Un rappel à l'ordre d'un milliard de dollars

Composer avec l'incertitude réglementaire et les risques de non-conformité

EY
Travailler ensemble pour un monde meilleur

Microsoft

En bref

- La conformité aux réglementations en matière d'accès aux données et de protection des données est devenue un élément important du profil de risque d'entreprise.
- La gestion du risque de non-conformité réglementaire requiert une mentalité opérationnelle, des processus durables et une plateforme intégrée.
- Une plateforme de cybersécurité intégrée, comme la suite d'outils de cybersécurité intégrés de Microsoft, peut s'avérer utile dans la simplification et le renforcement des cyberdéfenses tout en allégeant le fardeau de la conformité réglementaire.

En mai 2023, l'Union européenne a imposé à Meta une amende record de 1,3 G$ US après avoir conclu que l'entreprise avait enfreint son Règlement général sur la protection des données (RGPD) en transférant des données d'utilisateurs de l'Europe aux États-Unis[1]. Face à cette situation, l'Irish Data Protection Commission a ordonné à Meta de suspendre tout transfert de données personnelles appartenant aux utilisateurs de l'Union européenne et de l'Espace économique européen vers les États-Unis. L'amende dépasse celle prononcée contre Amazon en 2021 en vertu du RGPD, qui totalisait 877 M$ US.

Bien que le *New York Times* ait fait état le 10 juillet[2] d'une entente permettant aux données de Meta, de Google et d'autres entreprises de continuer à circuler entre les États-Unis et l'Union européenne, des représentants gouvernementaux des quatre coins de l'Europe ont menacé de faire échouer l'entente[3]. Certains observateurs de la scène européenne de la protection des données sont d'avis que le cadre de protection des données personnelles n'est pas autant à l'abri des contestations judiciaires que certains promoteurs de l'accord le laissent croire[4].

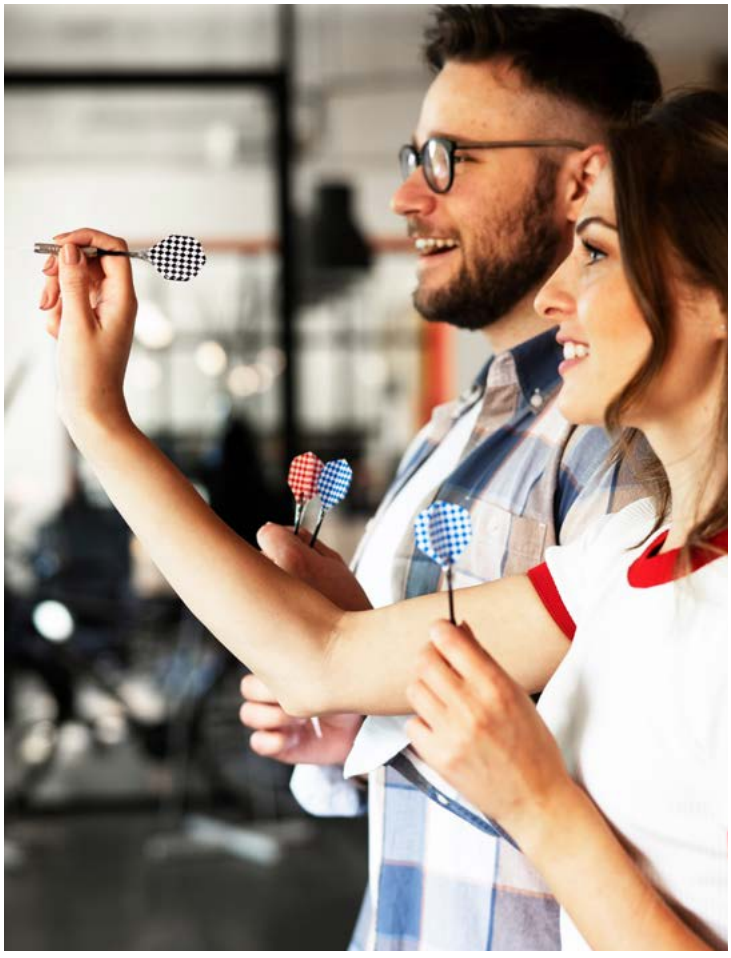
L'ombre de l'incertitude réglementaire : Appel à la simplification des données

Le doute qu'entraîne le contexte actuel met en évidence les conséquences majeures d'une non-conformité aux règlements en matière d'accès aux données et de protection des données, ainsi que la difficulté d'évoluer dans une époque d'incertitude réglementaire. Chez les dirigeants d'entreprise, l'affaire Meta devrait inciter à simplifier l'accès aux données et la protection des données, notamment en se servant d'une plateforme moderne de protection des données pour restreindre le problème et rendre les risques connexes plus simples à gérer.

Le contexte actuel de conformité réglementaire, riche en complexité, foisonne de processus manuels pour intervenir en cas de perte de données, recueillir de l'information sur l'emplacement des données et répondre aux demandes d'accès présentées par des personnes concernées. Les professionnels d'EY travaillent avec les clients pour l'adoption de technologies novatrices comme l'intelligence artificielle (IA) pour alléger leurs obligations en matière de conformité. En effet, il est fastidieux de se conformer à ces règlements complexes tout en veillant à ce que les données soient utilisées, stockées et transmises correctement de part et d'autre des frontières.

Simplifier la conformité grâce à des technologies novatrices

L'évolution des règlements pousse les organisations à apporter des changements provisoires à leurs stratégies de gestion des accès, de protection des données et de protection de la vie privée, une pratique qui ne s'inscrit pas dans le long terme. Plutôt que de s'appuyer sur des contrôles fragmentés de protection des données (chiffrement, conversion en jetons, masquage, etc.), les sociétés d'avant-garde établissent des politiques exécutoires s'appuyant sur une plateforme de sécurité intégrée qui sont mises en œuvre dans une optique opérationnelle.



[1] *Meta fined record $1.3 billion and ordered to stop sending European user data to US*, Associated Press, https://apnews.com/article/meta-facebook-data-privacy-fine-europe-9aa912200226c3d53aa293dca896 8f84, 22 mai 2023.

[2] *U.S. and E.U. Complete Long-Awaited Deal on Sharing Data*, The New York Times, https://www.nytimes.com/2023/07/10/technology/us-eu-data-privacy-deal.html?searchResultPosition=4, 10 juillet 2023.

[3] *New EU-US data transfer deal also faces criticism in Germany*, Euractiv, https://www.euractiv.com/section/data-protection/news/new-eu-us-data-transfer-deal-also-faces-criticism-in-germany/, 14 septembre 2023.

[4] *EU-US Data Privacy Framework to face serious legal challenges, experts say*, Computerworld, https://www.computerworld.com/article/3702550/eu-us-data-privacy-framework-to-face-serious-legal-challenges-experts-say.html, 12 juillet 2023.

Composer avec une réglementation variable : Un besoin de durabilité

Un nouveau livre blanc d'EY, intitulé « Proactively adapting to cross-border regulatory needs », pose un point de vue sur la conformité durable et son incidence sur les organisations, notamment sur la façon de répondre efficacement à de multiples exigences en matière de protection des données, enjeu au cœur du litige de Meta relativement au RGPD :

Les règlements de localisation des données sont stricts et exigent des organisations qu'elles utilisent, stockent ou traitent les données dans le pays de leur origine. Des pays comme l'Australie, le Royaume-Uni et la Chine, ainsi que certaines zones comme l'Europe, disposent de règlements locaux imposant non seulement de stocker et de traiter les données personnelles à l'intérieur de leurs frontières, mais aussi d'en restreindre l'accès aux personnes se trouvant à l'étranger. Pour appliquer des restrictions d'accès, l'organisation détermine d'abord de quel pays proviennent les données et si on peut y avoir accès à l'étranger. Si tel est le cas, le lieu d'identification et de collecte de données pose problème en raison des processus manuels de collecte de données et d'une compréhension lacunaire des données.

L'organisation peut recourir à l'orchestration et à des façons novatrices de visualiser des données issues de plusieurs pays sans modifier le lieu de stockage de données là où elles sont gérées. Une composante d'orchestration peut donner lieu à la coexistence d'un accès conditionnel aux anciens et aux nouveaux systèmes pour obtenir des données, accès dont les conditions peuvent se fonder sur des directives. L'orchestration permet aux services de TI d'évoluer selon les besoins de l'entreprise sans perturber les activités. De plus, elle permet de procéder à l'automatisation centrale des tâches et de surveiller différents applications et répertoires.

Fournir un accès aux données et une protection des données durables et sûrs ne va pas sans directives de cybersécurité claires, rédigées en langage simple et concis, qui répondent aux questions « Quoi? », « Où? » et « Pourquoi? » au sujet de l'entreprise, du conseil d'administration et des organismes de réglementation. Par exemple, les directives de gestion de l'identité et de l'accès doivent décrire précisément qui peut avoir accès à quelle information et fournir un cadre permettant de gérer cet accès de manière fiable.

Élaborer des directives de cybersécurité claires et concises : L'équilibre entre rigueur et capacité d'adaptation

Les entreprises doivent comprendre que les directives sur les fuites de données, l'utilisation acceptable des données et l'accès des fournisseurs sont plus que des lignes directrices ou des propositions. Elles doivent pouvoir faire preuve d'une certaine souplesse pour s'adapter à l'évolution du contexte d'affaires. Un cadre stratégique bien structuré doit être conçu pour tenir compte des différences entre les régions et les organismes de réglementation. Ce qui répond aux exigences du RGPD pourrait contrevenir à celles de l'Administration du cyberespace de la Chine ou de la Securities and Exchange Commission (SEC) des États-Unis.

Une plateforme de cybersécurité intégrée doit simplifier et renforcer les cyberdéfenses et la résilience, tout en facilitant la conformité réglementaire. Par exemple, la suite d'outils de cybersécurité intégrés de Microsoft comprend un Gestionnaire de conformité, qui offre des fonctionnalités de bout en bout comme l'intégration, la gestion de flux de travail, la mise en œuvre de contrôles et le catalogage de preuves, qui sont toutes requises pour répondre aux exigences réglementaires. L'outil offre en outre des modèles d'évaluation réglementaire prêts à l'emploi et personnalisables dans plusieurs nuages pour documenter la conformité.

Protéger les données personnelles, une priorité

Une société technologique multinationale s'appuyant sur différentes plateformes de stockage de données ne pouvait se permettre d'exposer des données personnelles de nature délicate à un accès non autorisé. Le risque de non-conformité réglementaire et de préjudice à la réputation de l'entreprise était trop élevé.

Le défi : mettre fin à tout accès non autorisé aux données et satisfaire à une réglementation exigeante sans perturber les activités. En collaborant avec les équipes d'EY, le client a pu éviter des poursuites de millions de dollars en raison d'accès non autorisés. Le projet comportait une stratégie étendue, des outils de pointe, une analyse des connexions de données, une évaluation rigoureuse des autorisations d'accès et une catégorisation méticuleuse des données.

L'entreprise est aujourd'hui dotée d'un cadre rigoureux de surveillance et de catégorisation permanentes des données et maintient sa fidélité procédurale au moyen d'une vérification régulière de la conformité. Nous avons contribué à n'ouvrir la voie qu'aux accès autorisés et à formuler une stratégie pour la gestion efficace des différends portant sur les accès. En alliant prouesse technologique, processus simplifiés et application stricte des règles de conformité, les équipes d'EY ont aidé le client à tirer parti d'une sécurité des données et d'une harmonisation des règlements durables.

Résumé

Les programmes de cybersécurité alliant rentabilité et conformité sont au cœur des préoccupations des conseils d'administration en matière de gouvernance et de responsabilité de l'entreprise. Les dirigeants axés sur les profits doivent considérer les programmes de cybersécurité non pas comme une dépense fixe, mais comme un coût pouvant être optimisé grâce à une solution de gouvernance et de conformité des données appropriée, comme Microsoft Purview. Les services qu'offre EY, alignés sur les fonctionnalités de Microsoft Purview, aident les entreprises à faire passer leur gouvernance et leur conformité en matière de données d'une tâche ardue à des possibilités d'économies de coûts, de production de rapports plus utiles, de responsabilisation et d'affectation des ressources de sorte à protéger leurs données les plus précieuses.

Personnes-ressources

Découvrez comment l'alliance entre EY et Microsoft simplifie la cybersécurité pour aider votre organisation à se transformer dans la confiance, la fiabilité et la résilience.

Melissa Tamblyn

Leader du groupe Microsoft

EY Canada

melissa.tamblyn@ey.com

Nick Galletto

Associé

Leader, Cybersécurité, EY Canada

nick.galletto@ey.com

EY | Travailler ensemble pour un monde meilleur

La raison d'être d'EY est de bâtir un monde meilleur, de créer de la valeur à long terme pour les clients, les gens et la société, et de renforcer la confiance envers les marchés financiers.

S'appuyant sur les données et la technologie, les équipes diversifiées d'EY présentes dans plus de 150 pays instaurent la confiance au moyen de la certification, et aident les clients à prospérer, à se transformer et à exercer leurs activités.

Que ce soit dans le cadre de leurs services de certification, de consultation, de stratégie, de fiscalité ou de transactions, ou encore de leurs services juridiques, les équipes d'EY posent de meilleures questions pour trouver de nouvelles réponses aux enjeux complexes du monde d'aujourd'hui.

4420506

ey.com/fr_ca