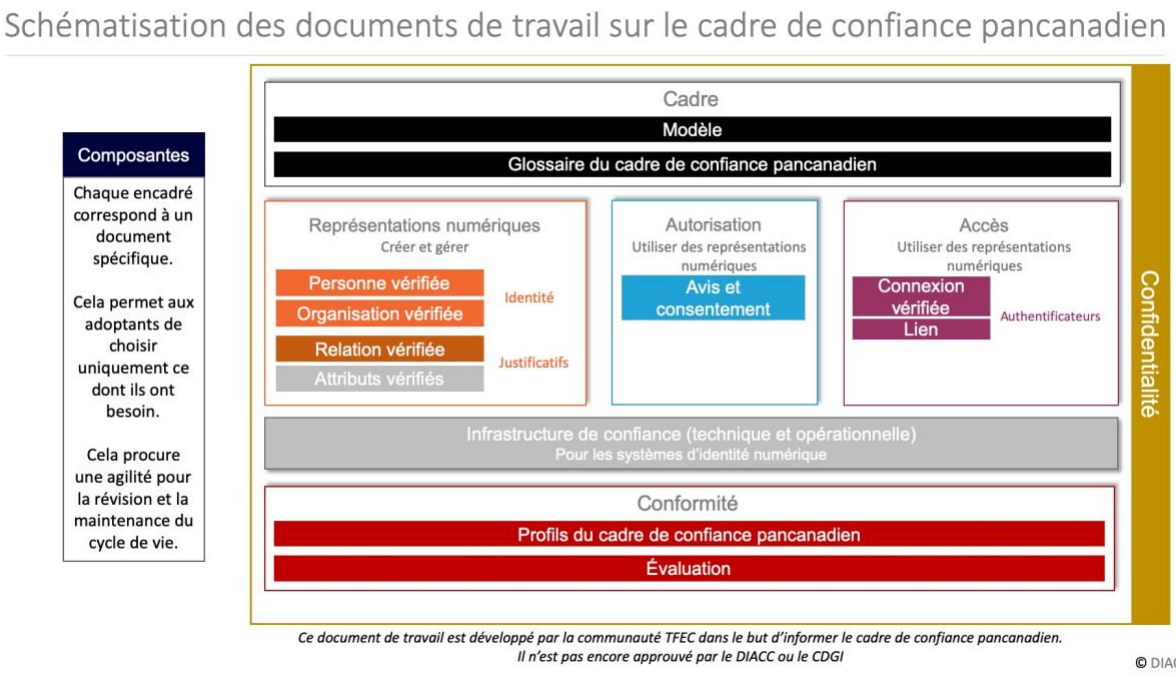


**Figure 1. Ébauche visuelle du modèle de cadre de confiance pancanadien**

## 1.2 Mots clés

Afin d'assurer une application uniforme, les mots clés indiqués en **gras** dans les critères de conformité doivent être interprétés comme suit :

- **DOIT** signifie qu'il s'agit d'une exigence impérative des critères de conformité;
- **NE DOIT PAS** signifie qu'il s'agit d'une interdiction impérative des critères de conformité;
- **DEVRAIT** signifie que même s'il peut y avoir des raisons valables dans des circonstances particulières pour ignorer l'exigence, il faut comprendre toutes les implications et les évaluer soigneusement avant de décider de ne pas respecter les critères de conformité ou de choisir une option différente de ce qui est spécifié par les critères de conformité;
- **NE DEVRAIT PAS** signifie qu'il peut y avoir une raison valable dans des circonstances particulières où l'exigence est acceptable ou même utile, mais qu'on devrait comprendre toutes les implications et évaluer soigneusement le cas avant de décider de ne pas se conformer à l'exigence telle que décrite;
- **PEUT** signifie que l'exigence est discrétionnaire mais recommandée.

D'autres mots clés, comme des définitions normatives dans des normes et spécifications connexes, seront également indiqués en **gras**.

## 1.3 Définitions

Il y a deux types de renseignements personnels :

- **Renseignements sur les services –** renseignements recueillis ou fournis par les participants (organisation divulgatrice, organisation requérante, entité(s) chargée(s) du traitement des avis et consentements ou fournisseur de réseau) pour les besoins de l'exploitation et du maintien du service (p. ex., pseudonymes spécifiques aux services, dossiers de transactions, preuves de transactions avec consentement).
- **Renseignements personnels du sujet –** renseignements qu'un sujet consent à partager entre une organisation divulgatrice et une organisation requérante (p. ex., nom, adresse de courriel, numéro de téléphone, adresse postale, date de naissance, renseignements sur les comptes).

## 1.4 Rôles

Les rôles suivants sont définis pour couvrir la portée de la composante « Respect de la vie privée ». Compte tenu de l'utilisation, différentes organisations peuvent assumer un ou plusieurs rôles.

- **Écosystème de l'identité numérique –** ensemble d'organisations des secteurs public et privé (p. ex., gouvernement, entreprises, organismes sans but lucratif et autres entités) qui offrent et utilisent des services d'identité numérique, et qui acceptent de se conformer à une série commune de critères de conformité pour leurs processus commerciaux et techniques lorsqu'elles échangent des renseignements sur l'identité numérique pour assurer la fiabilité des transactions électroniques.
- **Organisation divulgatrice –** organisation qui détient les renseignements personnels du sujet, que ce dernier consent à divulguer à une organisation requérante. Dans le contexte de l'identité numérique, il s'agira souvent d'un fournisseur d'identités ou d'attributs.

- **Organe de gouvernance –** organisation qui supervise le cadre de confiance et les exigences connexes de l'écosystème de l'identité numérique. Cela pourrait consister à fournir une gouvernance ainsi que des arrangements opérationnels, techniques ou commerciaux entre les parties à la transaction.
- **Entité chargée du traitement des avis et consentements –** organisation qui avise le sujet de la demande de renseignements personnels (de la part de l'organisation requérante), obtient et enregistre le consentement, et fournit au sujet les moyens de gérer par la suite le consentement, y compris de le reprendre.
- **Fournisseur de réseau –** organisation qui relie les parties ensemble dans une transaction multipartite sur l'identité. Il s'agit d'un participant actif qui ajoute de la valeur à la prestation du service d'identité numérique (p. ex., ce n'est pas un fournisseur de services internet qui procure passivement une connectivité internet).
- **Organisation requérante –** organisation à qui le sujet consent à divulguer des renseignements personnels. Dans le contexte de l'identité numérique, il s'agira souvent d'un fournisseur de services ou d'une partie dépendante.
- **Sujet –** personne naturelle à qui appartiennent les renseignements personnels en question (remarque : le présent document ne traite pas de l'autorité déléguée).

Ces rôles aident à isoler les différentes fonctions et responsabilités dans le processus intégral de respect de la vie privée. Ils ne visent pas à impliquer une solution, une architecture ou une mise en œuvre en particulier.

Dans certains cas, par exemple, l'avis et le consentement peuvent provenir d'une organisation qui facilite l'échange de renseignements personnels entre le sujet, l'organisation divulgatrice et l'organisation requérante. Dans d'autres cas, l'avis et le consentement peuvent être fournis directement par l'organisation divulgatrice ou requérante, auquel cas cette organisation sera aussi responsable du traitement de l'avis et du consentement.

# 2 Principes de confiance et critères de conformité

Les critères de conformité qui suivent sont organisés et prévus pour s'aligner sur les 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$^{o}$ 1 des critères de conformité de base »).

| Référence | Critère de conformité |
|---|---|
| **BASE** | **Critère de base**<br><br>**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 du traitement des avis et consentements, les fournisseurs de réseau et l'organe de gouvernance **DOIVENT** avoir un programme de gestion de la vie privée en place pour assurer la conformité juridique, notamment la mise en œuvre des politiques, pratiques, contrôles et outils d'évaluation en matière de respect de la vie privée. |

| | | |
|---|---|---|
| 133 | 2 | 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 en place un agent de protection de la vie privée qui est responsable de superviser le programme de gestion de la vie privée et les audits ou examens internes des pratiques de traitement des renseignements personnels (notamment ceux reliés à la communication de l'avis et à l'obtention du consentement). |
| 134 | 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 protection de la vie privée qui :<br>• fournit une description de ses pratiques de traitement des renseignements personnels; et<br>• est facilement accessible, simple à lire et mise à jour au besoin. |
| 135 | 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) pour s'assurer que les renseignements personnels sont traités de la façon décrite dans leur politique de respect de la vie privée. |
| 136 | 5 | L'organe de gouvernance **DOIT** s'assurer que les organisations menant des activités à l'intérieur de l'écosystème de l'identité numérique suivent les principes 1 à 10. |
| 137 | 6 | Dans le cadre de leurs programmes de gestion de la confidentialité, 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, ce qui inclut les étapes de signalement, confinement, correction et prévention. |
| 138 | **ACCO** | **Principe nº 1 - Imputabilité**<br><br>*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 relatifs à l'équité en matière d'information.* |
| 139 | 1 | Les organisations divulgatrices 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 de la protection de la vie privée dans leurs organisations respectives. Les organisations divulgatrices et requérantes, les entités chargées du traitement des avis et consentements, les fournisseurs de réseau et l'organe de gouvernance **DOIVENT** fournir au sujet le nom ou le titre de cette personne, ainsi que les moyens d'entrer en contact avec elle. |

| | | |
|---|---|---|
| 140 | 2 | L'organisation divulgatrice **DOIT** avoir un programme de gestion de la confidentialité qui inclut :<br>• des restrictions quant aux types d'organisations avec lesquelles les renseignements personnels du sujet seront partagés, entre autres basées sur le secteur ou l'environnement réglementaire (p. ex., santé, services financiers);<br>• le cas échéant, la spécification des exigences que les participants à l'écosystème de l'identité numérique doivent remplir en ce qui concerne le traitement des renseignements personnels du sujet;<br>• des restrictions sur le processus de partage des renseignements personnels du sujet, p. ex., le niveau d'assurance nécessaire;<br>• les processus à suivre lorsque les renseignements personnels du sujet sont partagés;<br>• les processus à suivre lorsque les renseignements personnels du sujet ayant déjà été partagés sont mis à jour, supprimés ou expirés;<br>• des consignes précises à l'intention du sujet sur le partage de ses renseignements personnels pour l'aider à savoir avec quelle partie il devrait communiquer compte tenu de la nature de sa demande de renseignements; et<br>• une évaluation de l'incidence sur la confidentialité, qui couvre explicitement le partage des renseignements personnels du sujet par le biais de l'écosystème de l'identité numérique. |
| 141 | 3 | L'organisation divulgatrice **DOIT** s'assurer que les responsabilités de la personne désignée pour s'occuper du respect de la vie privée incluent le pouvoir d'intervenir dans les questions de confidentialité spécifiquement reliées au rôle de l'organisation divulgatrice. Cela assurera une approche holistique et uniforme de la protection de la vie privée du sujet. |
| 142 | 4 | L'organisation requérante **DOIT** avoir un programme de gestion de la confidentialité qui inclut :<br>• des restrictions quant aux types d'organisations auprès desquelles les renseignements personnels du sujet seront obtenus, entre autres basées sur le secteur ou l'environnement réglementaire (p. ex., santé, services financiers);<br>• le cas échéant, les processus que l'organisation requérante doit suivre pour se conformer aux exigences spécifiques définies par une organisation divulgatrice en ce qui concerne les renseignements personnels du sujet;<br>• des restrictions sur le processus employé pour obtenir les renseignements personnels du sujet, p. ex., le niveau d'assurance nécessaire;<br>• les processus à suivre lorsque les renseignements personnels du sujet sont obtenus par le biais du système d'identité numérique;<br>• les processus à suivre lorsque les renseignements personnels du sujet préalablement obtenus sont mis à jour, supprimés ou expirés;<br>• des consignes précises à l'intention du sujet sur le partage de ses renseignements personnels pour l'aider à savoir avec quelle partie il devrait communiquer compte tenu de la nature de sa demande de renseignements; et<br>• une évaluation de l'incidence sur la confidentialité, qui couvre explicitement l'utilisation des renseignements personnels du sujet obtenus par le biais de l'écosystème de l'identité numérique. |

| | | |
|---|---|---|
| 143 | 5 | L'organisation requérante **DOIT** s'assurer que les responsabilités de la personne désignée pour s'occuper du respect de la vie privée incluent le pouvoir d'intervenir dans les questions de confidentialité spécifiquement reliées au rôle de l'organisation requérante. Cela assurera une approche holistique et uniforme de la protection de la vie privée du sujet. |
| 144 | 6 | L'entité chargée du traitement des avis et consentements **DOIT** avoir un programme de gestion de la confidentialité qui inclut :<br>• 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., elle ne devrait jamais être en possession des renseignements personnels du sujet ni les stocker;<br>• le cas échéant, les processus que l'entité chargée du traitement des avis et consentements doit suivre afin de se conformer à des exigences spécifiquement définies par une organisation divulgatrice à propos des renseignements personnels du sujet;<br>• les processus à suivre pour faciliter le partage des renseignements personnels du sujet;<br>• les processus à suivre lorsque les renseignements personnels du sujet préalablement partagés sont mis à jour, supprimés ou expirés;<br>• des consignes précises à l'intention du sujet sur le partage de ses renseignements personnels pour l'aider à savoir avec quelle partie il devrait communiquer compte tenu de la nature de sa demande de renseignements; et<br>• une évaluation de l'incidence sur la confidentialité qui couvre explicitement le rôle de facilitation, en cherchant surtout à réduire (voire éliminer) l'accès aux renseignements personnels ou à l'information sur les services ou encore leur visibilité. |
| 145 | 7 | L'entité chargée du traitement des avis et consentements **DOIT** s'assurer que les responsabilités de la personne désignée pour s'occuper du respect de la vie privée incluent le pouvoir d'intervenir dans les questions de confidentialité spécifiquement reliées au rôle de l'organisation chargée du traitement des avis et consentements. Cela assurera une approche holistique et uniforme de la protection de la vie privée du sujet. |

| | | |
|---|---|---|
| 146 | 8 | Le fournisseur de réseau **DOIT** avoir un programme de gestion de la confidentialité qui inclut :<br>• des restrictions sur l'utilisation des renseignements personnels stipulant que le fournisseur de réseau est un simple facilitateur; par exemple, celui-ci ne devrait jamais être en possession des renseignements personnels du sujet ni les stocker;<br>• les processus à suivre pour faciliter le partage des renseignements personnels du sujet;<br>• les processus à suivre lorsque les renseignements personnels du sujet préalablement partagés sont mis à jour, supprimés ou expirés;<br>• des consignes précises à l'intention du sujet sur le partage de ses renseignements personnels pour l'aider à savoir avec quelle partie il devrait communiquer compte tenu de la nature de sa demande de renseignements; et<br>• une évaluation de l'incidence sur la confidentialité qui couvre explicitement le rôle de facilitation, en cherchant surtout à réduire (voire éliminer) l'accès aux renseignements personnels ou à l'information sur les services ou encore leur visibilité. |
| 147 | 9 | L'organe de gouvernance **DOIT** avoir en place des arrangements en matière de gouvernance qui :<br>• assurent l'imputabilité des organisations menant des activités dans l'écosystème de l'identité numérique;<br>• le cas échéant, font en sorte que les participants pertinents à l'écosystème de l'identité numérique satisfont aux exigences spécifiquement définies par une organisation sur les renseignements personnels du sujet;<br>• incluent des règles en matière de normes et d'interopérabilité assurant que toutes les parties au partage des renseignements personnels du sujet traitent le sujet et ses renseignements personnels d'une manière uniforme et compatible;<br>• incluent 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<br>• facilitent la surveillance de la fraude à l'échelle de l'écosystème de l'identité numérique, notamment les dispositions relatives au partage des données afin de surveiller la fraude. |
| 148 | **IDEN** | **Principe n$^{o}$ 2 – Détermination des motifs**<br><br>*Les motifs pour lesquels les renseignements personnels sont recueillis doivent être déterminés par l'organisation avant ou au moment d'être obtenus.* |
| 149 | 1 | L'organisation divulgatrice **DOIT** avoir l'assurance que le principe n$^{o}$ 2 est suivi par les organisations requérantes et les entités chargées du traitement des avis et consentements avant de leur divulguer des renseignements personnels. |
| 150 | 2 | L'organisation divulgatrice **DOIT** maintenir et préserver un calendrier relatif aux documents récupérables pour les dossiers de demandes de renseignements et divulgations. Le calendrier peut consister en un seul événement (« demande et divulgation ponctuelles ») ou plusieurs événements compte tenu des circonstances de l'échange. |

| | | |
|---|---|---|
| 151 | 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. |
| 152 | 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. |
| 153 | 5 | L'organisation requérante **DOIT** mener périodiquement 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. |
| 154 | 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. |
| 155 | 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. |
| 156 | 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. |
| 157 | 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 suivent le principe n° 2. |
| 158 | 10 | L'organe de gouvernance **DOIT** inclure des procédures pour enquêter sur les écarts par rapport au principe n° 2 et les gérer, notamment en évaluant le risque pour les sujets et en signalant les violations aux organismes de réglementation et aux sujets. |
| 159 | **CONS** | **Principe n° 3 - Consentement**<br><br>*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.* |
| 160 | 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. |
| 161 | 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. |
| 162 | 3 | L'organisation divulgatrice **DOIT** s'assurer que l'entité chargée du traitement des avis et consentements joue son rôle d'une manière appropriée avant de divulguer les renseignements personnels du sujet. |

| | | |
|---|---|---|
| 163 | 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 et enregistrées d'une manière appropriée. |
| 164 | 5 | L'organisation divulgatrice **DOIT** confirmer que le consentement est valide (c.-à-d. ni expiré ni révoqué) au moment du partage des renseignements personnels du sujet. Dans l'éventualité où ce consentement ne serait pas valide, l'organisation divulgatrice **DOIT** fournir une réponse appropriée à l'organisation requérante. |
| 165 | 6 | L'organisation divulgatrice **DOIT** s'assurer que le sujet comprend la nature, le motif et les conséquences de la collecte, de l'utilisation ou de la divulgation des renseignements personnels pour lesquels il donne son consentement. |
| 166 | 7 | L'organisation requérante est à l'origine de la demande de consentement et **DOIT** donc être avant tout responsable de déterminer le contenu de l'avis. |
| 167 | 8 | L'organisation requérante **DEVRAIT** s'assurer que la demande est conforme au principe de la divulgation minimale. |
| 168 | 9 | L'organisation requérante **DOIT** s'assurer que l'entité chargée du traitement des avis et consentements remplit sa fonction d'une façon appropriée avant de recevoir les renseignements personnels du sujet. |
| 169 | 10 | L'organisation requérante **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, et enregistrées d'une manière appropriée. |
| 170 | 11 | L'organisation requérante **DEVRAIT** traiter convenablement la révocation du consentement au type d'abonnement par le biais de l'écosystème de l'identité numérique. |
| 171 | 12 | 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. |
| 172 | 13 | 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. |
| 173 | 14 | L'entité chargée du traitement des avis et consentements **DOIT** s'assurer que le sujet est authentifié avant d'afficher ses renseignements personnels dans un avis qui lui est adressé en validant l'identité du sujet. |
| 174 | 15 | 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). |
| 175 | 16 | 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. |
| 176 | 17 | 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. |

| | | |
|---|---|---|
| 177 | 18 | 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. |
| 178 | 19 | Le fournisseur de réseau **PEUT** intervenir pour déterminer ou découvrir quelles organisations divulgatrices sont des sources potentielles des renseignements personnels demandés. |
| 179 | 20 | Le fournisseur de réseau **NE DEVRAIT PAS** être en mesure de voir des renseignements personnels non protégés. Cela inclut des renseignements personnels présentés pendant le processus d'avis et de consentement, ainsi que la transmission des renseignements personnels par le biais du réseau. |
| 180 | 21 | L'organe de gouvernance **DEVRAIT** 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. |
| 181 | 22 | L'organe de gouvernance **DOIT** s'assurer que les organisations qui mènent des activités dans l'écosystème de l'identité numérique suivent le principe n° 3. |
| 182 | 23 | 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. |
| 183 | **LIMC** | **Principe n° 4 – Obtention limitée**<br><br>*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.* |
| 184 | 1 | Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DEVRAIENT** s'assurer que seuls les renseignements nécessaires seront obtenus auprès du sujet. |
| 185 | 2 | L'organisation divulgatrice **DOIT** avoir l'assurance que l'organisation requérante une raison valable et suffisante d'obtenir les renseignements personnels demandés. |
| 186 | 3 | 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. |
| 187 | 4 | 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. |
| 188 | 5 | Suppression de l'exigence (répétition du n° 4). Renuméroter dans la version finale. |
| 189 | 6 | L'organisation requérante **DOIT** documenter publiquement le genre de renseignements personnels recueillis et dans quel but. |
| 190 | 7 | L'organisation requérante **DOIT** s'assurer que les membres du personnel peuvent expliquer le genre de renseignements personnels qui sont recueillis et dans quel but. |

| | | |
|---|---|---|
| 191 | 8 | 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. |
| 192 | 9 | 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 réduits au minimum. |
| 193 | 10 | Le fournisseur de réseau **DOIT** faciliter le partage des renseignements personnels, mais il **NE DEVRAIT PAS** être en mesure de voir les renseignements personnels comme tels pendant l'obtention des renseignements personnels protégés pour les besoins du partage. |
| 194 | 11 | L'organe de gouvernance **DOIT** s'assurer que les organisations menant des activités dans l'écosystème de l'identité numérique suivent le principe n° 4. |
| 195 | 12 | L'organe de gouvernance **DOIT** avoir l'assurance que l'organisation requérante a une raison valable et suffisante de recueillir les renseignements personnels demandés. |
| 196 | 13 | 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. |
| 197 | 14 | 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. |
| 198 | **LIMU** | **Principe n° 5 – Limitation de l'utilisation, de la divulgation et de la rétention**<br><br>*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.* |
| 199 | 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 du sujet. |
| 200 | 2 | L'organisation divulgatrice **DOIT** documenter l'utilisation des renseignements personnels du sujet pour les besoins de la divulgation dans l'écosystème de l'identité numérique. |
| 201 | 3 | Dans l'éventualité où une politique définie sur la rétention minimale et maximale des données 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 du sujet en lien avec l'écosystème de l'identité numérique.<br>Remarque : Sous réserve des restrictions réglementaires. |
| 202 | 4 | L'organisation divulgatrice **DOIT** limiter la divulgation des renseignements personnels du sujet uniquement à ce qui est nécessaire pour les fins spécifiques et recherchées qui correspondent au consentement du sujet. |
| 203 | 5 | L'organisation divulgatrice **DOIT** limiter la divulgation des renseignements personnels du sujet à ceux qu'elle sait être exacts et à jour. |

| | | |
|---|---|---|
| 204 | 6 | L'organisation requérante **DOIT** documenter l'usage des renseignements personnels du sujet obtenus par le biais de l'écosystème de l'identité numérique. |
| 205 | 7 | L'organisation requérante **DOIT** instituer des périodes maximales et minimales valides pour conserver les renseignements personnels du sujet obtenus par le biais de l'écosystème de l'identité numérique. |
| 206 | 8 | L'organisation requérante **NE DOIT PAS** utiliser ou conserver, sans avoir obtenu le consentement approprié, les renseignements personnels du 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. |
| 207 | 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. |
| 208 | 10 | L'entité chargée du traitement des avis et consentements **DOIT** documenter l'utilisation des renseignements personnels du 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 du sujet dans le cadre du processus de consentement. |
| 209 | 11 | L'entité chargée du traitement des avis et consentements **DOIT** instituer des périodes maximales et minimales valides pour conserver les renseignements personnels du sujet, qui s'appliquent à l'écosystème de l'identité numérique. |
| 210 | 12 | 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. |
| 211 | 13 | Les renseignements personnels que le sujet consent à partager avec une ou des organisations requérantes **NE DOIVENT PAS** être transmis par l'entité chargée du traitement des avis et consentements à une organisation autre que l'organisation ou les organisations requérantes désignées dans le consentement. Cela inclut l'entité chargée du traitement des avis et consentements, exception faite des renseignements servant à authentifier le sujet. |
| 212 | 14 | Le fournisseur de réseau **DOIT** faciliter le partage des renseignements personnels mais il **NE DEVRAIT PAS** être en mesure de voir ces renseignements comme tels pendant l'obtention des renseignements personnels protégés dans le but de les partager. |
| 213 | 15 | L'organe de gouvernance **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. |
| 214 | 16 | L'organe de gouvernance **DOIT** définir clairement les limites de l'écosystème de l'identité numérique. |

| | | |
|---|---|---|
| 215 | 17 | L'organe de gouvernance **DOIT** définir et mettre en place des processus pour surveiller et faire appliquer les exigences relatives à l'utilisation, la divulgation et la rétention des renseignements personnels créés en tant que produit dérivé de l'utilisation de l'écosystème de l'identité numérique. |
| 216 | **ACCU** | **Principe nº 6 - Exactitude**<br><br>*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.* |
| 217 | 1 | Les organisations divulgatrices et requérantes, et les entités chargées du traitement des avis et consentements **DOIVENT** faire en sorte que le processus qu'un sujet doit suivre pour mettre à jour des renseignements personnels inexacts dans l'écosystème de l'identité numérique soit clair et direct. |
| 218 | 2 | L'organisation divulgatrice **DOIT** instaurer des politiques, procédures et systèmes pour repérer, corriger et gérer (p. ex., en mettant à jour les dossiers du sujet) les renseignements personnels désuets. Une organisation ne saura que les renseignements sont désuets que 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. |
| 219 | 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. |
| 220 | 4 | Lorsqu'elle partage les renseignements personnels d'un sujet avec une organisation requérante, l'organisation divulgatrice **DOIT** donner au sujet :<br>1. la possibilité d'examiner ses renseignements personnels qui sont partagés; et<br>2. des instructions ou les moyens de mettre à jour les renseignements personnels du sujet. |
| 221 | 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 **DEVRAIT** donner au sujet :<br>1. la possibilité d'examiner ses renseignements personnels devant être partagés; et<br>2. des instructions ou les moyens de mettre à jour ces renseignements sur les services. |
| 222 | 6 | Pour vérifier l'exactitude des renseignements personnels reçus de l'organisation divulgatrice, l'organisation requérante **DEVRAIT** donner au sujet la possibilité d'examiner les renseignements divulgués.<br><br>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. |

| | | |
|---|---|---|
| 223 | 7 | L'entité chargée du traitement des avis et consentements **DOIT** conserver une piste d'audit des renseignements sur les avis et consentements, qui pourrait inclure des preuves concernant des renseignements inexacts partagés par le passé. L'intégrité de cette piste d'audit doit être maintenue. La période de rétention pour la piste d'audit sera déterminée par le réseau de gouvernance et la législation et la réglementation applicables. |
| 224 | 8 | 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. |
| 225 | **SAFE** | **Principe nº 7 – Mesures de protection**<br><br>*Les renseignements personnels doivent être protégés par des mesures de sécurité appropriées compte tenu de la sensibilité des renseignements.* |
| 226 | 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, et que des mesures de protection sont en place au cas où quelque chose irait mal. |
| 227 | 2 | L'organisation divulgatrice **DOIT** développer et mettre en place une politique sur la sécurité afin de protéger les renseignements personnels qui inclut spécifiquement des mesures de protection utilisées dans la divulgation des renseignements personnels du sujet dans le contexte des systèmes d'identité numérique en cause. |
| 228 | 3 | L'organisation divulgatrice **DOIT** mettre en place des mesures de sécurité appropriées pour protéger l'accès aux renseignements personnels, au repos et en transit. |
| 229 | 4 | L'organisation divulgatrice **DOIT** employer des mesures de sécurité appropriées à la sensibilité des renseignements personnels du sujet et au risque de fraude ou d'utilisation malveillante. |
| 230 | 5 | L'organisation divulgatrice **DOIT** examiner et mettre à jour régulièrement les mesures de sécurité reliées à l'écosystème de l'identité numérique. |
| 231 | 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. |
| 232 | 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. |
| 233 | 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. |
| 234 | 9 | L'organisation requérante **DOIT** examiner et mettre à jour régulièrement les mesures de sécurité reliées à l'écosystème de l'identité numérique. |

| | | |
|---|---|---|
| 235 | 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 incluent spécifiquement les mesures de protection employées dans les processus d'avis et de consentement. |
| 236 | 11 | L'entité chargée du traitement des avis et consentements **DOIT** mettre en place des mesures de sécurité appropriées. |
| 237 | 12 | L'entité chargée du traitement des avis et consentements **DOIT** employer des mesures de sécurité appropriées à la sensibilité des renseignements personnels du sujet et au risque de fraude ou d'utilisation malveillante. |
| 238 | 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. |
| 239 | 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. |
| 240 | 15 | Le fournisseur de réseau **DOIT** mettre en place des mesures de sécurité appropriées. |
| 241 | 16 | Le fournisseur de réseau **DOIT** examiner et mettre à jour régulièrement les mesures de sécurité reliées à l'écosystème de l'identité numérique. |
| 242 | 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. |
| 243 | **OPEN** | **Principe nº 8 - Ouverture**<br><br>*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.* |
| 244 | 1 | Les organisations divulgatrices et requérantes, et les responsables 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. |
| 245 | 2 | L'organisation divulgatrice **DOIT** 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 que l'organisation divulgatrice ne peut pas voir. Par exemple, dans un écosystème camouflé, l'organisation divulgatrice peut ne pas savoir avec quelle organisation requérante les renseignements personnels ont été partagés, mais elle devrait être en mesure de fournir une explication au sujet et de lui conseiller de communiquer avec l'organisation requérante. |
| 246 | 3 | L'organisation divulgatrice **DOIT** fournir au sujet des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance. |

| | | |
|---|---|---|
| 247 | 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). |
| 248 | 5 | L'organisation requérante **DOIT** 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 qu'elle ne peut pas voir. |
| 249 | 6 | L'organisation requérante **DOIT** fournir au sujet des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance. |
| 250 | 7 | 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). |
| 251 | 8 | L'entité chargée du traitement des avis et consentements **DOIT** 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 qu'elle ne peut pas voir. |
| 252 | 9 | L'entité chargée du traitement des avis et consentements **DOIT** fournir au sujet des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance. |
| 253 | 10 | 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). |
| 254 | 11 | Le fournisseur de réseau **DOIT** fournir au sujet des renseignements sur son rôle selon les lignes directrices de l'organe de gouvernance. |
| 255 | 12 | 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). |
| 256 | 13 | 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. |
| 257 | 14 | L'organe de gouvernance **DOIT** collaborer avec les participants à l'écosystème pour s'assurer que tous les renseignements sont présentés d'une manière uniforme afin d'éviter des messages conflictuels ou qui portent à confusion. |
| 258 | 15 | 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'il suit les lignes directrices. |
| 259 | 16 | L'organe de gouvernance **DOIT** s'assurer qu'il y a des processus en place pour répondre une demande d'information de la part du sujet. |
| 260 | **INDI** | **Principe nº 9 – Accès individuel**<br><br>*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.* |

| | | |
|---|---|---|
| 261 | 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 divulgation 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.<br><br>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 divulgation de ses renseignements personnels, le processus pour obtenir une telle information **DOIT** être clair, direct et conforme à la LPRPDE. |
| 262 | 2 | L'organisation divulgatrice **DOIT** fournir au sujet des moyens clairs d'obtenir de l'information sur l'existence, l'utilisation et la divulgation de ses renseignements personnels dans le contexte de l'écosystème de l'identité numérique. |
| 263 | 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. |
| 264 | 4 | Lorsque le sujet avise l'organisation requérante que les renseignements personnels qu'elle détient ou utilise sont inexacts ou incomplets, l'organisation requérante **DOIT** avoir des processus appropriés en place pour corriger ou modifier les renseignements personnels. Cela peut consister à :<br>• demander de nouveau les renseignements à l'organisation ou aux organisations divulgatrices par le biais de l'écosystème de l'identité numérique; et<br>• collaborer d'une façon indépendante avec le sujet pour déterminer les renseignements personnels qui sont exacts. |
| 265 | 5 | Si l'organisation requérante détermine que les renseignements personnels qu'elle reçoit de l'écosystème de l'identité numérique sont inexacts ou incomplets, il **PEUT** exister des processus pour aviser l'organisation divulgatrice pertinente du problème. |
| 266 | 6 | 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 divulgation de ses renseignements personnels auprès de l'entité chargée du traitement des avis et consentements.<br><br>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. |
| 267 | 7 | 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).<br><br>Si le fournisseur de réseau n'a pas accès aux renseignements personnels, il **DOIT** alors se conformer au principe de l'« accès à l'information de la LPRPDE ». |

| | | |
|---|---|---|
| 268 | 8 | Les mesures de gouvernance prises par l'organe de gouvernance **DOIVENT** faire en sorte que les processus d'« accès à l'information » soient fournis conformément à l'écosystème de l'identité numérique. |
| 269 | **CHAL** | **Principe nº 10 – Remise en question de la conformité**<br><br>*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 du respect de la vie privée.* |
| 270 | 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 eux **DOIVENT** être simples et disponibles. |
| 271 | 2 | L'organisation divulgatrice **DOIT** avoir un programme de gestion de la conformité qui :<br>• dissocie d'une façon claire et simple l'implication dans l'écosystème de l'identité numérique des autres activités de l'organisation; et<br>• 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. |
| 272 | 3 | L'organisation requérante **DOIT** avoir un programme de gestion de la conformité qui :<br>• dissocie d'une façon claire et simple l'implication dans l'écosystème de l'identité numérique des autres activités de l'organisation; et<br>• 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. |
| 273 | 4 | Le fournisseur de réseau **DOIT** avoir un programme de gestion de la conformité qui :<br>• dissocie d'une façon claire et simple l'implication dans l'écosystème de l'identité numérique des autres activités de l'organisation; et<br>• 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. |
| 274 | 5 | L'organe de gouvernance **DOIT** s'assurer que toute organisation menant des activités dans l'écosystème de l'identité numérique suit le principe nº 10. |
| 275 | 6 | 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. |
| 276 | 7 | 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. |