

# Foire aux questions sur l'utilisation des principes généralement reconnus en matière de protection des renseignements personnels dans les missions WebTrust

## Table des matières

FOIRE AUX QUESTIONS SUR L'UTILISATION DES PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS (PPRP) DANS LES MISSIONS WEBTRUST .....	1
<b>Table des matières</b>	<b>1</b>
<b>Introduction</b>	<b>1</b>
<b>Lien entre les PPRP et les Services Trust .....</b>	<b>2</b>
<i>QUESTION 1 – PPRP ET WEBTRUST .....</i>	<i>2</i>
<i>QUESTION 2 – PPRP ET SYSTRUST.....</i>	<i>2</i>
<i>QUESTION 3 – LIBELLÉ D'UN RAPPORT WEBTRUST SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS EN LIGNE .....</i>	<i>2</i>
<i>QUESTION 4 – ÉTENDUE D'UNE MISSION DE VÉRIFICATION WEBTRUST SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS EN LIGNE.....</i>	<i>3</i>
<i>QUESTION 5 – COUVERTURE DES DIX PRINCIPES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS L'EXAMEN ET LE RAPPORT .....</i>	<i>3</i>
<i>QUESTION 6 – UNITÉ EN LIGNE ET AVIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS.....</i>	<i>4</i>
<i>QUESTION 7 – RELATION ENTRE LES SERVICES TRUST, PPRP ET WEBTRUST .....</i>	<i>4</i>
<i>QUESTION 8 – RESSOURCES.....</i>	<i>4</i>
<i>QUESTION 9 – SCEAU DE PROTECTION DES CONSOMMATEURS WEBTRUST.....</i>	<i>5</i>
<i>QUESTION 10 – DÉLIVRANCE D'UN RAPPORT HYBRIDE .....</i>	<i>5</i>
<i>QUESTION 11 – COMPARAISON DES PRINCIPES DES SERVICES TRUST.....</i>	<i>5</i>
<b>Annexe A- Exemple de rapport WebTrust du praticien indépendant</b>	<b>7</b>
<i>EXEMPLE 1 —RAPPORT SUR L'ASSERTION DE LA DIRECTION.....</i>	<i>7</i>
<i>EXEMPLE D'ASSERTION DE LA DIRECTION .....</i>	<i>8</i>
<i>EXEMPLE 2—RAPPORT PORTANT DIRECTEMENT SUR LES ÉLÉMENTS CONSIDÉRÉS .....</i>	<i>9</i>

## Introduction

Les principes généralement reconnus en matière de protection des renseignements personnels (PRPP) forment un ensemble de principes et de critères élaborés par l'ICCA et l'AICPA pour aider les organisations à créer un programme efficace de protection des renseignements personnels qui prend en compte les risques et les occasions d'affaires qui peuvent se présenter. Ces principes peuvent être utilisés par les organisations aux fins de la planification stratégique et d'entreprise, de l'analyse des faiblesses et des risques, de l'étalonnage, de la conception et de la mise en œuvre des politiques, de la mesure de la performance ainsi que de la surveillance et de la vérification des programmes en matière de protection des renseignements personnels. Les dix principes généralement reconnus en matière de protection des renseignements personnels s'appuient sur des critères fondés sur des pratiques d'information équitables reconnues à l'échelle internationale et énoncées dans de nombreux

textes légaux et réglementaires de divers pays concernant la protection des renseignements personnels, et sur des pratiques considérées comme bonnes.

Le service WebTrust, qui figure parmi les missions des Services Trust, consiste en une mission de vérification des assertions de la direction liées à une unité d'exploitation fondée sur le commerce électronique. À la publication d'un rapport de vérification sans réserve du praticien CA, l'entité peut décider (sous réserve de certaines conditions) d'afficher un sceau WebTrust et le rapport du vérificateur y afférent sur son site Web. Le travail de vérification exige le recours au chapitre 5025 du *Manuel de l'ICCA*, Normes relatives aux missions de certification. Les PPRP remplacent les principes et les critères auparavant utilisés dans le cadre des missions WebTrust et ont une portée plus vaste (par exemple, ils peuvent s'appliquer à l'ensemble de l'entreprise et non seulement à l'unité d'exploitation fondée sur le commerce électronique).

La présente foire aux questions (FAQ) donne des suggestions et des éclaircissements sur l'application des PPRP dans les missions de vérification et met l'accent sur les missions dans lesquelles les principes et critères de protection des renseignements personnels en ligne des services Trust étaient utilisés auparavant (notamment les missions WebTrust et des autres missions des Services Trust). Les réponses représentent les points de vue exprimés par le Groupe de travail mixte ICCA-AICPA sur la protection des renseignements personnels et ne représentent pas nécessairement les points de vue officiels de l'Institut Canadien des Comptables Agréés (ICCA) ou de l'American Institute of Certified Public Accountants (AICPA).

## **Lien entre les PPRP et les Services Trust**

### **Question 1 – PPRP et WebTrust**

Les PPRP peuvent-ils être utilisés dans le cadre d'une mission WebTrust?

Oui. Les critères en matière de protection des renseignements personnels sont maintenant intégrés aux Principes, critères et exemples des Services Trust qui peuvent être utilisés dans une mission WebTrust. Veuillez vous reporter à l'[Annexe C](#) de la version des PPRP destinée aux praticiens CA/CPA sur le site Web de l'ICCA (le document est également accessible sur le site Web de l'AICPA).

Lorsqu'une mission sur la protection des renseignements personnels a trait à une unité d'exploitation en ligne, l'entité peut choisir d'afficher le sceau WebTrust pour la protection des renseignements personnels en ligne. L'étendue de la mission doit inclure au moins une unité d'exploitation en ligne de l'entité.

### **Question 2 – PPRP et SysTrust**

Les principes généralement reconnus en matière de protection des renseignements personnels peuvent-ils être utilisés dans le cadre d'une mission SysTrust?

Non. Une mission SysTrust porte sur les contrôles dans un système donné. Par ailleurs, une mission de vérification relative à la protection des renseignements personnels (comme une mission WebTrust) couvre l'ensemble du cycle informationnel (soit de collecte à la destruction des renseignements) au sein de l'entreprise ou de l'unité d'exploitation, selon les modalités de la mission. Il arrive alors souvent que plusieurs systèmes soient en cause.

### **Question 3 – Libellé d'un rapport WebTrust sur la protection des renseignements personnels en ligne**

Quel devrait être le libellé d'un rapport sur la protection des renseignements personnels en ligne établi à partir des PPRP?

Voir l'[Annexe A](#) de la présente Foire aux questions.

#### **Question 4 – Étendue d'une mission de vérification WebTrust sur la protection des renseignements personnels en ligne**

Quelle est l'étendue d'une mission de vérification WebTrust relative à la protection des renseignements personnels en ligne exécutée selon les PPRP?

Comme l'indique l'[Annexe C](#) de la version PPRP destinée aux praticiens CA/CPA :

La mission peut porter 1) soit sur l'ensemble des renseignements personnels ou sur certains types seulement comme les renseignements sur les clients ou les renseignements sur les employés et 2) sur toutes les unités d'exploitation de l'entité dans son ensemble et tous les endroits où elle mène des activités ou encore sur certaines de ses unités d'exploitation seulement (par exemple les activités de vente au détail et non les activités de fabrication, ou encore seulement les activités menées par le truchement du site Web de l'entité) ou sur des activités menées dans un endroit précis (au Canada, par exemple). En outre :

- o l'étendue de la mission doit généralement cadrer avec la description des entités et des activités dont il est question dans l'avis qu'elle diffuse au sujet de la protection des renseignements personnels (voir le critère 2.2.2). L'étendue de la mission peut être souvent plus étroite que la portée de l'avis mais, ordinairement, elle ne peut l'excéder;
- o la mission doit couvrir toutes les activités du «cycle informationnel» relatives aux renseignements personnels en cause. Ces activités comprennent notamment la collecte, l'utilisation, la conservation, la communication, la destruction, la «dépersonnalisation» et la «désidentification» des renseignements. Le fait de déterminer une unité ne comportant pas un cycle complet pourrait induire en erreur l'utilisateur du rapport du praticien;
- o si les renseignements personnels identifiés qui sont couverts par la vérification sont amalgamés à des renseignements non couverts, la mission de certification relative à la production des renseignements personnels doit tenir compte des contrôles appliqués pour tous les renseignements à partir du moment où ils sont amalgamés.

À partir des indications ci-dessus, un rapport peut être délivré au sujet d'un système en ligne, comme s'il s'agissait d'une unité d'exploitation assujettie aux dispositions ci-dessus.

#### **Question 5 – Couverture des dix principes relatifs à la protection des renseignements personnels dans l'examen et le rapport**

Dans le cadre d'une mission WebTrust sur la protection des renseignements personnels en ligne, l'examen et le rapport doivent-ils couvrir les dix principes en la matière?

Oui. Les principes généralement reconnus en matière de protection des renseignements personnels sont fondés sur l'objectif suivant :

*La collecte, l'utilisation, la conservation et la communication des renseignements personnels se font en conformité avec les engagements énoncés dans l'avis sur la protection des renseignements personnels donné par l'entité et avec les critères établis dans le cadre des principes généralement reconnus en matière de protection des renseignements personnels publiés par l'ICCA et l'AICPA.*

Cet objectif correspond à un principe des Services Trust (par exemple la sécurité, l'accessibilité). Il ne peut être atteint qu'au moyen d'un examen et du respect des dix principes relatifs à la protection des renseignements personnels.

Comme il est indiqué dans l'Annexe C de la version des PPRP destinée aux praticiens CA/CPA :

«Le rapport de certification ayant trait à la protection des renseignements personnels couvre normalement les 10 principes. Tous les critères pertinents énoncés à l'égard de chacun de ces

principes doivent être remplis pendant la période visée par le rapport pour que le praticien puisse délivrer un rapport sans réserve.»

### **Question 6 – Unité en ligne et avis sur la protection des renseignements personnels**

Dans le cadre d'une mission WebTrust sur la protection des renseignements personnels, quelle est la différence entre la description de l'unité en ligne visée (énoncée dans le rapport du praticien) et l'avis sur la protection des renseignements personnels de l'organisation (habituellement mentionnée sur son site Web)?

Leur objet est entièrement différent. L'avis sur la protection des renseignements personnels donne de l'information sur les politiques instaurées de l'organisation en la matière, tandis que la description de l'unité d'exploitation en ligne donne de l'information sur l'entité visée par la mission.

Le praticien qui exécute une mission WebTrust s'assure que l'entité a maintenu des contrôles efficaces sur le système faisant l'objet de l'examen (en l'occurrence les PPRP) et qu'elle a rempli ses engagements concernant le(s) principe(s) des Services Trust énoncé(s) (en l'occurrence l'information communiquée dans l'avis sur la protection des renseignements personnels).

Idéalement, lorsque les PPRP sont utilisés dans le cadre d'une mission sur une unité en ligne, les organisations peuvent envisager la publication d'un avis sur la protection des renseignements personnels distinct pour les systèmes faisant l'objet de la mission afin de réduire le risque de confusion.

### **Question 7 - Relation entre les Services Trust, les PPRP et WebTrust**

Quelle est la relation entre les Services Trust, les PPRP et WebTrust?

Les **Services Trust** forment un ensemble de services de certification et de services-conseils professionnels fondés sur un cadre commun ayant trait aux risques et aux occasions liés aux technologies de l'information. Ils englobent les principes et critères suivants :

- Sécurité
- Accessibilité
- Intégrité du traitement
- Confidentialité
- Protection des renseignements personnels

Les **PPRP** représentent les principes et critères liés à la protection des renseignements personnels dans ce contexte.

Le service **WebTrust** consiste en un examen d'une unité d'exploitation fondée sur le commerce électronique et, lors de la délivrance d'un rapport de certification sans réserve, il permet à l'entité d'afficher un sceau WebTrust et le rapport du vérificateur y afférent sur son site Web. Comme il est expliqué à la question 1, la mission Webtrust sur la protection des renseignements personnels en ligne porte également sur l'unité d'exploitation en ligne et, lors de la délivrance d'un rapport de certification sans réserve, une entité peut décider d'afficher un sceau WebTrust de protection des renseignements personnels en ligne.

### **Question 8 – Ressources**

Où puis-je trouver de l'information sur les Services Trust et les services liés à la protection des renseignements personnels?

L'information est accessible sur les sites suivants :

Services Trust :

- [ICCA](#)
- [AICPA](#)

Services liés à la protection des renseignements personnels :

[ICCA](#)  
[AICPA](#)

L'ICCA offre les produits suivants pour les services de protection des renseignements personnels (cliquer sur Magasiner sur <https://www.knotia.ca>):

20 questions que les entreprises devraient poser sur la protection des renseignements personnels – N° 04421  
Solutions for Today's Privacy Issues – N° 02980

#### **Question 9 – Sceau de protection des consommateurs WebTrust**

Le sceau de protection des consommateurs WebTrust, qui était accordé auparavant aux entités qui respectaient les principes d'intégrité du traitement et de protection des renseignements personnels en ligne des Services Trust, peut-il être encore accordé?

Non. Ce sceau spécial et le rapport du praticien y afférent étaient rarement utilisés et ils ne sont plus offerts. C'est le sceau WebTrust, sans la mention «Protection du consommateur», qui peut être accordé.

#### **Question 10 – Délivrance d'un rapport hybride**

Est-il possible de délivrer un rapport hybride sur la protection des renseignements personnels (fondé sur les PPRP) et sur un autre principe des Services Trust (par exemple l'accessibilité)?

Oui, mais le groupe de travail le déconseille. Comme la protection des renseignements personnels doit couvrir l'ensemble du cycle informationnel, de la collecte à la destruction des renseignements, plusieurs systèmes entrent souvent en jeu. À moins que l'autre principe (l'accessibilité dans ce cas-ci) couvre tous les systèmes en cause dans l'ensemble du cycle informationnel, un rapport hybride serait normalement trop complexe et difficile à comprendre pour un utilisateur. Il est préférable de délivrer deux rapports distincts liés par un sceau commun.

#### **Question 11 – Comparaison des principes des Services Trust**

Pouvez-vous décrire sommairement le lien entre les différentes catégories de principes et de critères des Services Trust et les différents services?

Ce lien est décrit dans le tableau ci-dessous :

	Mission de certification sans sceau ni autre marque de l'ICCA	Services Trust	
		SysTrust	WebTrust
<b>Principes :</b>			
<b>Accessibilité</b>	Oui	Oui	Oui
<b>Sécurité</b>	Oui	Oui	Oui
<b>Intégrité du traitement</b>	Oui	Oui	Oui
<b>Confidentialité</b>	Oui	Oui	Oui
<b>Protection des renseignements personnels - PPRP</b>	Oui	Non	Oui

<b>Système</b>		Tout système décrit	Système en ligne
<b>Sceau</b>	Aucun sceau	Logo SysTrust peut être utilisé avec permission	Logo WebTrust peut être utilisé avec permission
<b>Rapport public</b>	Oui	Oui	Oui
<b>Autre</b>			

## Annexe A- Exemple de rapport WebTrust du praticien indépendant

### Exemple 1 — Rapport sur l’assertion de la direction

#### Rapport du vérificateur sur la protection des renseignements personnels WebTrust

À la direction de la société ABC inc. :

Nous avons vérifié l’assertion de la direction de la société ABC inc. (la société ABC) selon laquelle, au cours de la période du xx xxxx 2008 au yy yyyy 2008, la société ABC :

a exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de \_\_\_\_\_ [description des entités et activités visées, par exemple «les activités de ventes postales par catalogue»] (l’«activité») de façon à fournir l’assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés et communiqués conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels relatif à l’activité et aux critères établis dans le cadre des principes généralement reconnus en matière de protection des renseignements personnels publiés par l’Institut Canadien des Comptables Agréés (ICCA) et l’American Institute of Certified Public Accountants (AICPA);

a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels.

La responsabilité de cette assertion incombe à la direction. Notre responsabilité consiste à exprimer une opinion en nous fondant sur notre vérification.

Notre vérification a été effectuée conformément aux normes relatives aux missions de certification établies par l’ICCA. Ces normes exigent que la vérification soit planifiée et exécutée de manière à fournir une assurance raisonnable sur laquelle sera fondée notre opinion. Notre vérification a consisté 1) à acquérir une compréhension des contrôles exercés par la société ABC relativement à la protection des renseignements personnels, 2) à tester et à évaluer l’efficacité du fonctionnement de ces contrôles, 3) à vérifier que la société a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels et 4) à mettre en œuvre les autres procédés que nous avons jugés nécessaires dans les circonstances. Nous estimons que notre vérification constitue une base raisonnable à l’expression de notre opinion.

À notre avis, l’assertion de la direction de la société ABC selon laquelle, au cours de la période du xx xxxx 2008 au yy yyyy 2008, la société ABC :

a exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de l’activité de façon à fournir l’assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés et communiqués conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels et aux critères établis dans le cadre des principes généralement reconnus en matière de protection des renseignements personnels;

a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels,

donne, à tous les égards importants, une image fidèle de la réalité.

*OU*

À notre avis, l’assertion de la direction de la société ABC dont il est fait état plus haut donne, à tous les égards importants, une image fidèle de la réalité, qui est conforme à l’avis sur la protection des renseignements personnels donné par la société ABC et aux critères établis dans le cadre des principes généralement reconnus en matière de protection des renseignements personnels.

Étant donné les limites inhérentes des contrôles, il se peut que des erreurs ou des fraudes surviennent et ne soient pas détectées. De plus, la projection de conclusions sur des périodes

futures, faite à la lumière de nos constatations, risque d'aboutir à des conclusions erronées du fait de changements apportés au système et aux contrôles, de changements nécessaires mais non apportés ou d'une détérioration du degré d'efficacité des contrôles.

L'utilisation par la société ABC du sceau WebTrust est l'expression symbolique du contenu du présent rapport et ne vise ni à constituer une mise à jour du rapport, ni à fournir une assurance supplémentaire, et ne doit pas être interprétée en ce sens.

[*Nom du cabinet de CA*]  
Comptables agréés

[*Ville (Province)*]  
[*Date*]

### **Exemple d'assertion de la direction**

Au cours de la période du xx xxxx 2008 au yy yyyy 2008, la société ABC a, à tous les égards importants :

exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de \_\_\_\_\_ [*description des entités et activités visées, par exemple «les activités de ventes postales par catalogue»*] (l'«activité») de façon à fournir l'assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés et communiqués conformément aux engagements énoncés dans notre avis sur la protection des renseignements personnels relatif à l'activité et aux critères établis dans le cadre des principes généralement reconnus en matière de protection des renseignements personnels publiés par l'Institut Canadien des Comptables Agréés (ICCA) et l'American Institute of Certified Public Accountants (AICPA); respecté les engagements énoncés dans notre avis sur la protection des renseignements personnels.

## Exemple 2 — Rapport portant directement sur les éléments considérés

### Rapport du vérificateur sur la protection des renseignements personnels WebTrust

À la direction de la société ABC inc. :

Nous avons vérifié 1) l'efficacité des contrôles exercés par la société ABC inc. (la société ABC) sur les renseignements personnels recueillis dans le cadre de \_\_\_\_\_ [description des entités et activités visées, par exemple «les activités de ventes postales par catalogue»] (l'«activité») de façon à fournir l'assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés et communiqués conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels et aux critères établis dans le cadre des principes généralement reconnus en matière de protection des renseignements personnels publiés par l'Institut Canadien des Comptables Agréés (ICCA) et l'American Institute of Certified Public Accountants (AICPA), et 2) le respect, par la société ABC, des engagements énoncés dans son avis sur la protection des renseignements personnels relatif à l'activité au cours de la période du xx xxxx 2008 au yy yyyy 2008. La responsabilité du maintien de l'efficacité de ces contrôles et du respect des engagements énoncés dans l'avis sur la protection des renseignements personnels incombe à la direction de la société ABC. Notre responsabilité consiste à exprimer une opinion en nous fondant sur notre vérification.

Notre vérification a été effectuée conformément aux normes relatives aux missions de certification établies par l'ICCA. Ces normes exigent que la vérification soit planifiée et exécutée de manière à fournir une assurance raisonnable sur laquelle sera fondée notre opinion. Notre vérification a consisté 1) à acquérir une compréhension des contrôles exercés par la société ABC relativement à la protection des renseignements personnels, 2) à tester et à évaluer l'efficacité du fonctionnement de ces contrôles, 3) à vérifier que la société a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels et 4) à mettre en œuvre les autres procédés que nous avons jugés nécessaires dans les circonstances. Nous estimons que notre vérification constitue une base raisonnable à l'expression de notre opinion.

À notre avis, au cours de la période du xx xxxx 2008 au yy yyyy 2008, la société ABC a, à tous les égards importants, 1) exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de l'activité, de façon à fournir l'assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés et communiqués conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels et aux critères établis dans le cadre des principes généralement reconnus en matière de protection des renseignements personnels, et 2) respecté les engagements énoncés dans son avis sur la protection des renseignements personnels.

Étant donné les limites inhérentes des contrôles, il se peut que des erreurs ou des fraudes surviennent et ne soient pas détectées. De plus, la projection de conclusions sur des périodes futures, faite à la lumière de nos constatations, risque d'aboutir à des conclusions erronées du fait de changements apportés au système et aux contrôles, de changements nécessaires mais non apportés ou d'une détérioration du degré d'efficacité des contrôles.

L'utilisation par la société ABC du sceau WebTrust est l'expression symbolique du contenu du présent rapport et ne vise ni à constituer une mise à jour du rapport, ni à fournir une assurance supplémentaire, et ne doit pas être interprétée en ce sens.

[Nom du cabinet de CA]  
Comptables agréés

[Ville (Province)]  
[Date]