Perspectives ESG

Février 2018

Règlement général sur la protection des données (RGPD) – Quelle incidence sur les sociétés?

David Sneyd
Associé principal
Gouvernance et investissement durable

Les points de vue et opinions sont ceux de BMO Gestion mondiale d'actifs et ne doivent pas être considérés comme des recommandations ou des sollicitations d'achat ou de vente de sociétés qui auraient pu être mentionnées.

Les renseignements, opinions, estimations et prévisions qui figurent dans le présent document sont tirés de sources considérées comme fiables et peuvent changer à tout moment.

Sommaire

- Le Règlement général sur la protection des données (RGPD), qui entrera en vigueur le 25 mai 2018, vise à renforcer la cybersécurité, à accroître la protection des données à caractère personnel des citoyens européens et à unifier la législation en la matière au sein de l'Union européenne. Il remplace la directive en matière de protection des données personnelles (1995). Contrairement à la directive précédente, vu sa portée extraterritoriale, le nouveau règlement devient la première législation internationale en matière de protection des données.
- Depuis 1995, la technologie a énormément progressé et touche toutes les sphères de nos vies, ce qui affecte la façon dont les données sont recueillies, traitées et stockées. En parallèle, les entreprises d'aujourd'hui sont plus que jamais dépendantes de l'utilisation des données dans tous les aspects de leurs activités.
- Dans ce contexte, le Règlement général sur la protection des données vise à enchâsser le droit des Européens à la vie privée en leur donnant la possibilité de choisir à qui ils confient leurs données personnelles, l'utilisation qui en sera faite et les mesures de sécurité qui en assureront la protection. À cela s'ajoute le contexte d'augmentation des menaces d'attaques informatiques, car les renseignements personnels sont précieux aux yeux des criminels.
- Même si le Règlement général sur la protection des données profitera aux sociétés en simplifiant le cadre réglementaire de la protection des données, nous prévoyons qu'il touchera un éventail plus vaste de sociétés internationales que la directive actuelle, ce qui augmentera les frais de conformité et exigera une vaste réforme de la gouvernance et de la culture organisationnelle pour faire de la protection des données et du respect de la vie privée la priorité. Peu de sociétés sont bien préparées, mais nous croyons qu'un délai de grâce accordé par les organismes de réglementation permettra de réduire le risque lié à la conformité.

Nous joindre

Secteur institutionnel :

1.844.855.7034

bmoam.institutional@bmo.com

bmo.com/institutions

Contexte

Au cours des deux dernières décennies, des changements spectaculaires ont modifié la façon dont la société utilise la technologie et l'entreprise moyenne n'a jamais été aussi dépendante du traitement de données. Non seulement cela est-il vrai de la façon dont les sociétés exploitent leur entreprise, mais la technologie constitue l'essentiel de l'offre de produits de certaines des entreprises actuelles les plus prospères. Pendant ce temps, aussi bien dans les marchés développés qu'émergents, les consommateurs intègrent les services numériques à leur vie à un rythme sans précédent et, par conséquent, les données générées proviennent maintenant en grande partie de la sphère privée et ont de plus en plus de valeur.

Presque inévitablement, la situation a entraîné une augmentation similaire de la cybercriminalité, car les pirates informatiques cherchent à exploiter les renseignements personnels, que les entreprises rendent disponibles en ligne malgré elles, par l'intermédiaire de leurs systèmes informatiques par faute de mesures de protection des données adéquates visant à prévenir les intrusions. De plus, comme les sociétés dépendent de la technologie dans leurs activités quotidiennes, les risques de perturbation augmentent puisque les cybercriminels cherchent à profiter des sociétés en les prenant en otage. Enfin, le piratage par les États-nations signifie que les sociétés considérées comme faisant partie des infrastructures essentielles d'un pays ou étant d'une importance stratégique, comme les services aux collectivités, les banques et les télécommunications, sont particulièrement à risque.

« Les risques liés à la cybersécurité augmentent également, tant dans leur prévalence que dans leur potentiel perturbateur. Les attaques contre les entreprises ont presque doublé en cinq ans, et des incidents qui auraient été considérés comme extraordinaires deviennent de plus en plus courants. »

Rapport sur les risques mondiaux (2018), Forum économique mondial

C'est dans ce contexte que l'Union européenne a modifié les règles en matière de protection des données qu'elle avait mises en place en 1995. À l'origine, ce processus visait à enchâsser dans la réglementation le droit à la vie privée en tant que droit humain universel des citoyens de l'Union européenne, mais pendant la rédaction, le mandat a été élargi pour inclure la sécurité des données devant la menace croissante qui s'est matérialisée entre-temps.

Même si le nouveau Règlement général sur la protection des données a une portée plus étendue et plus restrictive que la législation précédente, l'Union européenne le dit plus avantageux que contraignant pour les sociétés. Cela est principalement dû au fait qu'il simplifie le processus de conformité en éliminant les nombreuses règles conflictuelles de protection des données actuellement en vigueur dans chaque état membre. Aussi, en créant un « guichet unique » pour les entreprises, celles-ci n'auront affaire qu'à une seule autorité locale de contrôle, sachant qu'une entente aura une incidence sur toutes les autres. Vu sa portée territoriale étendue (détails ci-dessous), il propose également une plus grande homogénéité dans le traitement des renseignements personnels entre les sociétés de l'Union européenne et les sociétés étrangères.

« Ces nouvelles règles paneuropéennes sont une bonne chose pour les citoyens et pour les entreprises. Ceux-ci bénéficieront de règles claires, adaptées à l'ère numérique, qui leur confèrent une protection forte tout en créant des opportunités et en favorisant l'innovation sur un marché unique numérique européen. »

Věra Jourová, Commissaire européenne pour la justice aux consommateurs et à l'égalité des genres

Cela étant dit, malgré ces avantages, la conformité au Règlement général sur la protection des données demeure un important défi pour les sociétés. Dans le présent point de vue, nous examinons les nouveaux éléments de cette nouvelle réglementation et leur incidence pour les sociétés

Différences entre le RGPD et la réglementation actuelle en matière de protection des données

- **Application potentielle à l'ensemble des sociétés du monde entier :** contrairement à la réglementation quelque peu ambiguë qui l'a précédé, le RGPD ne s'intéresse pas à l'emplacement des sociétés qui utilisent les données, mais plutôt à l'endroit où les clients réels et potentiels sont susceptibles de se trouver. La nouvelle réglementation s'appliquera à toute société qui traite les données personnelles d'un citoyen de l'Union européenne, que le traitement de données se fasse ou non dans l'Union européenne. Il s'agit de la première législation mondiale en matière de protection des données.
- **Définition élargie de données personnelles :** le terme « données personnelles » est défini de façon assez générale dans la législation actuelle, mais sera précisé dans le RGPD de manière à inclure toute donnée permettant d'identifier un individu. Cette définition comprend des renseignements qui peuvent sembler très génériques ou banals pris isolément, mais qui peuvent devenir uniques et personnels pris collectivement. Les nouveaux types de renseignements comprennent l'identité géographique, physiologique, générique, économique, culturelle et sociale d'un individu. En plus, dans certaines circonstances, les données personnelles comprendront désormais les données d'accès en ligne, comme les adresses IP et les codes d'accès aux appareils mobiles.
- **Sanctions plus importantes :** Tles infractions les plus graves du RGPD, comme un consentement incomplet du client au traitement de ses données ou des fuites de données causées par des mesures de protection des données

inadéquates, sont passibles d'amendes pouvant aller jusqu'à 4 % du chiffre d'affaires global annuel ou 30 millions de dollars1, selon le plus élevé des montants. Ces amendes sont nettement supérieures à celles autorisées en vertu de la législation en vigueur, soit 872 000 $1 au Royaume-Uni ou 1 374 000 $ aux Pays-Bas. Globalement, en imposant une amende allant jusqu'à 2 % du revenu global annuel pour des infractions mineures, comme l'absence de dossiers en règle ou l'omission d'aviser la personne concernée au sujet d'une infraction impliquant ses données, la nouvelle réglementation met de l'avant une approche à plusieurs niveaux à l'égard des amendes.

- **Moins de pouvoir aux sociétés et plus de droits aux personnes concernées :** contrairement aux dispositions actuelles en vertu desquelles les entreprises doivent obtenir le consentement des clients pour utiliser leurs données personnelles (consentement implicite avec option de retrait), les clients devront désormais donner explicitement leur consentement à l'utilisation de leurs données à des fins précises. Les entreprises ne seront plus autorisées à utiliser de longues modalités illisibles, truffées de jargon juridique pour obtenir le consentement. Qui plus est, la nouvelle réglementation introduit le « droit à l'oubli numérique » qui permet aux personnes, de manière simple et gratuite, de savoir quelles données les concernant sont conservées et d'interdire, de façon générale, l'utilisation de renseignements personnels à d'autres fins que celles auxquelles elles ont consenti au départ.
- **Nomination d'un délégué à la protection des données (DPD):** les entreprises dont les activités exigent un suivi systématique des personnes concernées à une grande échelle ou qui traitent des catégories particulières de données à grande échelle devront désigner un délégué à la protection des données. Le délégué à la protection des données doit avoir une connaissance approfondie de la législation en matière de protection des données, relever du plus haut niveau de la direction et peut être un salarié ou un consultant externe.
- **Nouvelle exigence relative à la notification des infractions à la protection des données :** les sociétés ne peuvent plus dissimuler les infractions à la protection des données et informer les clients ou le marché quand bon leur semble. Désormais, elles devront informer les autorités de contrôle et les personnes concernées dans les 72 heures après avoir pris connaissance de l'infraction qui « engendre un risque pour les droits et libertés des personnes physiques ». Cette exigence s'applique en particulier, lorsque l'atteinte peut (sans l'avoir fait) donner lieu, entre autres, à une discrimination, à un vol ou une usurpation d'identité, à une perte financière ou à une atteinte à la réputation.
- **Responsabilité de l'entreprise étendue aux tiers fournisseurs :** Aux termes de la réglementation actuelle, la responsabilité de préserver les données et de protéger leur caractère confidentiel revient au « contrôleur des données », c'est-à-dire la société qui souhaite utiliser les données et qui décide de leur traitement. À titre comparatif, le « responsable du traitement des données » traite les données pour le compte de l'entreprise. Il peut s'agir, par exemple, d'un fournisseur de logiciels tiers ou d'un fournisseur de service nuagique. En ce moment, les contrôleurs de données assument entièrement la protection des données, mais cette responsabilité sera désormais, aux termes du RGPD, étendue à l'ensemble des organisations tierces qui manipulent les données à caractère personnel.
- **Mesures prises par toute autorité européenne chargée de la protection des données :** prenons l'exemple de l'Irlande, où les entreprises américaines ont pris l'habitude d'installer leurs contrôleurs des données parce que l'autorité locale chargée de la protection des données est passablement indulgente. Aux termes du RGPD, toute autorité européenne pourra désormais prendre des mesures contre une organisation. Pour les sociétés, l'avantage est de faire affaire avec un seul organisme de réglementation puisque la conformité et les accords auprès de celui ci s'appliquent à tous les autres. Cependant, elles sont soumises à un régime d'application de la réglementation plus sévère, car les personnes concernées par les données dans un pays membre peuvent soumettre leurs préoccupations à l'organisme de réglementation local.
- **Exigence de protection des données proactive et volontaire par les sociétés :** la nouvelle législation imposera le principe de « respect de la vie privée assuré dès la conception », selon lequel les fonctions de sécurité de l'information sont intégrées dans la conception des systèmes, plutôt que d'être ajoutées ou conçues après coup. Avant le début d'un projet, les sociétés devront procéder à une évaluation des facteurs relatifs à la vie privée (EFVP), qui décrit la nature des points de données à recueillir ainsi que les méthodes employées pour les conserver, les protéger et les communiquer. Le délégué à la protection des données doit veiller à ce que l'évaluation des facteurs relatifs à la vie privée soit prise en compte dans la conception et l'utilisation des systèmes.

Quelles sont les conséquences pour les sociétés?

Comme les entreprises d'aujourd'hui sont les premières à dépendre autant du traitement des données, la majorité d'entre elles devront se soumettre aux exigences du RGPD. Nous pouvons résumer les principales répercussions de la nouvelle législation en matière de protection des données par les trois principaux thèmes suivants :

- **Portée élargie de la conformité des données**
  À l'heure actuelle, les sociétés établies hors de l'Union européenne qui traitent les données de leurs citoyens sur leur territoire ne sont pas tenues de respecter la réglementation de l'Union européenne en matière de protection des données. Les critères d'admissibilité du RGPD ont été élargis de manière à inclure non seulement le mode de traitement des données, mais les personnes visées par celui-ci, c'est-à-dire qu'une grande variété de sociétés établies hors de l'Union européenne seront maintenant assujetties à cette nouvelle norme beaucoup plus sévère que celles en vigueur ailleurs dans le monde. Par exemple, une société chinoise de livraison de fleurs qui reçoit des commandes de citoyens de l'Union européenne qui sont entièrement traitées en Chine n'est actuellement pas visée par la réglementation, mais le sera aux termes du RGPD.

[1] Source du taux de change : BMO Gestion mondiale d'actifs, au 31 janvier 2018

Le champ d'application de la réglementation a été élargi à un plus large éventail d'utilisations de données, qu'il s'agisse de données recueillies directement, par exemple, à partir d'algorithmes de profilage ou de données de localisation ou d'accès en ligne répondant à une définition élargie des données personnelles. Toute entreprise qui utilise le profilage de ses clients sera désormais assujettie à des contrôles procéduraux plus rigoureux, ce qui réduira l'efficacité de ces processus. En outre, comme les individus pourront se soustraire à ces processus complètement, les sociétés devront prévoir un nouveau processus pour répondre à ces demandes.

Enfin, aux termes de la nouvelle réglementation en matière de protection des données, la responsabilité revient autant aux contrôleurs des données (c.-à-d. les sociétés qui utilisent les données pour les besoins de leur entreprise) qu'aux responsables du traitement des données. Vu la tendance récente de recourir à des services infonuagiques et à l'externalisation des infrastructures technologiques proposées à des tiers, les sociétés qui offrent ces services devront désormais assumer un risque réglementaire élevé au nom de tous leurs clients. Aussi, les contrôleurs de données devront s'assurer que chaque personne qui interagit avec les données de ses clients pour son compte, qu'il s'agisse du transfert, de la conservation ou du traitement, les gère de façon appropriée et sécuritaire. Voilà qui introduit la notion de gestion de la chaîne d'approvisionnement des données, similaire à la chaîne d'approvisionnement ordinaire, qui repose sur des procédures de diligence raisonnable visant à s'assurer que tous les intervenants sont rigoureux et ne les exposent pas indûment à des risques de conformité.

- **Augmentation des coûts de conformité des données**
  Les frais les plus évidents découlant du RGPD sont les montants considérablement plus élevés des sanctions en cas d'infraction, qui peuvent aller jusqu'à 4 % du chiffre d'affaires global annuel ou 30 millions de dollars , selon le plus élevé des montants. Vu l'élargissement du champ d'application territoriale du RGPD, on peut s'attendre à ce que les autorités chargées de la protection des données de l'Union européenne imposent des sanctions par l'entremise des autorités locales, y compris les pays avec lesquels elle coopère déjà.

  C'est ce qui s'est produit en 2016 lorsque la société de télécommunications TalkTalk du Royaume-Uni s'est vu imposer une sanction de 400 000 livres sterling pour l'inefficacité de ses mesures de contrôles en matière de cybersécurité qui avait causé l'année précédente la fuite des données personnelles de 21 000 clients. Cette sanction frôlait le maximum autorisé en vertu des lois du Royaume Uni alors en vigueur en matière de protection des données. Aux termes du RGPD, cette amende aurait pu aller jusqu'à 72 millions de livres sterling, soit 4 % du chiffre d'affaires global annuel pour cette année-là. Ici, le risque ne peut qu'être aggravé par la difficulté accrue de se conformer au RGPD et les amendes considérables imposées à défaut de le faire

« L'entreprise qui est incapable de démontrer que la protection efficace des données est la pierre angulaire de ses pratiques s'expose à des sanctions ou à toute autre mesure d'application du règlement qui peuvent causer du tort à ses finances ou à sa réputation. »

Elizabeth Denham, Commissaire de l'information britannique

Parallèlement à cela, les nouvelles exigences du RGPD entraînent des coûts élevés liés à la conformité. Les sociétés doivent mettre à niveau les systèmes et les procédures qu'elles utilisent pour traiter les données afin de satisfaire les nouvelles exigences, y compris les procédures d'audit pour vérifier que le consentement a été obtenu de manière appropriée ou pour répondre aux demandes des personnes qui souhaitent savoir quels renseignements les concernant sont détenus ou exercer leur droit à l'oubli numérique. Les sociétés qui n'ont pas déjà investi dans la gouvernance des données ou dans des procédures efficaces de traitement des données devront investir des montants considérables pour se conformer aux nouvelles normes. Qui plus est, l'affectation de ressources au traitement de ces demandes qui feront désormais partie des processus habituels entraînera un ralentissement de la productivité.

- **Incidence sur les revenus provenant des produits et services reposant sur les données**
  L'autre coût important est la perte de revenu provenant des pratiques commerciales actuelles. Pendant des années, les sociétés ont utilisé les données des clients sans aucune restriction en obtenant le consentement implicite des utilisateurs, qui pouvaient choisir de le refuser.

« Plus de 80 % des entreprises visées par le Règlement général sur la protection des données ont déclaré devoir adapter leurs produits pour se conformer au règlement. »

Rapport annuel de gouvernance en matière de protection de la vie privée de l'Association internationale des professionnels de la protection de la vie privée (IAPP) et d'Ernst & Young (2017)

[1] Source du taux de change : BMO Gestion mondiale d'actifs, au 31 janvier 2018.

Certains secteurs, comme le commerce de détail, ont développé une dépendance envers les données pour structurer l'expérience en ligne de leurs clients en fonction des données personnelles et de l'historique d'achat de ceux-ci. Aux termes du RGPD, les individus n'auront pas seulement à donner le consentement à la collecte de leurs données, mais également à l'utilisation qui en sera faite. Considérant que les consommateurs sont de plus en plus conscients de l'importance de protéger la confidentialité de leurs données personnelles, on s'attend à ce qu'ils soient nombreux à refuser aux détaillants le consentement qui permettrait à ces derniers d'optimiser les achats des clients selon leurs pratiques commerciales actuelles. À titre d'exemple supplémentaire, un sondage de 2017 réalisé par PageFair a révélé que les personnes sondées étaient peu nombreuses (seulement 3 %) à croire que l'utilisateur moyen consentirait explicitement à la surveillance (par n'importe qui, sur n'importe quel site) de ses activités sur le web à des fins publicitaires. Dans la législation actuelle, cette pratique est permise sans consentement et est largement utilisée.

- **Réforme de la gouvernance et de la culture organisationnelle en matière de conformité des données**
  Selon un principe fondamental de la nouvelle législation, les sociétés devront s'investir à intégrer un volet confidentialité à leur culture organisationnelle. Toute tentative de changer la culture d'entreprise doit nécessairement passer par des personnes en position d'autorité qui donnent le ton aux niveaux supérieurs. Cependant, des données empiriques suggèrent que la prise en charge du problème par les niveaux hiérarchiques supérieurs pose un défi organisationnel, car la confidentialité et la sécurité des données ont toujours été perçues comme un problème opérationnel plutôt qu'une question d'ordre stratégique relevant du conseil d'administration.

"« Il ressort d'un sondage réalisé auprès d'environ 900 membres de l'Institut des administrateurs de sociétés… que près du tiers des administrateurs de sociétés n'ont pas entendu parler du RGPD, tandis que 40 % ne savent pas si leur société sera touchée par cette nouvelle réglementation. »

UK Institute of Directors, octobre 2017

En plus de cela, certaines sociétés pour qui le traitement des données est très complexe doivent désigner un délégué à la protection des données qui relève du plus haut niveau de la direction. Les sociétés qui n'ont pas déjà de procédures de gouvernance pour traiter les questions de confidentialité et de sécurité des données devront créer ce nouveau rôle et lui donner l'autorité interne et le lien hiérarchique nécessaires pour lui permettre de jouer son rôle efficacement.

Il en va de même pour ce qui est de mettre en place des procédures de signalement des infractions à la protection des données, que les sociétés doivent faire dans les 72 heures après avoir pris connaissance de l'infraction, conformément au RGPD. Les sociétés qui ont déjà établi une ligne de signalement et mis en place des procédures à cet égard auront un avantage; par exemple, certaines banques vont jusqu'à jouer à des jeux de cyberguerre pour assimiler le processus. Toutefois, les récents incidents concernant Equifax et Uber démontrent que dans les faits, certaines sociétés préfèrent mener une enquête approfondie qui peut durer plusieurs mois avant de communiquer l'incident à l'externe. Cette façon de faire ne sera plus permise par le nouveau Règlement général sur la protection des données. Les sociétés pour qui le concept est nouveau devront négocier une courbe d'apprentissage très prononcée.

Finalement, ce changement de culture devra se traduire dans le principe de « respect de la vie privée assuré dès la conception » du RGPD. Concrètement, les sociétés devront intégrer ces éléments dès le début dans leur planification stratégique ou processus de développement de produit plutôt que de les considérer comme un facteur après les faits.

Conclusions et prochaines étapes

Même si le RGPD offre aux sociétés internationales l'occasion de créer une relation simplifiée et plus productive avec les organismes de réglementation en matière de protection des données en Europe, il impose également des défis à relever dans un domaine de plus en plus pertinent pour les entreprises. Les législateurs de l'UE ont placé la barre haute en termes de réglementation mondiale sur la protection des données, ce qui entraînera des coûts considérables de mise en conformité et de maintien de la conformité. Parallèlement, nous considérons que les sociétés qui relèveront le défi et se conformeront aux exigences auront l'esprit tranquille, comprendront mieux les risques informatiques et tireront parti de la fidélité envers la marque en prenant au sérieux le droit des clients à la vie privée, autant d'atouts dont elles pourront faire un avantage concurrentiel.

Au début, la mise en œuvre du RGPD favorisera surtout les consommateurs au détriment des entreprises, mais pourra devenir à long terme un incitatif à faire preuve d'une plus grande transparence et à accroître la concurrence sur le marché. Les sociétés qui exercent leurs activités dans plusieurs territoires tireront également parti d'un processus de conformité simplifié. En adhérant à une norme de pratique aussi élevée en matière de gouvernance des données, les sociétés internationales sauront que leur conformité s'applique à l'ensemble de leurs activités dans le monde entier, ce qui leur évite de devoir jongler avec les nombreuses règles internationales actuellement en vigueur.

Il semblerait qu'une minorité de sociétés seront prêtes au moment de l'entrée en vigueur du RGPD le 25 mai 2018, mais les organismes de réglementation de la protection des données ont déclaré qu'ils ne feront pas de chasse aux sorcières ce jour-là, mais faciliteront plutôt la transition en accordant une période de grâce initiale. D'ici là, vu l'importance des changements à prévoir, certaines sociétés n'ayant pas pris au sérieux la protection des données jusqu'à ce jour n'auront pas assez de la période de grâce pour changer leurs pratiques et se conformer entièrement aux nouvelles règles.

Principales questions favorisant la mobilisation des sociétés :

- Votre conformité au RGPD sera-t-elle complète d'ici au 25 mai 2018?
- Sinon, que restera-t-il à faire? Quand aurez-vous terminé ce qu'il reste à faire??

Gouvernance et supervision :

- Comment le Conseil d'administration supervise-t-il les questions de protection des données et de cybersécurité?
- Le savoir-faire du conseil d'administration en matière de protection des données sera-t-il suffisant pour assurer une supervision efficace?
- Avez-vous nommé un délégué à la protection des données? De qui relève-t-il?
- Avez-vous mis en place une procédure de signalement en cas d'infraction? Avez-vous vérifié son efficacité?

Opérations – Produits :

- Prévoyez-vous que certaines gammes de produits seront affectées de manière négative par les nouvelles restrictions relatives à l'utilisation des données?
- Êtes-vous en mesure de répondre aux demandes des clients relatives à l'utilisation des données les concernant ou pour supprimer leurs données complètement?
- Avez-vous une politique de « respect de la vie privée assuré dès la conception »?

Cybersécurité:

- Qui est responsable de la cybersécurité? Fait-elle partie du système de gestion des risques de l'organisation?
- Avez-vous adopté des normes sectorielles de gestion du risque lié à la cybersécurité, comme la norme de gestion de la sécurité de l'information (ISO 27001)?
- Avez-vous soumis vos systèmes de sécurité des données

à des simulations de crise?

Quelles mesures de diligence avez-vous prises à l'égard des tiers responsables du traitement des données ou des fournisseurs de technologie?

Compte tenu des enjeux, la principale question qui se pose de notre part est de savoir comment les sociétés, en particulier leurs conseils d'administration, pourront surveiller efficacement la conformité au RGPD et l'application des procédures de protection des données. Plus précisément, chaque société doit prévoir des dispositions claires concernant l'intégration du nouveau rôle de délégué à la protection des données dans les rapports hiérarchiques de sa direction. D'autres exigences, comme l'inculcation d'une culture organisationnelle de protection des données et le signalement des infractions dans un délai de 72 heures, ont également une incidence immédiate de gouvernance d'entreprise sur la gestion du risque lié à la cybersécurité.

Maintenant que des lignes directrices claires ont été tracées par le RGPD à l'intention des sociétés qui naviguent dans le

cyberespace, la cybersécurité est devenue un élément important et émergent à considérer dans tous les secteurs. C'est pour cette raison que nous continuerons à aider les sociétés qui ont une longueur d'avance et celles qui ont pris du retard à établir de meilleures pratiques dans ce domaine.

La façon dont BMO Gestion mondiale d'actifs peut vous aider How can BMO Global Asset Management help?

BMO Gestion mondiale d'actifs offre un éventail d'approches conçues pour aider les clients à gérer les risques liés aux changements climatiques et les occasions de faire croître leurs portefeuilles.

- Nous offrons pour tous les portefeuilles d'actions et d'obligations de sociétés un service de représentation superposé appelé ***reo***[MD]. Dans le cadre de ce service, nous gérons un programme de mobilisation pluriannuel axé sur le risque lié aux changements climatiques et demandons aux sociétés d'élaborer et de dévoiler des stratégies sur les changements climatiques, conformément aux recommandations du groupe de travail.
- Notre g**amme de fonds responsables** repose sur une stratégie complète qui explique comment ces fonds peuvent favoriser le passage à une économie à faibles émissions de carbone, y compris le retrait des investissements dans les entreprises possédant des réserves de combustibles fossiles, les investissements dans celles qui offrent des solutions énergétiques propres, l'engagement et la communication de l'empreinte carbone des fonds.
- Aussi, dans le cadre de **mandats d'investissement en obligations vertes** que nous gérons pour les clients, nous investissons dans des obligations soigneusement sélectionnées de sociétés dont les revenus sont orientés vers des solutions liées aux changements climatiques et permettons ainsi aux clients d'orienter le capital dans une économie à faibles émissions de carbone.

Communiquez avec nous pour en apprendre davantage

Prix et récompenses

Le fonds d'actions mondiales responsable de F&C* a obtenu les mentions suivantes :

- Meilleur fonds d'investissement à caractère durable dans le cadre de l'Investment Week
- Meilleur fonds d'investissement à caractère éthique et fonds ISR selon Money Observer

* Le Fonds ESG d'actions mondiales responsable de BMO Gestion d'actifs est offert aux investisseurs institutionnels canadiens et géré selon une stratégie similaire à celle appliquée au fonds d'actions mondiales responsable de F&C.