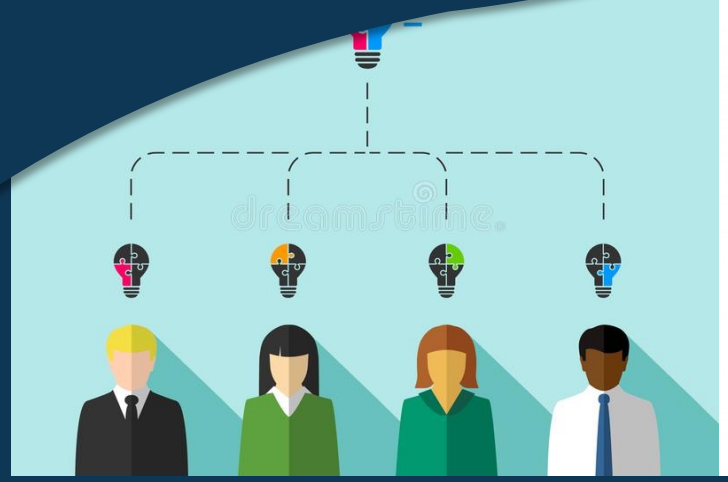
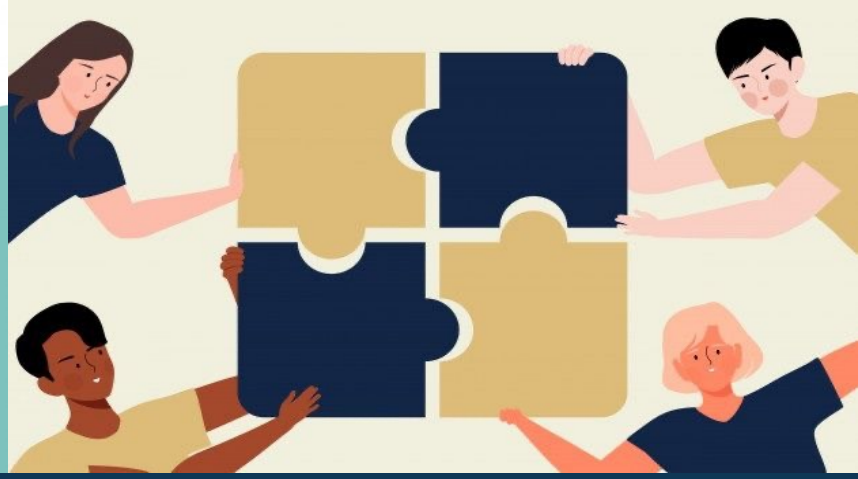
Citizen F1RST

OPTIMISÉ PAR
Institut des services axés sur les citoyens

Protection de la vie privée dès la conception dans les services gouvernementaux numériques

- Importance de la protection de la vie privée dès la conception dans les services gouvernementaux numériques
- État actuel de la confidentialité en matière de numérique dans les services gouvernementaux
- Défis et occasions liés à la mise en œuvre de la confidentialité dès la conception





RAPPORT EXÉCUTIF MENSUEL DES CONSEILS MIXTES

Créé par le comité de recherche

Juin 2023

Images : iStock

1. Importance de la protection de la vie privée dès la conception dans les services gouvernementaux numériques

La confidentialité dès la conception (CdC) dans les services gouvernementaux numériques est une approche proactive qui consiste à intégrer la confidentialité dans les spécifications de conception des technologies, des pratiques commerciales et de l'infrastructure physique.

À l'ère du numérique, la CdC est essentielle, car la protection des renseignements personnels constitue une préoccupation primordiale. La CdC n'est pas seulement un enjeu de conformité, mais également un enjeu en matière de renforcement de la confiance et d'amélioration de l'expérience client. Elle permet aux services gouvernementaux d'être transparents et responsables, favorisant la confiance des citoyens à l'égard des activités numériques du gouvernement.

La CdC propose un système de prévention, un peu comme un modèle médical de prévention, qui tente d'empêcher les atteintes à la vie privée et à la protection des données, améliorant ainsi la protection des données, dès le départ.

Ce principe vise essentiellement à garantir que la confidentialité fait partie intégrante de l'architecture et des opérations du système. Au lieu de traiter la confidentialité comme une fonction complémentaire ou un exercice superficiel, l'approche « dès la conception » intègre la confidentialité dans la conception du système, garantissant ainsi une protection plus robuste et systématique de la confidentialité.

À l'ère des mégadonnées et de l'analyse, la CdC garantit que la confidentialité n'est pas une caractéristique ajoutée après coup, mais un élément de la conception du système. La CdC permet d'éviter les atteintes à la vie privée coûteuses, ainsi que les atteintes à la réputation qui en découlent. La CdC dans les services gouvernementaux numériques favorise l'assurance de la confidentialité et le respect des lois et règlements en matière de confidentialité. Elle s'inscrit dans la tendance mondiale en matière de règlements en matière de protection des données, comme le *Règlement général sur la protection des données* (RGPD) de l'UE.

La mise en œuvre de la CdC dans les services gouvernementaux numériques peut également mener à l'innovation en matière de prestation de services. Elle permet le développement de nouveaux services numériques non seulement efficaces, mais également respectueux du droit à la vie privée.

Pourquoi ce rapport est-il important?

Le rapport revêt une importance considérable pour plusieurs raisons. Premièrement, il souligne le besoin pressant en matière de confidentialité dès la conception (CdC) dans les services gouvernementaux numériques, un concept qui devient de plus en plus essentiel au sein de la société actuelle axée sur les données.

En soulignant la pertinence et l'urgence de la CdC, le rapport vise à attirer l'attention des décideurs politiques et des parties prenantes du secteur public et à les inciter à agir. Deuxièmement, il présente un portrait exhaustif de l'état actuel de la confidentialité en matière de numérique dans les services gouvernementaux, permettant une évaluation plus précise de la situation. On ne soulignera jamais assez l'importance de CdC, car elle constitue la base de toutes les décisions et stratégies ultérieures.

Enfin, le rapport recense les défis et les occasions découlant de la mise en œuvre de la CdC, offrant un point de vue équilibré visant à éclairer les décisions à venir. Il décrit également des mesures pratiques concernant la mise en œuvre de la CdC, ce qui en fait un guide précieux pour les décideurs.

Qu'est-ce qui est abordé dans ce rapport exécutif?

Ce rapport comprend les éléments suivants :

- Importance de la protection de la vie privée dès la conception dans les services gouvernementaux numériques
- État actuel de la confidentialité en matière de numérique dans les services gouvernementaux
- Défis et occasions liés à la mise en œuvre de la confidentialité dès la conception
- Mesures visant à mettre en œuvre la confidentialité dès la conception dans les services gouvernementaux numériques
- Avantages et perspectives d'avenir concernant la confidentialité dès la conception dans les services gouvernementaux numériques

Sources : 1. Cavoukian, A. (2010). Privacy by Design: The 7 Foundational Principles.
2. Bélanger, F., et Carter, L. (2008). Trust and risk in e-government adoption. The Journal of Strategic Information Systems.

2. État actuel de la confidentialité en matière de numérique dans les services gouvernementaux

L'état actuel de la confidentialité en matière de numérique dans les services gouvernementaux est mitigé. Certains gouvernements ont réalisé d'importants progrès en matière d'intégration de la confidentialité dans leurs services numériques, tandis que d'autres accusent un retard.

La numérisation accrue des services gouvernementaux a ouvert de nouvelles voies pour la collecte et le traitement des données. Toutefois, cette situation a également soulevé des inquiétudes quant à l'utilisation malveillante éventuelle des données personnelles et au risque d'atteinte à la protection des données. Dans de nombreux cas, les règlements en matière de confidentialité n'ont pas suivi le rythme des progrès technologiques. Cela a entraîné des lacunes réglementaires, laissant les données personnelles exposées à l'utilisation malveillante éventuelle.

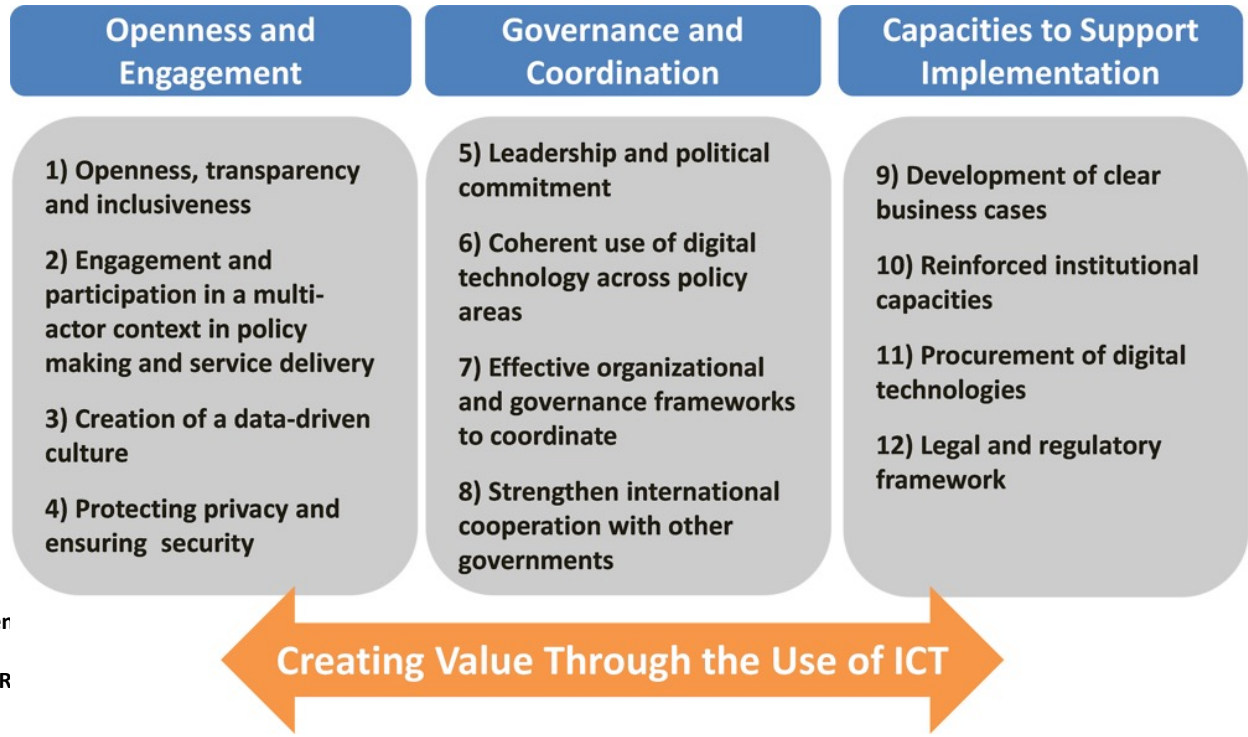
Du côté positif, certains gouvernements ont pris des mesures proactives pour répondre à ces préoccupations. Ils ont mis en œuvre les principes de CdC, garantissant que la confidentialité fait partie intégrante de leurs services numériques. Toutefois, il reste encore beaucoup de travail à faire. De nombreux services gouvernementaux ne disposent pas d'une stratégie exhaustive en matière de protection de la vie privée, ce qui les rend vulnérables aux risques liés à la vie privée.

En outre, il est nécessaire d'accroître la transparence et la responsabilité dans le traitement des données personnelles par les services gouvernementaux. Les citoyens doivent avoir la garantie que leurs données sont traitées de manière responsable et sécurisée.

L'intégration de nouvelles technologies comme l'intelligence artificielle (IA) et l'Internet des objets (IdO) dans les services gouvernementaux pose des défis supplémentaires en matière de confidentialité. Quoique ces technologies puissent améliorer considérablement la prestation de services, elles augmentent également le potentiel d'atteinte à la vie privée si elles ne sont pas gérées de manière convenable.

Il existe souvent un manque d'alphabétisation numérique chez les citoyens, ce qui entraîne une mauvaise compréhension et une maîtrise médiocre des données personnelles. Les gouvernements doivent jouer un rôle proactif dans l'éducation du public sur les droits en matière de protection des renseignements personnels et sur la manière dont leurs données sont utilisées dans les services numériques.

Malgré les défis, de nombreux gouvernements reconnaissent désormais l'importance de la confidentialité en matière de numérique et prennent des mesures pour l'améliorer. Ces efforts doivent être cohérents et continus, car la protection de la vie privée n'est pas une tâche ponctuelle, mais un engagement continu.



Sources :
- **Reddick, C. G. (2010). The Adoption of Centralized Customer Service Systems: A Survey of Local Governments. Governmer Information Quarterly.**
- **Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. Computer Law & Security R**
- **OECD**

3. Défis et occasions liés à la mise en œuvre de la confidentialité dès la conception

La mise en œuvre de la CdC dans les services gouvernementaux numériques comporte des défis complexes, mais elle ouvre également la porte à des occasions sans précédent en matière d'amélioration de la protection de la vie privée et de la prestation de services. Pour réussir la mise en œuvre réussie, il est nécessaire de comprendre l'interaction entre les avancées technologiques, les paysages réglementaires, les cultures organisationnelles et les limites des ressources, et de les exploiter stratégiquement pour renforcer la confidentialité et la qualité du service.

Défis technologiques

- Les avancées technologiques rapides peuvent compliquer l'intégration de la confidentialité dans les services numériques. Toutefois, ces avancées offrent également de nouveaux outils et de nouvelles méthodes permettant d'améliorer la confidentialité, comme la confidentialité différentielle et le chiffrement homomorphe, qui peuvent être utilisés pour protéger les données de nature délicate tout en permettant une analyse utile des données.
- La complexité croissante des services numériques pose également un défi. Toutefois, l'évaluation approfondie de l'incidence sur la vie privée et l'intégration des mesures de contrôle de la confidentialité directement dans l'architecture des systèmes permettent de gérer cette complexité.

Défis en matière de règlements

- La conformité aux différents règlements à l'échelle mondiale en matière de confidentialité peut être une tâche ardue pour les services gouvernementaux numériques. Toutefois, la mise en œuvre de la CdC peut aider à garantir la conformité dans différents territoires de compétence, réduisant ainsi le risque réglementaire.
- Comme les paysages réglementaires peuvent changer de manière imprévisible, la CdC fournit un cadre souple permettant aux services gouvernementaux de s'adapter aux nouveaux règlements, réduisant ainsi les coûts éventuels liés à la conformité.

Défis organisationnels

- La culture organisationnelle et les attitudes à l'égard de la confidentialité peuvent poser un défi important. Toutefois, la promotion d'une culture de confidentialité peut renforcer la confiance tant au sein de l'organisme que chez le public.
- La mise en œuvre de la CdC peut exiger des modifications importantes aux processus et stratégies opérationnels. Toutefois, cette transformation peut mener à l'accroissement de l'efficacité et de la sûreté des activités, améliorant ainsi la prestation de services.

Défis liés aux ressources

- La mise en œuvre de la CdC peut être gourmande en ressources, exigeant des investissements dans les nouvelles technologies, la formation du personnel et éventuellement dans la restructuration. Toutefois, ces investissements peuvent être rentables à long terme, car ils permettent d'éviter les atteintes à la vie privée ainsi que les amendes connexes, et de renforcer la confiance du public.
- S'il peut être difficile d'obtenir un budget suffisant, la CdC peut également présenter des occasions d'économies découlant de la simplification de la gestion des données et de processus de conformité efficaces.

Sources : Hoepman, J.-H. (2014). Privacy Design Strategies. ICT Systems Security and Privacy Protection; Bennett, C. J., et Raab, C. D. (2006). The governance of privacy: policy instruments in global perspective. MIT press.

4. Mesures visant à mettre en œuvre la confidentialité dès la conception dans les services gouvernementaux numériques

Plusieurs mesures peuvent être prises pour mettre en œuvre de manière efficace la confidentialité dès la conception dans les services gouvernementaux numériques, chacune exigeant une planification et une exécution réfléchies. Ces mesures améliorent non seulement la protection de la vie privée, mais contribuent également à créer un environnement numérique plus sûr et plus fiable pour les citoyens. En adoptant ces pratiques, les gouvernements peuvent renforcer la confiance du public, atténuer les risques et créer un précédent positif pour une transformation numérique respectueuse de la vie privée.

Élaborer une stratégie exhaustive en matière de confidentialité : une stratégie exhaustive en matière de confidentialité sert de feuille de route pour la mise en œuvre des principes de la CdC. Pour ce faire, on doit recenser les risques en matière de confidentialité, définir les objectifs en matière de confidentialité et décrire les mesures visant à atteindre ces objectifs. On doit également harmoniser la stratégie en matière de confidentialité avec la stratégie numérique globale, en veillant à ce que la confidentialité ne soit pas compromise dans le cadre de la transformation numérique.

Mener des évaluations des facteurs relatifs à la vie privée : les évaluations des facteurs relatifs à la vie privée (ÉFVP) sont un outil essentiel pour cerner et atténuer les risques liés à la vie privée dans les services numériques. Les ÉFVP doivent être menées périodiquement et chaque fois que des modifications importantes sont apportées aux services numériques. Ces évaluations peuvent aider à cerner les risques éventuels d'atteinte à la vie privée au début du processus de développement, ce qui permet de traiter les risques de manière proactive plutôt que réactive.

Favoriser une culture de confidentialité : il est essentiel d'intégrer une culture de confidentialité au sein de l'organisme. Cela exige de former les employés en ce qui concerne les principes de confidentialité et l'importance de protéger les renseignements personnels. Une culture de la confidentialité repose également sur la promotion de la transparence et de la responsabilité quant aux pratiques de traitement des données, renforçant la confiance du public à l'égard des services gouvernementaux numériques.

Investir dans les technologies de protection de la vie privée : l'investissement dans les technologies de protection de la vie privée peut aider à protéger les données personnelles et à renforcer la confidentialité au sein des services numériques. Ces technologies peuvent comprendre le chiffrement, des outils d'anonymisation et des solutions de stockage de données sécurisées. Quoique cela puisse exiger un investissement préalable, cette mesure peut être rentable à long terme, car elle permet d'éviter les atteintes à la vie privée ainsi que les atteintes connexes à la réputation et aux finances.

Mobiliser les parties prenantes : la mobilisation des parties prenantes, y compris les citoyens, les employés et les organismes de réglementation, est essentielle. Leur apport peut éclairer la conception des services numériques afin de garantir qu'ils répondent aux attentes en matière de confidentialité et aux exigences réglementaires. La mobilisation des parties prenantes peut également renforcer la confiance et promouvoir la compréhension des pratiques en matière de confidentialité, renforçant ainsi la crédibilité des services gouvernementaux numériques.

Examiner et mettre à jour périodiquement les pratiques en matière de confidentialité : les pratiques en matière de confidentialité doivent faire l'objet d'un examen et d'une mise à jour périodiques pour garantir leur harmonisation avec les avancées technologiques, les modifications réglementaires et l'évolution des attentes en matière de confidentialité. Cette approche proactive peut aider à éviter les pièges éventuels en matière de confidentialité et à améliorer la conformité. Des examens périodiques permettent également d'évaluer l'efficacité des pratiques en matière de confidentialité existantes et d'apporter des améliorations, au besoin.

Sources : Hustinx, P. (2010). Privacy by Design: delivering the promises. Identity in the Information Society; Warren, S. D., et Brandeis, L. D. (1890). The right to privacy. Harvard law review.

Renforce la confiance du public : la mise en œuvre de la CdC dans les services gouvernementaux numériques renforce la confiance du public. Lorsque les citoyens constatent que leur vie privée est respectée et protégée, leur confiance à l’égard des services numériques augmente.

Cette confiance est essentielle pour une adoption réussie des services numériques. Cela améliore également la réputation des services gouvernementaux, en les présentant comme des gardiens responsables des renseignements personnels.

Atténue les risques juridiques et réglementaires : la CdC aide à atténuer les risques juridiques et réglementaires en garantissant le respect des lois et règlements en matière de confidentialité. Cela peut aider à éviter des amendes coûteuses et des différends d’ordre juridique. La CdC fournit un cadre souple qui peut s’adapter à l’évolution des règlements. Cette capacité d’adaptation est essentielle dans un paysage réglementaire en évolution rapide.

Stimule l’innovation : la CdC peut stimuler l’innovation dans les services gouvernementaux numériques. Le fait de tenir compte de la confidentialité dès la phase de conception permet d’élaborer des solutions nouvelles et créatives pour fournir des services dans le respect de la confidentialité.

Cette approche peut mener au développement de technologies et de services distincts qui améliorent la confidentialité, établissant une référence à suivre pour d’autres secteurs.

Simplifie les activités : la CdC peut simplifier les activités en intégrant la confidentialité dans le processus de conception des services. Cela peut renforcer l’efficacité des processus de gestion des données et de conformité. L’intégration de la confidentialité dans l’architecture des systèmes permet de résoudre les problèmes éventuels relatifs à la confidentialité, dès le début du processus de développement, réduisant ainsi les modifications coûteuses, plus tard.

Perspectives d’avenir : à l’avenir, la CdC demeurera un élément clé des services gouvernementaux numériques. En raison des préoccupations croissantes relatives à la confidentialité des données et de la surveillance réglementaire croissante, la CdC propose une approche proactive en matière de protection de la vie privée. À l’avenir, la CdC gagnera probablement en popularité, un nombre accru de gouvernements adoptant cette approche. Cette tendance améliorera non seulement la protection de la vie privée, mais favorisera également l’innovation et la confiance du public à l’égard des services gouvernementaux numériques.

Sources : Bélanger, F., et Carter, L. (2008). Trust and risk in e-government adoption. The Journal of Strategic Information Systems; Van Dijk, Niels, Raphaël Gellert, et Kjetil Rommetveit. « A risk to a right? Beyond data protection risk assessments. » Computer Law & Security Review 32.2 (2016): 286-306.

Autres documents à consulter

- Schaar, Peter. « Privacy by design. » Identity in the Information Society 3, no. 2 (2010): 267-274.
- Gürses, Seda, Carmela Troncoso, et Claudia Diaz. « Engineering privacy by design. » Computers, Privacy & Data Protection 14, no. 3 (2011): 25.
- Rubinstein, Ira S. « Regulating privacy by design. » Berkeley Tech. LJ 26 (2011): 1409.
- Langheinrich, Marc. « Privacy by design – principles of privacy-aware ubiquitous systems. » In Ubicomp 2001: Ubiquitous Computing: International Conference Atlanta Georgia, USA, September 30–October 2, 2001 Proceedings, pp. 273-291. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001.
- Hustinx, Peter. « Privacy by design: delivering the promises. » Identity in the Information Society 3, no. 2 (2010): 253-255.
- Klitou, Demetrius. « Privacy-invading technologies and privacy by design. » Inf. Technol. Law Ser 25 (2014): 27-45.

Autres articles dignes de mention :

- Barth, Susanne, Dan Ionita, et Pieter Hartel. « Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines. » ACM Computing Surveys (CSUR) 55, no. 3 (2022): 1-37.
- Wiese Schartum, Dag. « Making privacy by design operative. » International Journal of Law and Information Technology 24, no. 2 (2016): 151-175.

Dépôt de recherches

Consultez le Dépôt de recherches de Citoyens en tête.

Ajouts récents au dépôt de recherches :

Processus décisionnel fondé sur les données au gouvernement

Ce rapport comprend les éléments suivants :

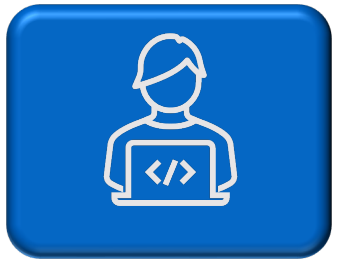
- Collecte et gestion des données pour pouvoir prendre des décisions judicieuses
- Tirer parti de l'analyse des données et de l'IA dans les politiques publiques
- Défis et risques liés au processus décisionnel gouvernemental axé sur les données
- Stratégies de mise en œuvre

Tendances dans le bulletin quotidien

L'accord de principe qui a mis fin à la plus importante grève des employés fédéraux depuis des décennies pourrait être à l'origine d'un tout nouveau conflit concernant le travail à distance, une demande qui venait juste après les salaires dans l'impasse de deux semaines et qui ne s'estompe pas.

« Cette grève ne devait pas avoir lieu », a déclaré Linda Duxbury, professeure titulaire en gestion, à l'Université Carleton, et spécialiste de l'équilibre travail-vie personnelle et du travail à distance.

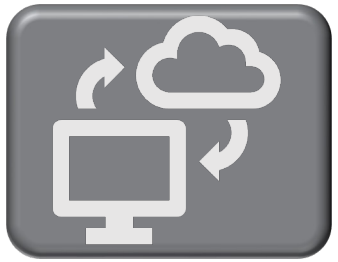
Elle reproche à la fois au gouvernement et à son plus important syndicat fédéral, l'Alliance de la fonction publique du Canada, de ne pas avoir géré les attentes des travailleurs concernant le travail à distance, qui, selon elle, est un « privilège, non un droit ».



Les types de conflits d'intérêts qui ont déclenché un scandale au sein de l'entreprise mondiale PwC sont « répandus » dans le secteur des services-conseils, selon d'anciens hauts responsables et spécialistes indépendants.

Le gouvernement fédéral a également été informé que les cabinets-conseils pourraient adapter leurs conseils au gouvernement afin d'accroître leurs recettes, au lieu de donner des conseils francs dans l'intérêt supérieur des contribuables.

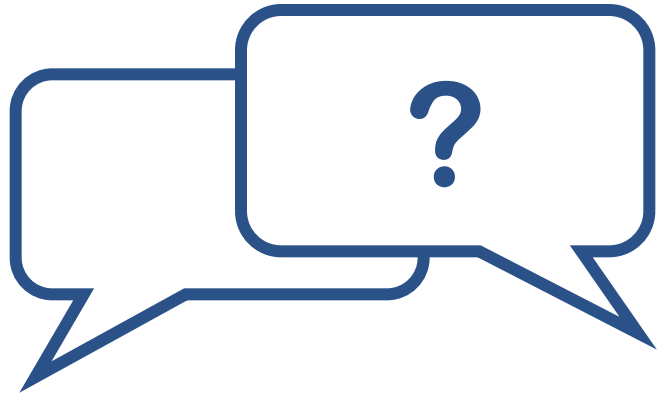
Lundi soir, le directeur général de PwC Australie, Tom Seymour, a démissionné à la suite des critiques soutenues à l'encontre de l'entreprise qui aurait tiré parti de la diffusion de la politique fiscale confidentielle du gouvernement après de ses collègues.



Dans le cadre du balado Priorities, le dirigeant principal de l'information par intérim de l'Illinois, Brandon Ragle, fait valoir que la plateforme d'identité de l'État détermine la façon dont l'État traite les services numériques.

Plus de deux millions de résidents de l'Illinois sont inscrits à la plateforme d'identité de l'État, appelée ILogin. L'outil permet aux résidents d'accéder à plusieurs services au moyen d'une seule connexion.

« Au cours des dernières années, nous avons travaillé à la modernisation de nos plateformes numériques, pour en arriver cet espace où nous pouvons obtenir des sites Web assez utilisables », indique M. Ragle. « Cette année, nous souhaitons nous efforcer d'obtenir plus de nos applications utilisées pour les services en ligne en arrière-plan et de vraiment nous attarder au volet convivialité. »



Vos idées nous intéressent!

Connaissez-vous quelqu'un que le rapport exécutif des conseils mixtes pourrait intéresser? Veuillez lui transmettre une copie de ce rapport. Si vous n'êtes pas déjà abonné, vous pouvez maintenant vous inscrire afin de recevoir le rapport exécutif. Envoyez vos questions à info@iccs-isac.org.

Suivez-nous :