

# Ébauche de recommandations pour l'aperçu de la composante « 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.

L'auditoire ciblé pour cette ébauche sont les décideurs qui peuvent ou non être des experts dans la technologie des domaines. En examinant cette ébauche, veuillez tenir compte de ce qui suit, et noter que les réponses à ces questions ne sont pas contraignantes et visent à améliorer le Cadre de confiance pancanadien.

1. La composante « Respect de la vie privée » du Cadre de confiance pancanadien est un thème horizontal qui s'applique à tous les autres profils du Cadre de confiance pancanadien. Dans ce contexte, les critères de conformité sont-ils clairs et exhaustifs?
2. Les documents font-ils bien la part entre l'élaboration de principes du respect de la vie privée pour l'identité numérique alignés sur la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), sans reprendre ce que dit la LPRPDE?
3. Votre organisation pourrait-elle identifier des obstacles (commerciaux, juridiques ou techniques) à la conformité?
4. La distinction entre le traitement des renseignements personnels spécifiques au sujet et au service est-elle claire et complète?
5. Les notions présentées dans l'aperçu sont-elles claires et complètes (p. ex. définitions de base, rôles dans l'écosystème de l'identité numérique, portée)?
6. Les critères de conformité devraient être pris dans le contexte pancanadien du Cadre de confiance pancanadien et peuvent ne pas répondre à des exigences supplémentaires spécifiques, qui sont reflétées dans des politiques ou règlements, dans une seule

42 province, un seul territoire ou une seule verticale de l'industrie. Dans ce contexte, les  
43 critères de conformité sont-ils clairs et exhaustifs?

44 REMARQUES :

- 45 • Les critères applicables aux profils du Cadre de confiance pancanadien portant sur une  
46 composante spécifique (p. ex. Avis et consentement, Connexion vérifiée) sont abordés  
47 dans ces profils. Veuillez vous référer à d'autres ébauches de composantes si vous  
48 n'êtes pas sûr qu'un sujet en particulier est couvert.
- 49 • Les critères de conformité de la composante « Respect de la vie privée » sont censés  
50 être agnostiques pour ce qui est de la technologie et de la méthode de mise en œuvre.

51

## 52 **Table des matières**

53

54	1	Introduction à la composante « Respect de la vie privée » du Cadre de confiance	
55		pancanadien.....	2
56	1.1	Raison d'être et avantages anticipés.....	3
57	1.2	Portée.....	4
58	1.2.1	Inclus dans la portée.....	5
59	1.2.2	Exclus de la portée.....	5
60	1.3	Relation avec le Cadre de confiance pancanadien.....	6
61	2	Conventions de la composante « Respect de la vie privée ».....	6
62	2.1	Termes et définitions.....	6
63	2.2	Rôles.....	7
64	3	Principes essentiels de la composante « Respect de la vie privée ».....	8
65	3.1	Renseignements personnels.....	8
66	3.2	Changements apportés aux renseignements personnels à la source (organisation	
67		communicante).....	8
68	3.3	Traitement en amont et en aval des renseignements personnels.....	8
69	3.4	Respect de la vie privée dès la conception.....	9
70	4	Notes et hypothèses.....	10
71	5	Références.....	10

72

# 73 **1 Introduction à la composante**

# 74 **« Respect de la vie privée » du Cadre**

# 75 **de confiance pancanadien**

76 Ce document donne un aperçu de la composante « Respect de la vie privée » du Cadre de  
77 confiance pancanadien. Pour avoir une introduction générale sur le Cadre de confiance  
78 pancanadien, notamment de l'information contextuelle et les buts et objectifs du Cadre de  
79 confiance pancanadien, veuillez vous référer au document « Aperçu du modèle de Cadre de  
80 confiance pancanadien ».

81 Chaque composante du Cadre de confiance pancanadien comporte deux documents :

- 82 1. Aperçu – Il introduit le sujet de la composante. L'aperçu fournit des renseignements  
83 essentiels pour comprendre les critères de conformité de la composante, à savoir des  
84 définitions des termes clés, des concepts et les processus de confiance qui font partie  
85 de la composante.
- 86 2. Profil de conformité – Il spécifie les critères de conformité utilisés pour uniformiser et  
87 évaluer l'intégrité des processus de confiance qui font partie de la composante.

88 Cet aperçu fournit des renseignements reliés au profil de conformité de la composante  
89 « Respect de la vie privée » du Cadre de confiance pancanadien, qui sont nécessaires pour  
90 l'interpréter d'une manière uniforme.

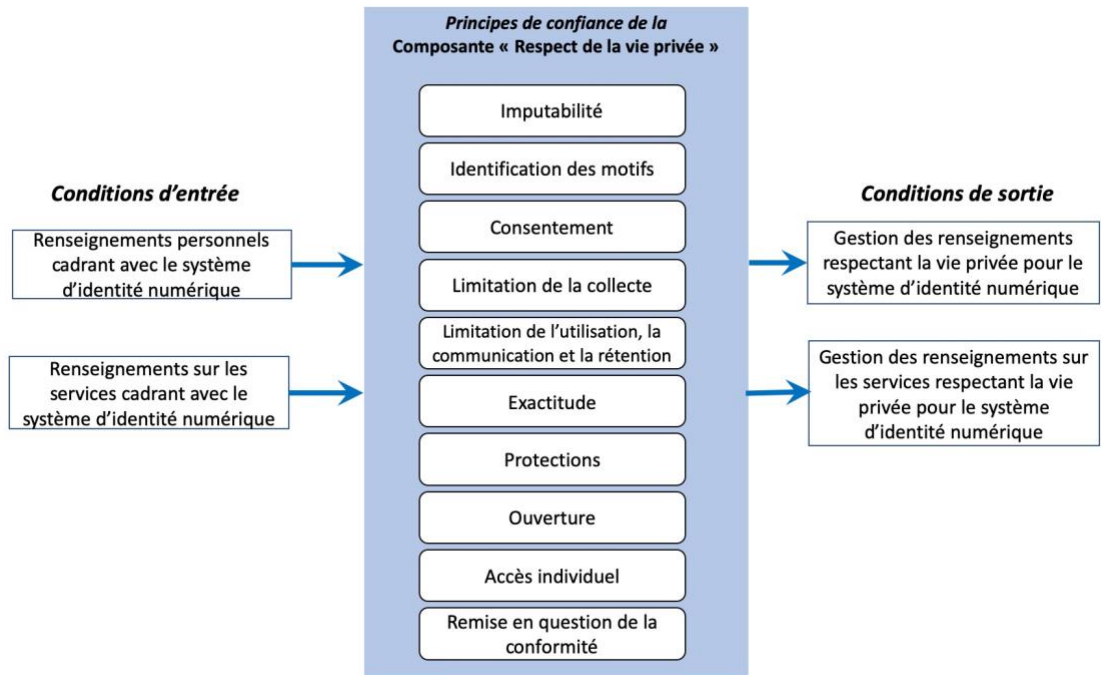
## 91 **1.1 Raison d'être et avantages anticipés**

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

98  
99 La composante « Respect de la vie privée » du Cadre de confiance pancanadien porte sur le  
100 traitement des données personnelles pour les besoins de l'identité numérique. Elle a pour  
101 objectif d'assurer l'intégrité permanente des processus, politiques et contrôles des organisations  
102 en matière de confidentialité dans un écosystème de l'identité numérique grâce à des critères  
103 de conformité uniformisés qui sont utilisés pour l'évaluation et la certification par rapport au  
104 Cadre de confiance pancanadien. Les critères de conformité pour la composante « Respect de  
105 la vie privée » spécifient les exigences qui, une fois remplies, déterminent qu'une organisation  
106 assumant le rôle des organisations divulgatrices et requérantes, des entités chargées du  
107 traitement des avis et consentements, des fournisseurs de réseau et l'organe de gouvernance  
108 traitent les renseignements sur l'identité numérique conformément aux 10 principes définis à  
109 l'annexe 1 de la LPRPDE. La LPRPDE s'applique aux organisations qui traitent des  
110 renseignements personnels dans le cadre d'activités commerciales. (Remarque : Ils ne  
111 remplacent pas les règlements existants; on s'attend à ce que les organisations se conforment  
112 aux lois, politiques et règlements pertinents sur la protection de la vie privée dans leur province  
113 ou territoire.)

114  
115 Il se pourrait que les versions futures de cette composante incorporent des critères de  
116 conformité pertinents à d'autres consignes sur la protection de la vie privée (p. ex., respect de la  
117 vie privée dès la conception, modernisation de la LPRPDE) et cadres réglementaires (p. ex.,

118 lois fédérales et provinciales sur la protection de la vie privée).  
 119 La figure 1 donne un aperçu conceptuel et une organisation logique de la composante  
 120 « Respect de la vie privée ».



121  
 122 **Figure 1. Composante « Respect de la vie privée »**

123  
 124 La composante « Respect de la vie privée » est constituée des éléments suivants :

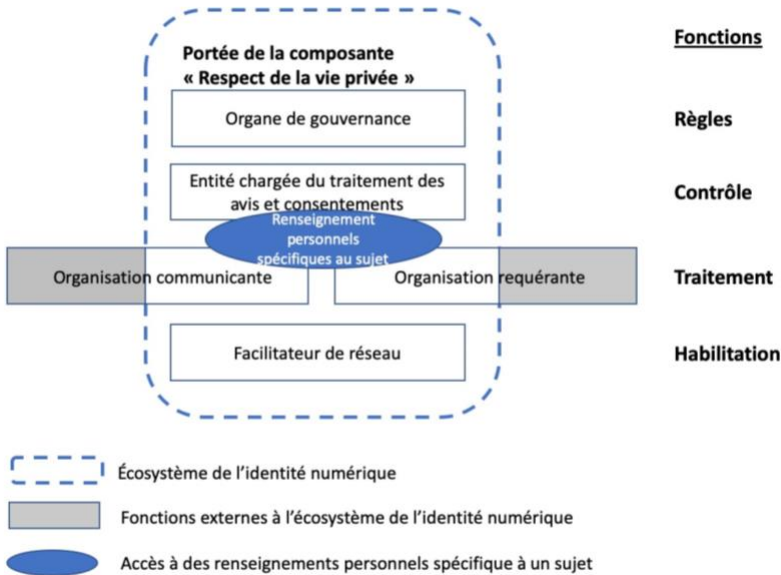
- 125 • **Principes de confiance** – ensemble de principes auxquels les organisations (p. ex.,  
 126 organisations divulgatrices, organisations requérantes, entités chargées du traitement  
 127 des avis et consentements, fournisseurs de réseau) sont censées se conformer  
 128 lorsqu'elles traitent des renseignements sur des personnes et des services dans un  
 129 système d'identité numérique. Chaque principe de confiance est évalué selon un  
 130 ensemble de critères de conformité associés à ce principe.
- 131 • **Intrants** – ce qui est intégré dans les principes de confiance, p. ex., les renseignements  
 132 personnels exigeant une gestion de la confidentialité pour agir.
- 133 • **Extrants** – ce qui résulte de l'application des principes de confiance, p. ex., les  
 134 politiques et les contrôles en matière de respect de la vie privée appliqués aux  
 135 renseignements personnels.

## 136 1.2 Portée

137 La figure 3 illustre la portée de la composante « Respect de la vie privée », qui inclut les  
 138 fonctions accomplies par les organisations divulgatrice et requérante, et l'entité chargée du  
 139 traitement des avis et consentements, ainsi que les rôles des fournisseurs de réseau et organes  
 140 de gouvernance tels que décrits dans la section Rôles.

141  
 142 Dans le contexte du Cadre de confiance pancanadien, seuls ceux dont les rôles consistent à

143 traiter des renseignements sur l'identité numérique dans l'écosystème numérique et qui  
 144 empêcheront l'accès à ces fins auront normalement accès aux renseignements personnels  
 145 spécifiques au sujet. Les participants qui interviennent dans le Cadre de confiance pancanadien  
 146 pour favoriser, contrôler et mettre en place des règles visant à faciliter le partage des  
 147 renseignements personnels ne devraient idéalement pas y être exposés (p. ex., à moins que la  
 148 loi ne l'exige) . L'entité chargée du traitement des avis et consentements, qui remplit des  
 149 fonctions de contrôle, pourrait être exposée à des renseignements personnels (compte tenu de  
 150 la façon dont cette entité est présentée), mais cela devrait être minimisé (selon les critères de  
 151 conformité pour limiter la collecte LIMC-9).



152  
 153 **Figure 3. Portée et rôle de la composante « Respect de la vie privée »**

154 **1.2.1 Inclus dans la portée**

- 155
- 156 • Dans le contexte du Cadre de confiance pancanadien, les exigences en matière de
  - 157 respect de la vie privée s'appliquant aux rôles dans le cadre de l'écosystème de
  - 158 l'identité numérique. Pour voir un aperçu du modèle de Cadre de confiance pancanadien
  - 159 et de ses composantes, veuillez vous reporter à l'aperçu du modèle de Cadre de
  - 160 confiance pancanadien.
  - 161 • Exigences pour le traitement des renseignements personnels spécifiques au sujet et des
  - 162 renseignements spécifiques aux services associés à l'identité numérique.
  - 163 • Responsabilité de la politique et des processus reliés à la protection de la vie privée qui
  - s'appliquent à la prestation de l'identité numérique assurée.

164 **1.2.2 Exclus de la portée**

- 165
- 166 • Surveillance de la fraude : La composante « Respect de la vie privée » inclut les critères
  - 167 de conformité concernant le signalement des violations de la vie privée et des fraudes
  - 168 pour les rôles spécifiques à la composante « Respect de la vie privée » (pour tous les
  - 169 rôles, voir Base - BASE 6; pour l'organe de gouvernance, voir Imputabilité - ACCO 9,
  - ainsi que Détermination de la raison d'être IDENT-9, Consentement CONS-23, et

170 Limitation de la collecte LIMC-14). Les exigences s'appliquant à une surveillance plus  
 171 générale et au signalement de la fraude, et les mesures à prendre dans le cadre de  
 172 l'écosystème de l'identité numérique imposent de poursuivre l'étude et le  
 173 développement dans le contexte du Cadre de confiance pancanadien.  
 174 • Exigences connexes spécifiques abordées dans d'autres profils du Cadre de confiance  
 175 pancanadien.

## 176 1.3 Relation avec le Cadre de confiance pancanadien

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

183 La figure 2 illustre les composantes du Cadre de confiance pancanadien. La composante  
 184 « Respect de la vie privée » englobe toutes les sous-composantes ».



185  
 186 **Figure 2. Composantes du Cadre de confiance pancanadien**

187 Les critères de conformité du Cadre de confiance pancanadien ne remplacent ou n'annulent  
 188 pas les règlements existants; on s'attend à ce que les organisations et les particuliers se  
 189 conforment aux lois, politiques et règlements pertinents dans leur juridiction.

## 190 2 Conventions de la composante

### 191 « Respect de la vie privée »

#### 192 2.1 Termes et définitions

##### 193 **Avis**

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

## 197 **Consentement**

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

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

207 **Écosystème de l'identité numérique** – Système interrelié pour l'échange et la vérification des  
208 renseignements sur l'identité numérique, impliquant des organisations des secteurs public et  
209 privé (p. ex., entités gouvernementales, commerciales, sans but lucratif et autres) qui se  
210 conforment à un cadre de confiance commun pour la gestion et l'utilisation d'identités  
211 numériques, et les sujets de ces identités numériques. Dans le contexte de la composante  
212 « Respect de la vie privée », l'écosystème de l'identité numérique fait référence à l'écosystème  
213 canadien de l'identité numérique conforme au Cadre de confiance pancanadien.

## 214 **Renseignements personnels**

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

- 219 • **Renseignements spécifiques aux services** – Renseignements recueillis ou générés  
220 par les participants (organisation divulgateuse, organisation requérante, entité(s)  
221 chargée(s) de traiter les avis et consentements, ou fournisseur de réseau) afin  
222 d'exploiter et de maintenir le service (p. ex., pseudonymes spécifiques aux services,  
223 dossiers de transactions, preuves de transactions incluant le consentement). Dans  
224 certains cas, les renseignements spécifiques aux services peuvent être partagés, avec  
225 le consentement du sujet.
- 226 • **Renseignements personnels spécifiques au sujet** – Renseignements qu'un sujet  
227 consent à partager d'une organisation communicante à une organisation requérante  
228 (p. ex., nom, adresse de courriel, numéro de téléphone, adresse postale, date de  
229 naissance, renseignements sur les comptes).

## 230 **2.2 Rôles**

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

- 234 • **Organisation communicante** – Organisation qui détient actuellement les  
235 renseignements personnels spécifiques au sujet, que le sujet consent à communiquer à  
236 une organisation requérante ou que l'organisation communicante peut divulguer  
237 légalement en vertu de la législation pertinente. Dans un contexte numérique, ce sera  
238 souvent un fournisseur d'identités ou d'attributs.

- 239 • **Organe de gouvernance** – Organisation qui supervise le cadre de confiance et les  
240 exigences connexes de l'écosystème de l'identité numérique. Cela pourrait impliquer  
241 une gouvernance ainsi que des arrangements d'affaires, techniques ou commerciaux  
242 entre les parties à la transaction.
- 243 • **Entité chargée du traitement des avis et consentements** – Organisation qui fournit  
244 au sujet l'avis de demande de renseignements personnels (provenant de l'organisation  
245 requérante), obtient et enregistre le consentement, et fournit au sujet les moyens de  
246 gérer à l'avenir le consentement, notamment le retrait du consentement.
- 247 • **Fournisseur de réseau** – Organisation qui relie les parties dans une transaction sur  
248 une identité multipartite. Cette organisation est un participant actif et ajoute de la valeur  
249 à la prestation du service d'identité numérique (p. ex., pas un fournisseur de services  
250 Internet qui fournit passivement une connectivité Internet). Par exemple, un fournisseur  
251 de chaînes de blocs ou un logiciel en tant que service (SaaS) qui facilite le réseau.
- 252 • **Organisation requérante** – Organisation à laquelle le sujet consent de divulguer des  
253 renseignements personnels. Dans un contexte d'identité numérique, il s'agira souvent  
254 d'un fournisseur de services ou d'une partie utilisatrice.
- 255 • **Sujet** – Personne naturelle à qui les renseignements personnels en question  
256 s'appliquent. (Remarque : L'autorité déléguée n'est pas couverte dans le présent  
257 document).

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

261 Par exemple, dans certains cas, l'avis peut provenir et le consentement peut être obtenu d'une  
262 organisation qui facilite l'échange de renseignements personnels entre le sujet, l'organisation  
263 communicante et l'organisation requérante. Dans d'autres cas, l'avis peut provenir et le  
264 consentement peut être obtenu directement de l'organisation communicante ou requérante,  
265 auquel cas cette organisation serait aussi l'entité chargée du traitement des avis et  
266 consentements.

## 267 **3 Principes clés de la composante**

### 268 **« Respect de la vie privée »**

#### 269 **3.1 Renseignements personnels**

270 Les pratiques ayant trait au respect de la vie privée reposent sur le principe selon lequel les  
271 personnes sont informées des détails ainsi que des éventuels avantages et conséquences  
272 associés à la gestion de leurs renseignements personnels. Les renseignements personnels  
273 incluent l'information que l'utilisateur final consent à communiquer (p. ex., nom, adresse de  
274 courriel, numéro de téléphone, adresse postale, date de naissance, renseignements sur les  
275 comptes, etc.) ainsi que des renseignements sur le fonctionnement et le maintien du service  
276 (p. ex., pseudonymes spécifiques aux services, dossiers de transactions).



277 **3.2 Changements apportés aux renseignements**  
278 **personnels à la source (organisation**  
279 **communicante)**

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

288 **3.3 Traitement en amont et en aval des**  
289 **renseignements personnels**

290 Le traitement des renseignements personnels d'un sujet par une organisation communicante  
291 est assujéti aux lois et règlements pertinents en matière de protection de la vie privée, et n'est  
292 généralement considéré comme étant visé par la portée du Cadre de confiance pancanadien  
293 que lorsque ces données sont traitées dans le but d'être partagées par le biais de l'écosystème  
294 de l'identité numérique. Il y a toutefois une exception quand une organisation requérante a des  
295 exigences spécifiques pour le traitement des renseignements personnels par leur source  
296 (l'organisation communicante). Ces exigences feront donc partie de la gouvernance de  
297 l'écosystème de l'identité numérique et constitueront les exigences « en amont » auxquelles  
298 doit se conformer toute organisation communicante qui dessert cette organisation requérante.  
299 De même, le traitement des renseignements personnels spécifiques à un sujet par une  
300 organisation requérante est assujéti aux lois et règlements pertinents en matière de protection  
301 de la vie privée, et n'est généralement considéré comme étant visé par la portée des exigences  
302 du Cadre de confiance pancanadien que lorsque ces données sont traitées dans le but d'être  
303 partagées par le biais de l'écosystème de l'identité numérique. Il y a toutefois une exception  
304 quand une organisation communicante a des exigences spécifiques pour le traitement des  
305 renseignements personnels par leur destinataire (l'organisation requérante). Ces exigences  
306 feront donc partie de la gouvernance de l'écosystème de l'identité numérique et constitueront  
307 les exigences « en aval » auxquelles doit se conformer toute organisation requérante qui reçoit  
308 des données de l'organisation communicante.

309

310

311 **3.4 Respect de la vie privée dès la conception**

312 Le respect de la vie privée dès la conception est un des principes directeurs adoptés par le  
313 CCIAN pour un écosystème canadien de l'identité numérique, qui consiste spécifiquement à  
314 « mettre en place, protéger et améliorer la protection de la vie privée dès la conception ». Les  
315 questions de respect de la vie privée font partie intégrante du développement d'une solution en

316 matière d'identité numérique et devraient être prises en considération à tous les stades de ce  
317 développement. Les outils visant à améliorer le respect de la vie privée permettent à une  
318 personne de gérer ses renseignements et l'utilisation qui en est faite.  
319 Le Comité permanent de l'accès à l'information, de la protection des renseignements  
320 personnels et de l'éthique (ETHI) de la Chambre des communes a recommandé que la  
321 LPRPDE soit modifiée afin d'inclure les principes du respect de la vie privée dès la conception  
322 [1], mais les principes équitables actuels de la LPRPDE ne le couvrent pas explicitement. Par  
323 conséquent, les critères de conformité de la composante « Respect de la vie privée » du Cadre  
324 de confiance pancanadien n'incluent pas des critères pour évaluer la conformité au respect de  
325 la vie privée dès la conception.

## 326 4 Notes et hypothèses

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

## 336 5 Références

### 337 Notes

338 [1] [Rapport du Comité permanent de l'accès à l'information, de la protection des](#)  
339 [renseignements personnels et de l'éthique](#), février 2018, recommandation 14, p. 52  
340 [2 ] Cela ne vise pas à dégager l'organisation communicante de ses obligations juridiques et  
341 réglementaires.  
342 [Survol de la LPRPDE \(révisé : mai 2019\)](#)  
343 Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents*  
344 *électroniques* (LPRPDE) du gouvernement du Canada  
345 ISO-27701