Deloitte.

RYERSON UNIVERSITY

Protection intégrée de la vie privée

Nouvelle norme de certification de protection de la vie privée

La protection intégrée de la vie privée est un cadre qui se fonde sur l'intégration proactive de la protection de la vie privée dans la conception et le fonctionnement des systèmes informatiques, de l'infrastructure des réseaux et des pratiques d'affaires.

Cadre de la protection intégrée de la vie privée

Les organisations comprennent bien la nécessité de combiner l'innovation à la protection des renseignements personnels et confidentiels de leurs clients, de leurs employés et de leurs partenaires d'affaires. La tâche devient cependant de plus en plus difficile à l'ère des « données massives », pour plusieurs raisons :

- La mondialisation favorise un environnement où les travailleurs du savoir ressentent le besoin d'échanger des renseignements plus rapidement, exposant ainsi les organisations à une plus forte probabilité d'atteintes à la sécurité de l'information.

- Les frontières organisationnelles ne sont plus statiques, faisant en sorte qu'il est difficile de savoir comment et où les renseignements sont conservés et gérés, et qui y a accès.

- La collaboration et les outils de réseautage social promettent de nouvelles possibilités, mais ils s'accompagnent également de vulnérabilités qui peuvent être sérieuses en l'absence d'une gestion proactive.

> « Il devient de plus en plus difficile de protéger la vie privée tout en répondant aux exigences réglementaires visant la protection des données dans le monde. Une approche axée sur le risque exhaustive et mise en œuvre de façon appropriée – selon laquelle les risques définis à l'échelle mondiale sont prévus et des contre-mesures sont intégrées dans les systèmes et les activités dès la conception – peut être beaucoup plus efficace et plus susceptible de répondre au large éventail d'exigences des nombreux territoires de compétence. » – Dr Ann Cavoukian, directrice générale du Privacy and Big Data Institute de l'Université Ryerson, trois mandats à titre de commissaire à l'information et à la protection de la vie privée de l'Ontario, créatrice de La protection intégrée de la vie privée

Dans ce contexte électronique complexe des affaires, un modèle de conformité qui se résume à cocher des cases crée un faux sentiment de sécurité. Voilà pourquoi il devient nécessaire d'adopter une approche axée sur le risque pour cerner les vulnérabilités numériques et combler les lacunes en matière de protection de la vie privée. Lorsque vous avez pris les mesures nécessaires pour vous assurer de façon proactive que des contrôles sont mis en place et que les renseignements sont sécurisés, faire certifier vos pratiques en matière de protection de la vie privée par rapport à une norme mondiale peut porter le niveau de protection de la vie privée et de sécurité de votre entreprise à un échelon supérieur. De plus, en combinant la prévention du risque d'entrave à la vie privée et la certification, on obtient la **certification de protection intégrée de la vie privée**.

La capacité éprouvée à sécuriser et à protéger les données numériques – tant les vôtres que celles de vos clients – est de plus en plus reconnue comme un impératif d'affaires qui procure un avantage concurrentiel.

7 principes fondamentaux

La protection intégrée de la vie privée consiste à intégrer la protection de la vie privée dans la conception, le fonctionnement et la gestion d'un système, d'un processus d'affaires ou d'une spécification de conception. Elle repose sur le respect de 7 principes fondamentaux :

1. **Prendre des mesures proactives et non réactives, des mesures préventives et non correctives**
   Prévoir, repérer et prévenir les incidents d'atteinte à la vie privée avant qu'ils ne se produisent; autrement dit, agir avant et non après de tels incidents.
2. **Assurer la protection implicite de la vie privée**
   Veiller à ce que les renseignements personnels soient systématiquement protégés au sein des systèmes informatiques ou dans le cadre des pratiques internes, de sorte que les particuliers n'ont à poser aucun geste.
3. **Intégrer la protection de la vie privée dans la conception**
   Les mesures de protection de la vie privée ne doivent pas être greffées après coup, mais plutôt constituer des éléments pleinement intégrés du système.
4. **Assurer une fonctionnalité intégrale (selon un paradigme à somme positive et non à somme nulle)**
   La protection intégrée de la vie privée se fonde sur une approche gagnante à l'égard de tous les objectifs légitimes de conception des systèmes; autrement dit, la protection de la vie privée et la sécurité sont deux objectifs importants, et aucun compromis inutile n'est nécessaire pour réaliser les deux.
5. **Assurer la sécurité de bout en bout**
   La sécurité du cycle de vie des données signifie que toutes les données doivent être conservées de façon sécurisée, puis détruites quand elles ne sont plus utiles.
6. **Assurer la visibilité et la transparence, garder la porte ouverte**
   Assurer aux intervenants que les pratiques et les technologies fonctionnent conformément aux objectifs et sous réserve d'une vérification indépendante.
7. **Respecter la vie privée des utilisateurs, garder le regard axé sur l'utilisateur**
   Adopter une approche axée sur l'utilisateur; les intérêts du droit individuel à la vie privée doivent être soutenus par des mesures strictes et implicites de protection de la vie privée, d'avis appropriés et des fonctions conviviales.

Toute organisation qui lance de nouveaux produits, services ou technologies novatrices, ou qui étend ses activités à de nouvelles régions au moyen de fusions ou acquisitions, peut bénéficier énormément de la certification de protection de la vie privée.

Avantages de la certification : récolter les fruits

Assurer la protection de la vie privée et la sécurité – à toutes les étapes du cycle de vie des données (p. ex., collecte, utilisation, conservation, stockage, élimination ou destruction) – est devenu essentiel pour éviter la responsabilité juridique, assurer la conformité à la réglementation, protéger la marque et préserver la confiance des clients. Cela est d'autant plus vrai dans le cas des organisations qui font de plus en plus l'objet d'une surveillance accrue, tant à l'interne par leur conseil d'administration qu'à l'externe par les organismes de réglementation et leurs partenaires d'affaires. Grâce à une approche dynamique et proactive en matière de protection de la vie privée, la certification de protection intégrée de la vie privée conférera à votre organisation les capacités suivantes :

- Assurer la conformité en devançant la législation et en minimisant le risque lié à la conformité
- Réduire la probabilité d'amendes et de pénalités, notamment les pertes financières ou la responsabilité associée aux atteintes à la vie privée
- Consolider son image de marque en favorisant une meilleure confiance des consommateurs, obtenant ainsi un avantage concurrentiel appréciable
- Mieux gérer la situation faisant suite à des incidents d'atteinte à la vie privée afin de regagner la confiance des consommateurs
- Maintenir des meilleures pratiques en faisant vérifier les contrôles de protection de la vie privée et de sécurité par un organisme indépendant plutôt que de s'en tenir à l'autodéclaration ou à l'autoévaluation

Coût associé à l'adoption d'une approche réactive face aux atteintes à la vie privée

La protection intégrée de la vie privée va bien au-delà des pratiques équitables de traitement de l'information et des normes de protection de la vie privée reconnues, garantissant pratiquement la conformité à la réglementation, peu importe où vous exercez vos activités.

Étapes de la certification

Mise en œuvre de la protection intégrée de la vie privée : trois étapes à suivre

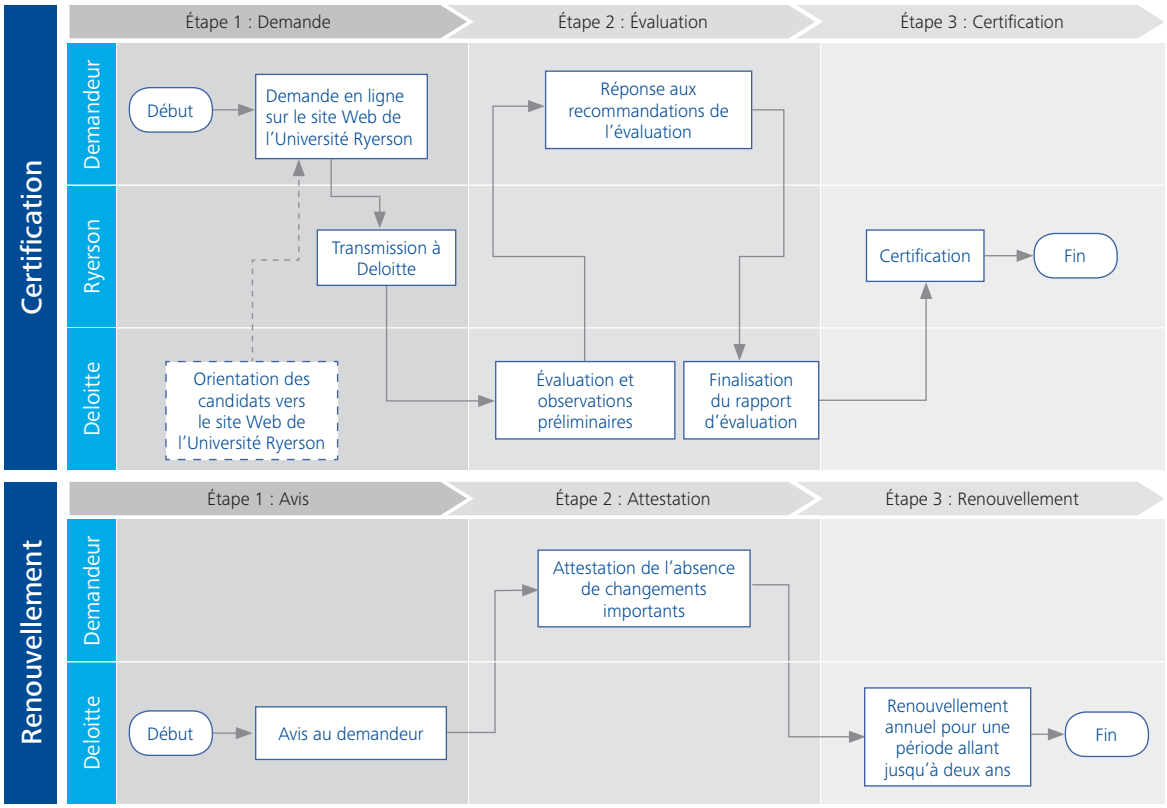
En vertu du cadre de la protection intégrée de la vie privée, l'Université Ryerson a la responsabilité d'accréditer les organisations qui répondent aux critères nécessaires en matière de protection de la vie privée. Pour obtenir la certification, les organisations doivent d'abord faire l'objet d'une première évaluation par Deloitte.

En utilisant un ensemble de critères d'évaluation bien définis, les professionnels de la protection de la vie privée et de la sécurité de Deloitte vérifieront votre produit, service ou gamme de services par rapport aux 7 principes fondamentaux de la protection intégrée de la vie privée. Nous évaluons également la solidité de vos pratiques en matière de protection de la vie privée par rapport à des principes reconnus internationalement, notamment les règlements en matière de protection de la vie privée, les exigences d'autoréglementation du secteur et les meilleures pratiques sectorielles (p. ex., normes FIPS, OCDE, PPGR, CBR et cadre de protection de la vie privée de l'APEC) selon une méthode d'évaluation qui se fonde sur des exigences légales harmonisées en matière de protection de la vie privée et de sécurité.

À cette fin, Deloitte a mis en œuvre le cadre de protection intégrée de la vie privée en élaborant 30 critères de protection de la vie privée et 107 contrôles indicatifs de la protection de la vie privée à l'égard desquels les organisations seront évaluées, au moyen d'une technique unique de carte de pointage qui renvoie à chacun des 7 principes fondamentaux.

Faire de la protection de la vie privée une priorité : Deloitte s'appuie sur notre équipe mondiale de professionnels de la protection de la vie privée et de la sécurité de l'information qui détiennent la certification de protection intégrée de la vie privée, notamment un ancien responsable de la réglementation en matière de protection de la vie privée, des avocats spécialisés en droit relatif au respect de la vie privée, ainsi que des spécialistes des TI et de la sécurité. Adoptant une approche globale axée sur le risque, Deloitte vérifiera vos contrôles au moyen d'une technique de carte de pointage quantifiable pour offrir la certification de protection de la vie privée dont votre organisation a besoin.

La certification consiste en un simple processus en trois étapes : demande, évaluation et certification.



Les organisations peuvent obtenir la certification une fois que l'évaluation est terminée; toute cote d'évaluation inférieure à « satisfaisante » devra être examinée avant l'attribution de la certification complète.

Approche d'évaluation de Deloitte

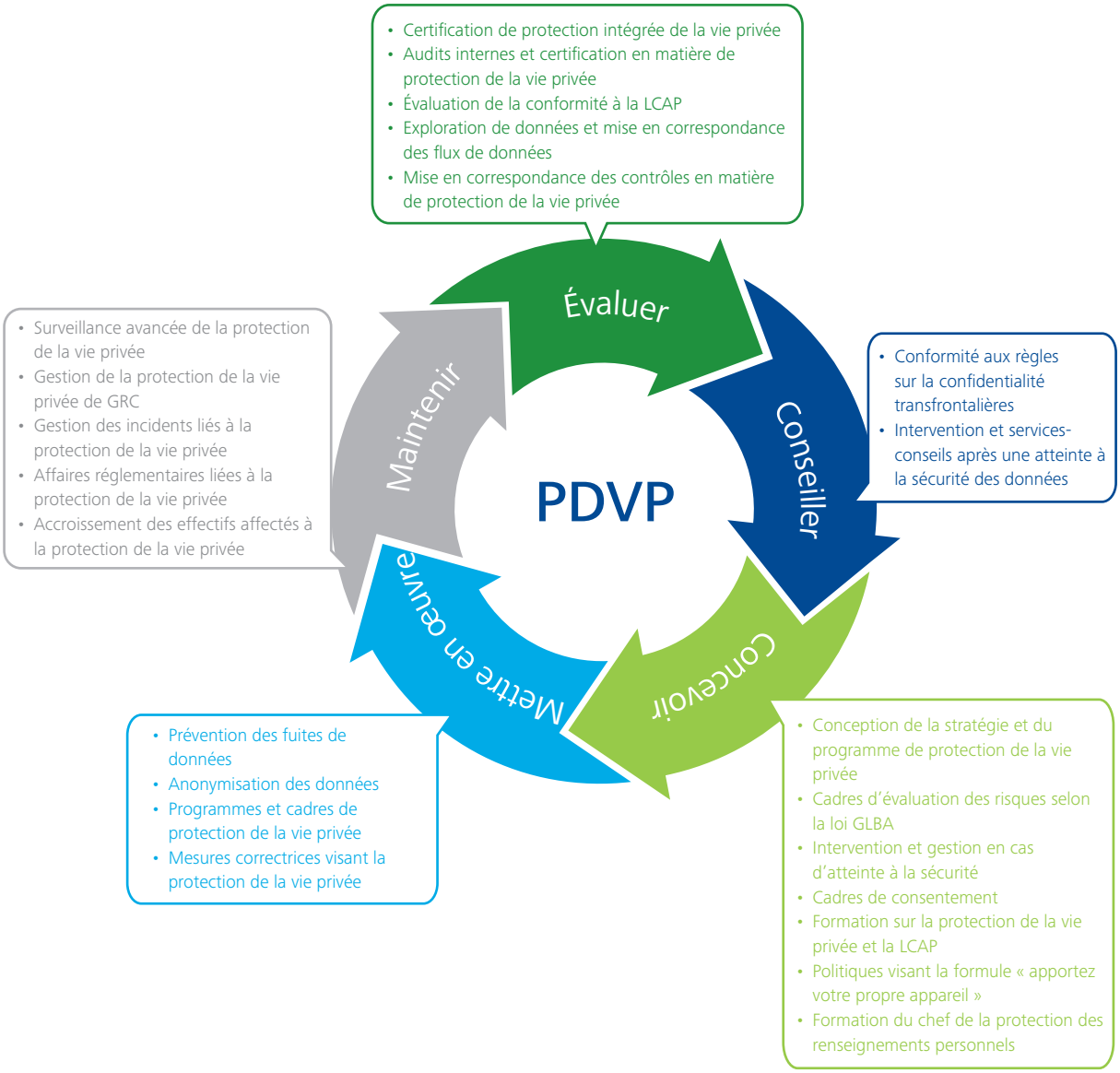
Voici comment se déroule le processus avant l'obtention de la certification :

Portée	Nous collaborons d'abord avec vous afin de déterminer la portée de l'examen de vos mesures de protection de la vie privée. **La portée de l'évaluation peut comprendre :** ☑ Tous les types de renseignements personnels détenus et les processus d'affaires connexes, incluant les renseignements médicaux et les renseignements sur les employés ☑ Un secteur défini de l'organisation, un secteur d'activité, un service, un système ou une initiative
Évaluation et tests	**Nos professionnels de la protection de la vie privée et de la sécurité :** ☑ Utilisent une combinaison d'examens manuels, d'échantillonnage et d'informations fournies dans les cartes de pointage pour évaluer vos contrôles de conception actuels et les pratiques connexes en matière de traitement de l'information ☑ Effectuent des entrevues au sein de l'entreprise, des visites sur place (s'il y a lieu) et l'exploration des données (sur demande) afin de repérer les problèmes liés à la collecte et à l'emplacement des données ☑ Déterminent s'il existe des contrôles de la protection de la vie privée ou de la sécurité, et si les activités ou les contrôles liés à la protection de la vie privée sont bien conçus ☑ Comparent l'architecture de solutions, les pratiques connexes en matière de traitement de l'information et les processus opérationnels par rapport aux activités de contrôle
Rapport	**Nous présentons les résultats dans un rapport détaillé d'utilisation restreinte, sous forme de carte de pointage, qui :** ☑ Indique les manquements ou les lacunes dans la conception des systèmes informatiques, les politiques et les pratiques ☑ Comprend une analyse des renseignements personnels et des lacunes connexes liées à la protection de la vie privée dans tout le cycle de vie des données ☑ Contient une analyse des exigences en matière de conformité avec l'ensemble des politiques, pratiques, lois, codes et contrats pertinents ☑ Analyse chaque élément du programme, des politiques et des procédures de protection des renseignements personnels de votre organisation ☑ Comprend une analyse des lacunes qui met en évidence l'écart entre l'état de gestion des risques visé et l'état actuel ☑ Fournit à la direction des observations et des recommandations détaillées pour combler les lacunes relevées en matière de protection de la vie privée
Certification	**Dans le cadre du processus de certification, Ryerson :** ☑ S'assure que toute lacune relevée dans votre carte de pointage sur la protection de la vie privée est comblée et résolue ☑ Affiche le nom de votre entreprise sur sa page de validation pour permettre de vérifier en temps réel que la certification est à jour et valide

Une fois que vous avez obtenu la certification de protection intégrée de la vie privée, vous pouvez l'afficher sur votre site Web ou vos produits ou services, et communiquer les résultats de l'évaluation ainsi que votre certification à vos partenaires d'affaires.

Services de protection des données et de la vie privée de Deloitte

La certification de protection intégrée de la vie privée fait partie de la gamme complète des services de protection des données et de la vie privée (PDVP) offerts par Deloitte



Personnes-ressources

Sylvia Kingsmill, B.A., LL.B.
Leader nationale de la protection des données et de la vie privée
Service des risques d'entreprise
skingsmill@deloitte.ca

Dr. Ann Cavoukian, Ph.D.
Directrice générale du Privacy and Big Data Institute
ann.cavoukian@ryerson.ca

À propos de Sylvia Kingsmill

Sylvia Kingsmill, B.A., LL. B., dirige le groupe Protection des données et de la vie privée de Deloitte Canada. Elle possède 15 ans d'expérience en services-conseils stratégiques en matière de conformité fondée sur les risques et de protection de la vie privée, servant une clientèle mondiale diversifiée. Elle se spécialise dans la prestation de services-conseils aux équipes de direction sur l'élaboration et la mise en œuvre de stratégies numériques axées sur les données afin de soutenir les importantes transformations des TI et des activités, et la conformité aux exigences réglementaires. Elle intervient souvent au nom de ses clients auprès des organismes de réglementation, dont les commissaires à la protection de la vie privée, afin de corriger les problèmes liés à la conformité et d'optimiser la gestion des données et les pratiques de gouvernance. Mme Kingsmill a récemment mis au point le programme de certification de protection intégrée de la vie privée en collaboration avec le Privacy and Big Data Institute de l'Université Ryerson pour aider les clients à lancer de nouvelles technologies visant à renforcer la protection de la vie privée. Elle offre des conseils sur les utilisations éthiques et novatrices des données massives tout en protégeant la vie privée afin d'aider ses clients à gérer non seulement les risques liés à la réglementation, mais leur marque et leur stratégie de marketing à mesure qu'ils accroissent leur présence numérique.

À propos de Ann Cavoukian

Ann Cavoukian, Ph. D., est reconnue comme l'une des principales spécialistes dans le domaine de la protection de la vie privée au monde. Elle est actuellement directrice générale du Privacy and Big Data Institute de l'Université Ryerson. Nommée commissaire à l'information et à la protection de la vie privée de l'Ontario, au Canada, en 1997, Mme Cavoukian a été la première personne à cumuler trois mandats à ce titre. C'est au cours de ces mandats qu'elle a créé la protection intégrée de la vie privée, un cadre qui prévoit l'intégration proactive de la protection de la vie privée dans les spécifications de conception des technologies de l'information, de l'infrastructure des réseaux et des pratiques d'affaires, assurant ainsi la meilleure protection possible. En octobre 2010, les responsables de la réglementation présents à la Conférence internationale des commissaires à la protection des données et à la vie privée ont adopté à l'unanimité une résolution reconnaissant la protection intégrée de la vie privée en tant qu'élément essentiel de la protection fondamentale de la vie privée. Les documents sur la protection intégrée de la vie privée ont depuis été traduits en 37 langues.

Le groupe Protection des données et de la vie privée de Deloitte

Le groupe national Protection des données et de la vie privée de Deloitte regroupe des professionnels multidisciplinaires spécialisés en technologies, politiques, sécurité, droit, gouvernance et gestion de l'information, gestion de projets, communications, et affaires réglementaires liées à la protection de la vie privée. Le groupe aide les clients des secteurs public et privé, qui sont nombreux à gérer des renseignements financiers, personnels et médicaux de nature délicate conformément à d'innombrables normes et règlements régionaux et internationaux.

À propos de l'Université Ryerson et du Privacy and Big Data Institute

L'Université Ryerson est le chef de file au Canada en matière d'éducation innovatrice axée sur la carrière. Université indéniablement urbaine, elle met l'accent sur l'innovation et l'entrepreneuriat. Ryerson a pour mission de répondre aux besoins de la société et s'est depuis longtemps engagée à mobiliser sa communauté. Le Privacy and Big Data Institute de l'Université Ryerson a été créé dans le but de servir de carrefour pour les professeurs, le personnel et les étudiants de Ryerson qui participent à des projets de recherche, d'innovation et d'éducation axés sur les données. Sa mission consiste à réaliser et à promouvoir la collaboration sectorielle et à relever les défis en matière de protection de la vie privée, de sécurité et d'analytique des données.

La certification de protection intégrée de la vie privée est offerte par le Privacy and Big Data Institute de l'Université Ryerson et n'est pas associée au commissaire à l'information et à la protection de la vie privée de l'Ontario, ni synonyme de conformité avec les lois sur la protection de la vie privée de l'Ontario.

www.deloitte.ca

Conçu et produit par le Service de conception graphique de Deloitte, Canada. 15-2971H