Spécialiste de la protection des données/agent de la protection de la vie privée

Cadre de référence de la NICE	Supervision et gouvernance, OV-LGA-002, agent de protection de la vie privée/gestionnaire du respect de la vie privée
Description fonctionnelle	Le titulaire élabore, met en œuvre, conseille et administre le programme de respect de la vie privée qui soutient les exigences de protection des renseignements personnels.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou un mauvais jugement peuvent entraîner une compromission ou une violation des renseignements personnels, ce qui outre les conséquences et la responsabilité individuelles potentielles, peut entraîner des amendes importantes pour la violation, ainsi qu'une perte de réputation et de confiance.
Parcours de perfectionnement	Ce rôle peut être soutenu par des voies techniques ou non techniques qui mènent à un rôle de premier échelon lié à la gestion de la vie privée/des données sensibles et à la progression vers le niveau de conseiller en politique. Les personnes peuvent se spécialiser davantage dans la sécurité des données ou comme analyste des politiques ou conseiller principal.
Autres titres	▪ Agent de la protection de la vie privée ▪ Agent/gestionnaire du respect de la vie privée
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 416X – Chercheurs, experts-conseils/expertes-conseils et agents/agentes des politiques et des programmes (en fonction du contexte)
Tâches	▪ Interpréter et appliquer les lois, règlements, politiques, normes ou procédures à des questions relatives à la protection de la vie privée ▪ Mener des évaluations de l'impact périodiques et des activités de contrôle de conformité continues pour repérer les lacunes en matière de conformité ou les domaines à risque afin de garantir que les préoccupations, les exigences et les responsabilités en matière de protection de la vie privée sont traitées ▪ Mettre en place et maintenir un mécanisme de suivi de l'accès aux renseignements dans le cadre de l'organisation et conformément à la loi, afin de permettre au personnel qualifié d'examiner ou de recevoir ces renseignements ▪ Établir et mettre en œuvre un programme d'audit interne sur la protection de la vie privée, et préparer des rapports d'audit qui tirent des conclusions techniques et procédurales, déterminent les violations de la vie privée, et recommandent des solutions correctives ▪ Fournir des conseils et des orientations sur les lois, les règlements, les politiques, les normes ou les procédures à la direction, au personnel ou aux principaux services ▪ Veiller au respect des lois, règlements et politiques en matière de vie privée et de cybersécurité, et à l'application cohérente des sanctions en cas de non-respect des mesures énoncées pour l'ensemble du personnel de l'organisation ▪ Lancer, faciliter et promouvoir des activités de sensibilisation à la protection de la vie privée au sein de l'organisation, notamment la collecte, l'utilisation et le partage des renseignements ▪ Suivre les progrès des technologies renforçant la protection de la vie privée et veiller à ce que l'utilisation des technologies soit conforme

<table>
<tr><td></td><td colspan="2">aux exigences en matière de respect de la vie privée et de cybersécurité, y compris la collecte, l’utilisation et la divulgation de renseignements
▪ Examiner les plans et projets de sécurité des réseaux de l’organisation pour s’assurer qu’ils sont conformes aux objectifs et politiques en matière de protection de la vie privée et de cybersécurité
▪ Collaborer avec le conseil juridique et la direction pour s’assurer que l’organisation dispose d’un consentement approprié en matière de vie privée et de confidentialité, que les formulaires d’autorisation et les documents pertinents sont conformes aux pratiques et exigences juridiques
▪ Élaborer, fournir et superviser le matériel de formation et les activités de sensibilisation à la protection de la vie privée</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Études postsecondaires dans un domaine applicable (par exemple : administration des affaires, droit, sciences politiques, sciences sociales ou domaine équivalent)</td></tr>
<tr><td>Formation</td><td>Formation spécialisée sur la confidentialité et la sécurité des données, les bases de la cybersécurité, l’analyse des répercussions sur la vie privée, la législation relative à la protection de la vie privée et la conformité</td></tr>
<tr><td>Expérience professionnelle</td><td>Formation et expérience antérieures (2 à 3 ans) dans un rôle d’analyse des politiques liées à la sécurité ou à la vie privée, généralement requises pour un rôle de premier échelon</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Législation et politiques en matière de vie privée et d’information
▪ Exigences de conformité
▪ Mécanismes et modèles de rapports
▪ Évaluations des répercussions sur la vie privée et énoncés de sensibilité
▪ Évaluation de la menace et des risques
▪ Exigences en matière de données et de renseignements
▪ Outils et méthodologies d’évaluation de la protection de la vie privée</td></tr>
<tr><td>Compétences</td><td colspan="2">Les CCH s’appliquent au niveau de base :
☐ Connaissance pratique des principes et des éléments de la cybersécurité
☐ Connaissances techniques permettant de comprendre la sécurité et l’intégrité des données, les exigences de sécurité et la conception fonctionnelle et technique des réseaux et des systèmes, ainsi que les solutions de cybersécurité
☐ Conceptions et fonctions de sécurité des données, méthodologies d’analyse, essais et protocoles
☐ Gestion, mesures et suivi du programme de cybersécurité

Les CCH sont appliquées à un niveau avancé :
☐ Évaluation de la menace et des risques (axée sur la protection de la vie privée/la sécurité des données)
☐ Lois, règlements, politiques et procédures nationales et internationales
☐ Politiques, procédures et réglementations en matière de sécurité de l’information</td></tr>
</table>

	☐ Incidences spécifiques des lacunes et des failles de la cybersécurité ☐ Suivi des progrès des lois et des politiques en matière de protection de la vie privée ☐ Évaluations des répercussions sur la vie privée ☐ Déclarations de confidentialité fondées sur les lois et règlements ☐ Signalement des infractions
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités dans la protection des données sensibles et la réponse aux violations potentielles et le signalement de ces dernières. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment les outils seront intégrés à la protection des renseignements personnels au sein de l'organisation et comment cela doit se traduire en politiques, procédures et pratiques. ▪ L'utilisation accrue des outils automatisés par les acteurs de menace remettra probablement en question les technologies et les ressources existantes destinées à gérer la protection des renseignements personnels. En conséquence, des outils, des processus ou des formations supplémentaires seront nécessaires pour garder une longueur d'avance sur les menaces. ▪ Des mécanismes visant à soutenir le niveau requis de confiance et de risque organisationnel devront être mis en place pour soutenir le suivi et la communication des résultats des outils automatisés. Par conséquent, il faudra comprendre les risques organisationnels posés pour les renseignements personnels/données, les mesures de sécurité et les politiques, processus ou procédures à mettre en place. ▪ L'émergence et l'utilisation des technologies quantiques par les acteurs de menace vont fondamentalement modifier la sécurité du chiffrement. Le chiffrement utilisé pour protéger les renseignements personnels exigera des connaissances et des compétences pour garantir que les renseignements personnels restent protégés contre la menace quantique.