Analyse comparative du cadre de protection de la vie privée des entreprises : points saillants du rapport annuel 2019 de l'IAPP et d'EY

03 octobre 2019

L'IAPP et EY ont publié la semaine dernière leur cinquième rapport annuel sur la gouvernance de la protection de la vie privée (le « Rapport »).

Les auteurs ont interrogé des sociétés de partout dans le monde pour connaître les tendances du domaine. Ils ont cherché à comprendre la structure des programmes de protection de la vie privée (notamment sur le plan du budget, de l'affectation de personnel et du perfectionnement professionnel), à mesurer les efforts de conformité en la matière (en particulier, cette année, la conformité au Règlement général sur la protection des données [RGPD] de l'Union européenne) et à décrire l'évolution récente des activités quotidiennes menées par les professionnels de la protection de la vie privée et des données.

Bien que les sociétés sondées proviennent des quatre coins du globe, bon nombre des réponses et des tendances peuvent présenter un intérêt pour les entreprises canadiennes qui sont en train d'analyser et d'actualiser leur cadre de gouvernance de la protection de la vie privée. Nous avons résumé dans le présent bulletin les points suivants du Rapport : le rôle du conseil d'administration, les types de dossiers communiqués au conseil, la fonction et les responsabilités pertinentes au sein des entreprises, la gestion des fournisseurs indépendants et les types de demandes de personne concernée que les organisations reçoivent.

Répondants

Les répondants sont des professionnels de la protection de la vie privée (délégués à la protection des données mandatés au sens du RGPD, responsables, directeurs ou analystes de la protection de la vie privée, etc.) de plusieurs territoires, qui travaillent dans divers secteurs pour des entreprises de tailles variées.

- **Territoire :** Les répondants viennent du Canada (6 %), des États-Unis (39 %), de l'Union européenne (33 %), du Royaume-Uni (13 %) et d'autres pays (7 %).
- **Secteur d'activité :** Les répondants travaillent dans divers secteurs : technologies (22 %), services financiers (22 %), soins de santé et produits

pharmaceutiques (9 %), fonction publique (5 %), services-conseils (3 %) et autres (39 %).
- **Taille de l'organisation :** La plupart des répondants travaillent pour une organisation comptant un nombre moyen ou élevé d'employés : 1 000 à 4 999 (21 %), 5 000 à 24 999 (24 %), 25 000 à 74 999 (11 %) et plus de 75 000 (12 %).

Fait intéressant, le Rapport fait état d'une augmentation du nombre de répondants qui sont avocats – en particulier avocats généraux –, ce qui pourrait signifier la promotion de professionnels du domaine au poste d'avocat général ou (plus vraisemblablement) l'adoption de nouvelles responsabilités par des avocats généraux qui consacraient naguère moins d'attention aux questions de protection de la vie privée.

Rôle du conseil

Ces dernières années, les conseils d'administration ont commencé à reconnaître l'importance des risques juridiques et d'atteinte à la réputation posés par les questions de protection de la vie privée. Le Rapport souligne que même si les conseils ont toujours joué un rôle majeur en matière de gouvernance de la protection de la vie privée, ce rôle a été rehaussé récemment par l'ordonnance de règlement rendue par la FTC à l'endroit de Facebook dans l'affaire Cambridge Analytica. Dans ce dossier, en plus d'imposer à Facebook une amende de 5 milliards de dollars, la FTC a sommé le conseil de la société de créer un comité spécial indépendant chargé d'encadrer le programme de protection de la vie privée de l'entreprise et d'en assumer la responsabilité. La SEC a elle aussi réprimandé Facebook pour avoir omis de révéler à ses investisseurs que ses clients risquaient de subir des atteintes à la vie privée, et elle lui a imposé une amende de 100 millions de dollars. Le Rapport indique ce qui suit :

« Bien que ces sommes soient relativement peu élevées en regard du chiffre d'affaires de plus de 50 milliards de dollars de la société, elles sont néanmoins impressionnantes et devraient attirer l'attention sur la protection de la vie privée aux échelons les plus élevés des entreprises. »

Communications au conseil

Il est intéressant pour les entreprises canadiennes de savoir de qui relèvent les responsables de la protection de la vie privée au sein des organisations. D'après le Rapport, les responsables sont plus susceptibles de relever du conseil s'ils sont des délégués à la protection des données (67 %), si le chiffre d'affaires de la société est inférieur à 100 millions de dollars (39 %), si le siège social se situe dans l'Union européenne (35 %) ou si la société compte moins de 5 000 employés (29 %).

Le Rapport indique qu'aux États-Unis, le responsable de la protection de la vie privée relève du conseil d'administration dans 10 % des cas, contre 35 % dans l'Union européenne. Dans les autres cas, le responsable relève de l'avocat général (35 % du temps aux É.-U. et 18 % dans l'UE) ou du chef de la direction (16 % du temps aux É.-U. et 25 % dans l'UE).

Le Rapport nous apprend en outre que les dossiers communiqués au conseil se rapportent habituellement à des atteintes à la protection des données (68 % du temps) ou à la conformité au RGPD (64 % du temps). Les autres dossiers communiqués au

conseil relativement à la protection de la vie privée concernent les indicateurs de rendement clés des programmes (58 %), l'avancement des initiatives (47 %), les litiges (38 %), le nombre de plaintes (36 %), des incidents particuliers (36 %), l'évolution de la conformité (26 %), les plans et stratégies élaborés en prévision du *California Consumer Privacy Act* (CCPA) (23 %), les données budgétaires (22 %), l'information concernant les certifications et attestations (21 %), les incidences importantes du CCPA (17 %) ou les questions d'éthique des données (15 %).

Fonction et responsabilités

La fonction de protection de la vie privée ne s'exerce pas au même endroit dans toutes les organisations. D'après le Rapport, la moitié des équipes de protection de la vie privée sont intégrées au service juridique, tandis que les autres font partie du service de conformité réglementaire (22 %), de protection de la vie privée et des données (17 %), de la sécurité de l'information (14 %), de déontologie (10 %) ou des technologies de l'information (8 %), ou encore d'un autre service (22 %).

Quant aux types de responsabilités des répondants selon le territoire (États-Unis et Union européenne), voici ce qu'indique le Rapport : conformité au RGPD (72 % aux É.-U. c. 97 % dans l'UE), suivi de l'évolution législative (92 % aux É.-U. c. 80 % dans l'UE), gestion des fournisseurs de service (83 % aux É.-U. c. 64 % dans l'UE), prise de décision éthique concernant l'emploi de données (72 % aux É.-U. c. 56 % dans l'UE), abonnements et publications (60 % aux É.-U. c. 33 % dans l'UE), préparation en vue du CCPA (80 % aux É.-U. c. 17 % dans l'UE), communication avec les consommateurs et réparation (47 % aux É.-U. c. 33 % dans l'UE) et certification et homologation Web (38 % aux É.-U. c. 21 % dans l'UE).

Le Rapport mentionne que 33 % des répondants sont très satisfaits de leur emploi et que 49 % en sont satisfaits. De plus, bon nombre d'entre eux s'attendent à une promotion. Leurs principales fonctions sont les suivantes : gestion des politiques, des procédures et de la gouvernance; conscientisation et formation au sein de l'entreprise; résolution des problèmes concernant les produits et services; suivi de l'évolution législative; évaluation des facteurs relatifs à la vie privée (EFVP); intervention en cas d'incident; communications; conformité au RGPD; conception et mise en œuvre des contrôles; intégration de la protection de la vie privée au développement des produits; enquêtes; et recensement et mappage des données.

Gestion des fournisseurs indépendants

En général, les organisations canadiennes demeurent responsables des renseignements personnels transmis à un fournisseur indépendant aux fins de traitement. Elles doivent donc prendre des mesures pour continuer de protéger adéquatement ces renseignements pendant qu'ils sont entre les mains d'un tiers. Or, les organisations ont souvent du mal à déterminer les types de mesures à prendre.

Sur la question de la gestion des fournisseurs indépendants, le Rapport indique ce qui suit :

- 94 % des répondants « s'en remettent aux garanties du contrat » pour s'assurer que les fournisseurs respectent leurs obligations concernant le RGPD, la

protection de la vie privée et la sécurité, et 88 % d'entre eux affirment que leur premier critère de sélection d'un fournisseur est l'existence de garanties relatives à la protection des données et à la sécurité de l'information.
- 57 % des répondants font remplir un questionnaire portant sur les pratiques de traitement des données.
- 48 % des répondants exigent une attestation ou une certification externe. ISO 27001 demeure le premier choix (44 %). Les autres certifications nommées sont le Bouclier de protection des données UE-États-Unis (23 %), PCI (25 %), SOC 2 Privacy (27 %), ISO 27002 (16 %), SOC 2 HIPAA (10 %), ISO 27018 (9 %), TrustArc (anciennement TRUSTe) (3 %) et CSA STAR (3 %).
- 26 % des répondants affirment mener des audits dans les bureaux de leurs fournisseurs afin de vérifier leurs programmes de traitement des données.

Parmi les autres points importants, citons la vérification diligente du fournisseur et la limitation des renseignements personnels transmis à ce dernier.

Types de demandes de personne concernée reçus

Les organisations constatent souvent que les incidents et les scandales très médiatisés relatifs aux renseignements personnels entraînent une hausse des demandes de personne concernée.

Selon le Rapport, la plupart des demandes faites par des particuliers au cours de l'année précédente étaient des demandes d'accès (68 %), suivies par les demandes de suppression (60 %), de rectification (32 %), de restriction ou de cessation du traitement (31 %) et de portabilité des données (14 %).

Les types de demandes de personne concernée les plus complexes sont ceux qui concernent la localisation de renseignements personnels non structurés (56 %), la surveillance des pratiques de tiers en matière de protection des données ou de la vie privée (36 %), la minimisation des données (28 %), la création d'un outil de retrait centralisé et convivial (25 %), l'anonymisation (20 %), la nécessité de modifier les avis relatifs à la vie privée (9 %), les dispositifs interconnectés (9 %), la modification des politiques relatives aux témoins de connexion (4 %) ou l'intelligence artificielle (4 %).

Conclusion

Les organisations canadiennes peuvent se servir du Rapport comme d'un outil d'analyse comparative pour mettre en place un programme de protection de la vie privée et y associer des pratiques exemplaires. Elles peuvent également y trouver un aperçu de ce qui les attend si le Canada adopte une loi plus stricte sur la gouvernance de la protection de la vie privée, inspirée du RGPD de l'Union européenne.

Le Rapport traite également du salaire des professionnels de la protection de la vie privée et des budgets que les organisations consacrent à cette question. À propos, le Rapport souligne que les entreprises augmentent leurs dépenses à cet égard et que 55 % des répondants s'attendent à une hausse de leur budget au cours des douze prochains mois. Cela témoigne de la complexité croissante du contexte mondial de la protection de la vie privée à l'heure où les lois sur cet enjeu voient le jour à un rythme accéléré.

Par

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels

---

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

Les présents renseignements sont de nature générale et ne sauraient constituer un avis juridique, ni un énoncé complet de la législation pertinente, ni un avis sur un quelconque sujet. Personne ne devrait agir ou s'abstenir d'agir sur la foi de ceux-ci sans procéder à un examen approfondi du droit après avoir soupesé les faits d'une situation précise. Nous vous recommandons de consulter votre conseiller juridique si vous avez des questions ou des préoccupations particulières. BLG ne garantit aucunement que la teneur de cette publication est exacte, à jour ou complète. Aucune partie de cette publication ne peut être reproduite sans l'autorisation écrite de Borden Ladner Gervais S.E.N.C.R.L., S.R.L. Si BLG vous a envoyé cette publication et que vous ne souhaitez plus la recevoir, vous pouvez demander à faire supprimer vos coordonnées de nos listes d'envoi en communiquant avec nous par courriel à desabonnement@blg.com ou en modifiant vos préférences d'abonnement dans blg.com/fr/about-us/subscribe. Si vous pensez avoir reçu le présent message par erreur, veuillez nous écrire à communications@blg.com. Pour consulter la politique de confidentialité de BLG relativement aux publications, rendez-vous sur blg.com/fr/ProtectionDesRenseignementsPersonnels.

© 2025 Borden Ladner Gervais S.E.N.C.R.L., S.R.L. Borden Ladner Gervais est une société à responsabilité limitée de l'Ontario.