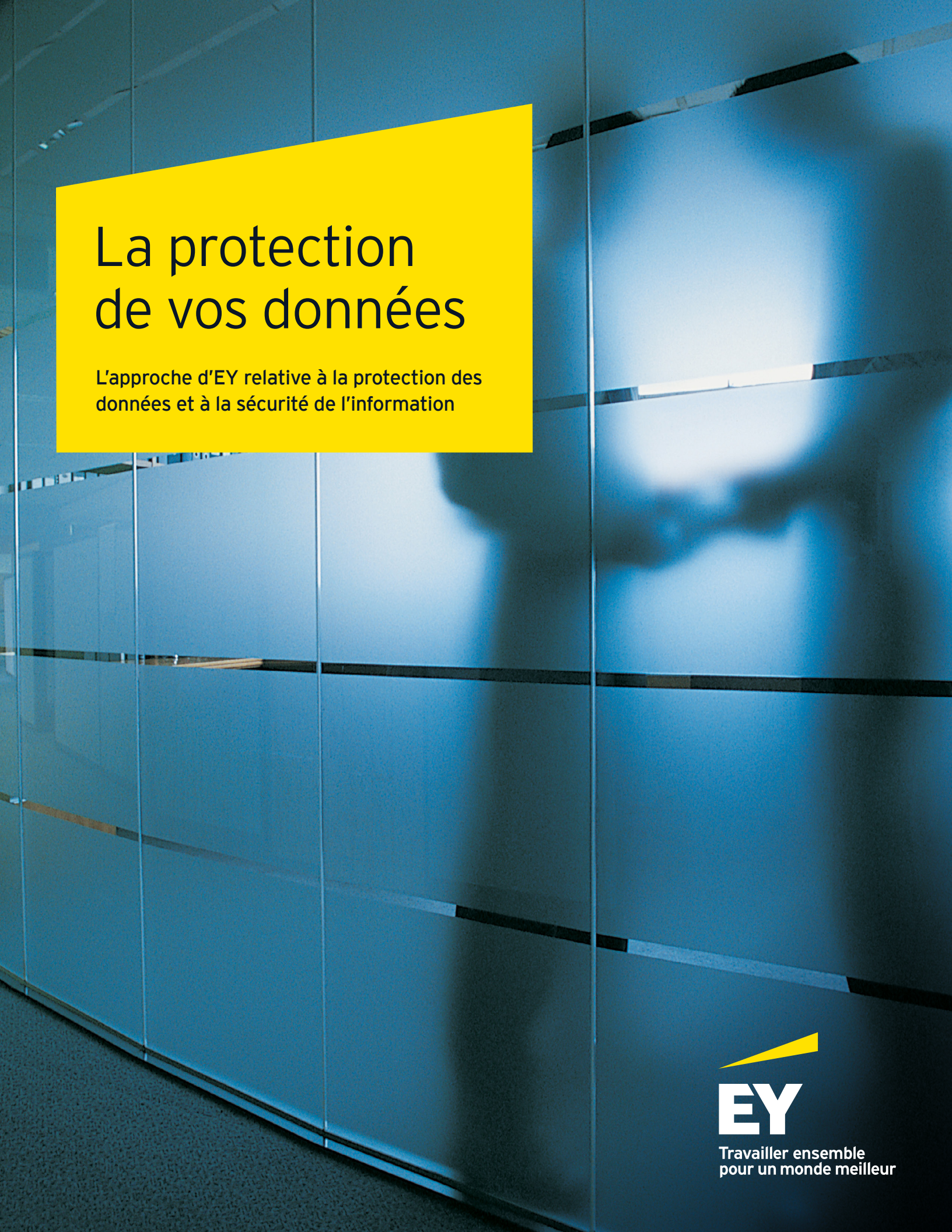


La protection de vos données

L'approche d'EY relative à la protection des données et à la sécurité de l'information

Travailler ensemble pour un monde meilleur

Pour EY, la réputation d'une entreprise passe par l'excellence de ses programmes de protection des données et de sécurité de l'information.

Nous considérons que la protection des données et la sécurité de l'information sont des aspects fondamentaux de la conduite des affaires. Nous nous engageons à protéger les actifs informationnels, les données à caractère personnel et les informations des clients. Selon nous, toute grande société de services professionnels se doit d'être dotée de rigoureux programmes de protection des données et de sécurité de l'information. Le présent document vise à résumer notre approche en matière de protection des données et de sécurité de l'information, et à présenter un aperçu des mesures que nous prenons pour protéger les informations des clients et nos systèmes d'information qui les sous-tendent. Les particularités de ces mesures dépendent parfois des services fournis et des dispositions réglementaires applicables dans le pays concerné. Nos programmes et pratiques de protection des données et de sécurité de l'information favorisent le partage approprié et légitime de l'information, dans le respect de la confidentialité, de l'intégrité et de la disponibilité des données.

Une stratégie de protection des données et de sécurité de l'information bien définie

Les équipes d'EY sont en mesure de fournir à leurs clients un service uniforme et de meilleure qualité à l'échelle mondiale, en toute transparence, grâce à une stratégie de protection des données et de sécurité de l'information bien définie. Nous protégeons les actifs informationnels, les données à caractère personnel et les informations des clients, peu importe où et quand ils sont créés, traités, transmis ou stockés. Nous maintenons également une gouvernance efficace et respectons les normes réglementaires nationales et internationales applicables.

Le réseau mondial de la protection des données et l'organisation mondiale sur la sécurité de l'information, deux entités distinctes, mais bien arrimées, mettent en œuvre et gèrent nos programmes et nos pratiques en matière de protection des données et de sécurité de l'information. Ces entités ont pour mission de prévenir la collecte, la conservation, l'utilisation, la communication, la modification ou la destruction non autorisées des actifs informationnels de l'organisation EY et de ses clients. Pour ce faire, elles s'appuient sur des directives, des normes, des lignes directrices et leurs procédures connexes, des contrôles technologiques et administratifs, ainsi que sur des activités continues de formation et de sensibilisation.

Le réseau mondial de la protection des données et l'organisation mondiale sur la sécurité de l'information d'EY sont animés par des priorités que partagent toutes les sociétés EY à l'échelle mondiale. C'est donc une même vision cohérente de la protection des actifs informationnels, des données à caractère personnel et des informations des clients qui est véhiculée au sein d'EY.

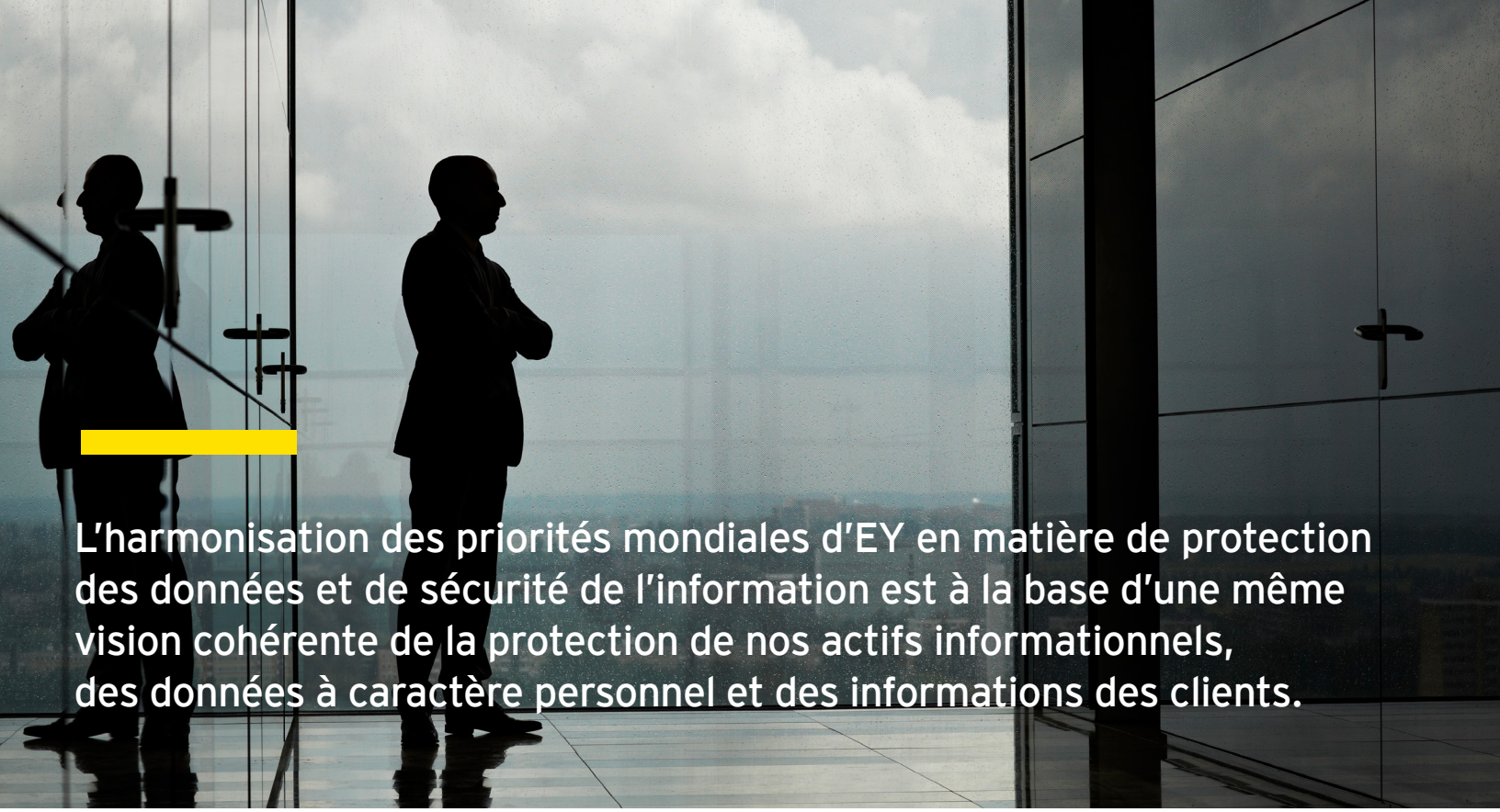
Notre cadre de protection des données
Notre cadre de protection des données repose sur des principes de droit pertinents (y compris le *Règlement général sur la protection des données* (RGPD) de l'Union européenne (UE)), d'autres exigences réglementaires ainsi que sur des normes professionnelles applicables. Il démontre l'engagement de toutes les sociétés EY à protéger les données à caractère personnel et les données confidentielles (y compris les données des clients), qui repose sur les principes suivants :

- Licéité, loyauté et transparence : Utiliser les données de manière éthique, raisonnable, clairement communiquée et licite.
- Limitation des finalités : N'utiliser les données que pour des usages définis et approuvés.
- Minimisation des données : Recueillir et traiter uniquement les données nécessaires aux finalités établies.
- Exactitude : Veiller à ce que les données soient exactes et d'une qualité suffisante eu égard aux finalités établies.
- Limitation de la conservation : Conserver les données uniquement le temps nécessaire eu égard aux finalités pour lesquelles elles ont été collectées.
- Intégrité et confidentialité : Veiller à ce que la sécurité et la confidentialité des données soient préservées et à ce que l'accès soit contrôlé et accordé de façon sélective.
- Responsabilité : Être en mesure de démontrer que les principes relatifs à la protection des données ont été respectés conformément à la Directive mondiale sur la protection et la confidentialité des données et au Code de conduite mondial d'EY.
- Renseignements sensibles : Prêter une attention particulière lors du traitement des données à caractère personnel sensibles ou des informations sensibles des clients.
- Sous-traitants indépendants : Veiller à ce que les tiers qui traitent des données à caractère personnel ou des données confidentielles, y compris les données des clients, pour le compte de l'organisation EY aient adopté un cadre de protection des données qui protège adéquatement de telles données, et à ce que les contrats conclus avec ces tiers comportent des modalités en matière de protection des données qui respectent les lois applicables.

Éléments de notre cadre de protection des données

Transferts internationaux de données
Les transferts internationaux de données à caractère personnel sont rigoureusement régis par des lois et règlements clés concernant la protection des données (comme le droit européen en matière de protection des données). Diverses lois sur la protection des données dans le monde interdisent le transfert des données à caractère personnel à l'étranger, à moins que l'organisation procédant à un tel transfert ait mis en place des garanties appropriées. Les équipes d'EY emploient des mécanismes de transfert des données approuvés pour se conformer aux lois sur la protection des données. Nous gardons également à l'esprit l'arrêt rendu par la Cour de justice de l'Union européenne (CJUE) dans l'affaire « Schrems II » concernant le transfert de données européennes à caractère personnel vers des pays hors de l'Espace économique européen qui ne disposent pas de mesures législatives globales en matière de protection des données. Ces pays n'assurent donc pas, du point de vue de l'UE, un niveau de protection adéquat des droits des personnes à la confidentialité des données.

- Les équipes d'EY analysent l'impact des lois et pratiques locales sur le transfert des données et recourent à des mesures supplémentaires appropriées pour s'assurer que la protection des données à caractère personnel est adéquate, au besoin.
- Les équipes d'EY ont déterminé des règles d'entreprise contraignantes (REC) destinées au responsable du traitement et au sous-traitant, qui régissent le transfert international des données à caractère personnel entre les sociétés EY. Grâce à ces règles, nous pouvons procéder au transfert fluide des données à caractère personnel d'une société EY à une autre, ce qui facilite la coopération interfonctionnelle. Les REC, qui s'appliquent à toutes les sociétés EY à l'échelle mondiale, sont publiées à l'adresse ey.com/bcr.
- Les sociétés EY intègrent des clauses contractuelles types approuvées aux contrats conclus avec les clients et les tiers, s'il y a lieu.
- La société américaine Ernst & Young LLP et ses entités américaines affiliées adhèrent au cadre de protection des données UE–États-Unis (de même qu'à l'extension britannique de celui-ci) et au cadre de protection des données Suisse–États-Unis publiés par le département du Commerce américain. Pour en savoir plus, consultez la page Ernst & Young LLP EU-US Data Privacy Framework Privacy Statement.



L'harmonisation des priorités mondiales d'EY en matière de protection des données et de sécurité de l'information est à la base d'une même vision cohérente de la protection de nos actifs informationnels, des données à caractère personnel et des informations des clients.

Programmes de formation et de sensibilisation
Les informations, lignes directrices et activités de formation que nous offrons aux gens d'EY doivent suivre l'évolution des stratagèmes d'attaque informatique. Tenir nos gens au fait des menaces d'atteinte à la confidentialité des données et à la sécurité de l'information est un processus dynamique auquel nous attachons beaucoup d'importance, comme en témoignent les activités de formation régulièrement mises à jour que doivent suivre les professionnels de toutes les gammes de services d'EY, de même que les diverses autres activités informationnelles visant l'ensemble des membres d'EY à l'échelle mondiale.

Directive mondiale d'EY en matière de sécurité de l'information

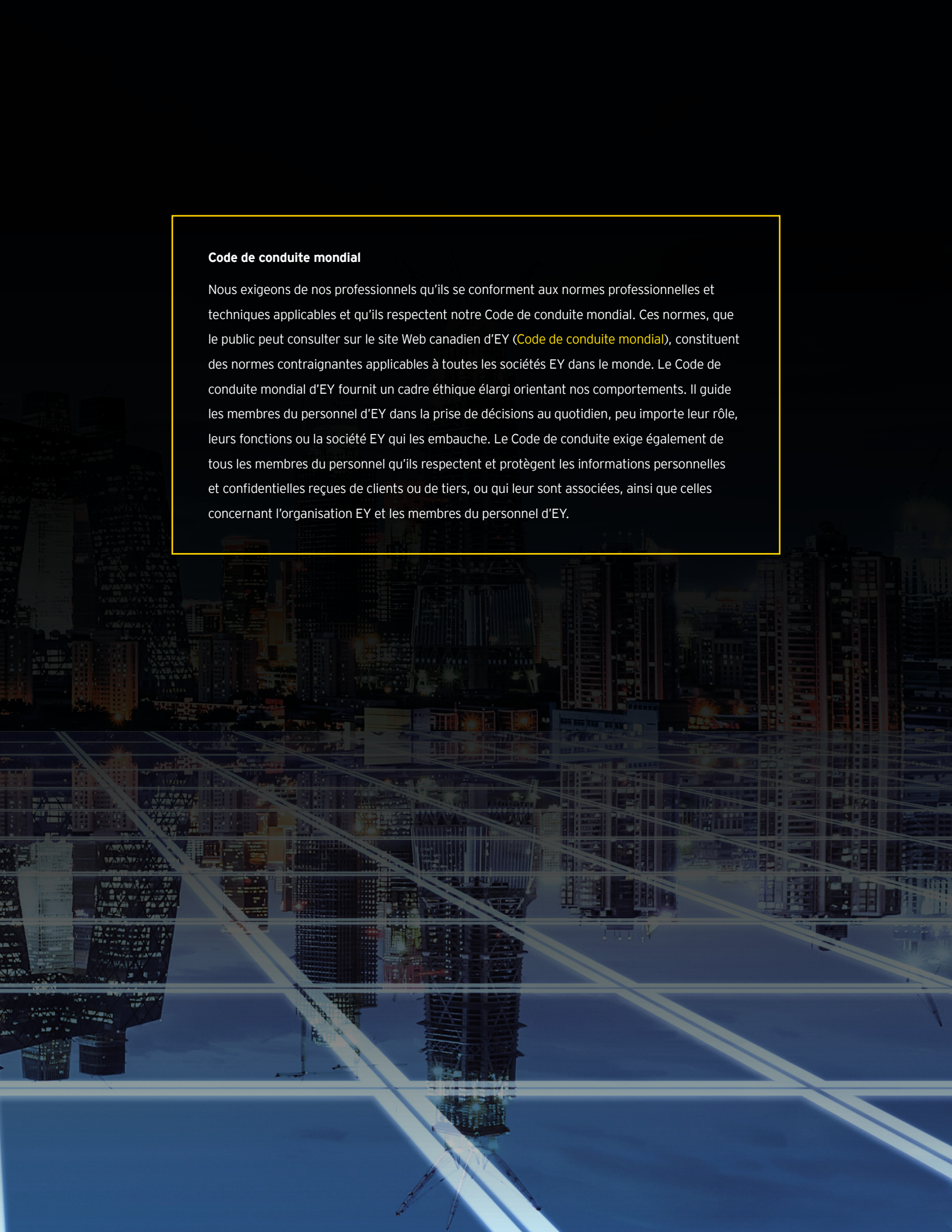
Nous réexaminons régulièrement notre directive sur la sécurité de l'information et les normes et contrôles sur lesquels celle-ci s'appuie, de façon à veiller à ce que leur contenu demeure exact et à jour et qu'il reflète les obligations légales et réglementaires auxquelles notre organisation est assujettie. Conformément aux cadres reconnus, notamment la norme ISO 27001, des énoncés de politique obligatoires ou suggérés portent sur près d'une douzaine d'aspects de la sécurité de l'information largement reconnus, tels que :

- Le contrôle des accès
- La gestion des actifs : classification et contrôle
- La sécurité des communications et des activités
- La sécurité des ressources humaines : personnel
- L'acquisition, le développement et la maintenance des systèmes d'information
- La sécurité physique et environnementale
- La gestion des risques

Contrôles de sécurité technologique
Notre approche relative à la sécurité de l'information ne repose pas que sur une directive ou une norme de sécurité écrite. Nous préservons également la confidentialité, l'intégrité et la disponibilité de l'information en protégeant nos ressources et actifs technologiques. Voici certaines des mesures prises à cet égard :

- Cryptage intégral du disque dur des ordinateurs de bureau et portables
- Utilisation d'outils de cryptage des supports amovibles
- Installation de pare-feu dans les ordinateurs de bureau et portables
- Utilisation d'antivirus et de programmes de protection contre les logiciels malveillants
- Utilisation de méthodes d'authentification multifactorielle
- Évaluation des vulnérabilités en matière de sécurité et application de correctifs automatisées
- Mise en place de contrôles physiques, environnementaux, réseaux et périmétriques rigoureux
- Recours à des technologies de détection et de prévention des intrusions
- Emploi de systèmes de surveillance et de détection

De plus, nous consacrons beaucoup de temps et de ressources à l'acquisition de technologies de sécurité d'avant-garde. Nous harmonisons notre stratégie de sécurité de l'information avec notre feuille de route technologique et restons liés de près avec les services technologiques que nous offrons. C'est ainsi que nous pouvons répondre adéquatement aux problèmes de sécurité qui, autrement, risqueraient de porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité de nos ressources technologiques.



Code de conduite mondial

Nous exigeons de nos professionnels qu'ils se conforment aux normes professionnelles et techniques applicables et qu'ils respectent notre Code de conduite mondial. Ces normes, que le public peut consulter sur le site Web canadien d'EY (Code de conduite mondial), constituent des normes contraignantes applicables à toutes les sociétés EY dans le monde. Le Code de conduite mondial d'EY fournit un cadre éthique élargi orientant nos comportements. Il guide les membres du personnel d'EY dans la prise de décisions au quotidien, peu importe leur rôle, leurs fonctions ou la société EY qui les embauche. Le Code de conduite exige également de tous les membres du personnel qu'ils respectent et protègent les informations personnelles et confidentielles reçues de clients ou de tiers, ou qui leur sont associées, ainsi que celles concernant l'organisation EY et les membres du personnel d'EY.

Sécurité de l

Continuité des activités et reprise après sinistre
Nos capacités en matière de reprise après sinistre et de continuité des activités, en conformité avec la norme ISO 22301, témoignent de la volonté renouvelée de l'organisation EY de protéger ses propres données ainsi que celles de ses clients. Nous nous engageons à protéger nos gens, nos installations, nos infrastructures, nos processus d'affaires, nos applications et nos données avant, pendant et après un éventuel sinistre. Les procédures d'intervention en cas de sinistre et de reprise des systèmes applicables à nos applications d'affaires critiques ont été soigneusement planifiées et testées. Nos méthodologies en matière de reprise après sinistre et de continuité des activités comprennent ce qui suit :

- L'évaluation des incidences sur l'entreprise
- Les plans de reprise après sinistre essentiels à la mission, fondés sur les normes sectorielles
- Le soutien de concepteurs de plans de reprise après sinistre et de continuité des activités certifiés
- La mise à l'essai régulière des plans de reprise après sinistre ou de continuité des activités aux fins de la vérification de leur état de préparation opérationnelle

Programme de gestion des risques liés aux fournisseurs
Ce programme est harmonisé avec nos processus de contrôle diligent de gestion des relations avec les fournisseurs, de façon à couvrir les activités avec des tiers relatives à la sécurité de l'information, à l'approvisionnement, aux contrats, à la protection des données et à l'indépendance :

- Évaluation de la conformité des fournisseurs potentiels à nos directives et contrôles mondiaux harmonisés avec les normes ISO 27001 et 27002
- Revues de contrôle diligent, y compris les cotes de risque et les constatations
- Soutien à l'atténuation des constatations quant aux risques
- Soutien à la sélection des fournisseurs et aux négociations de contrats

Nous nous appuyons sur des évaluations de la sécurité conformes aux normes du secteur pour apprécier le risque inhérent ou résiduel en matière de sécurité de l'information et de conformité de même que d'autres catégories de risques, comme le classement, l'emplacement, l'accès et le type de transmission des données.

Stratégie et attitude en matière de sécurité
Notre programme de sécurité à volets multiples repose sur les directives en matière de sécurité de l'information et de conduite personnelle déployées dans le monde entier. Il vise à favoriser la protection de la confidentialité, de l'intégrité et de la disponibilité des données à caractère personnel et des actifs informationnels de nos clients. Nous soutenons les efforts en ce sens en utilisant des technologies de protection des données en conformité avec les dispositions législatives et réglementaires applicables en matière de confidentialité, ainsi qu'avec les normes ISO 27001 et 27002 sur la gestion des programmes de sécurité, qui sont reconnues sur la scène internationale.

Notre organisation intervient de façon proactive aux fins de la sécurisation et de la gestion adéquate des informations confidentielles et personnelles, en s'appuyant sur son programme de sécurité de l'information reposant sur les normes ISO 27001 et 27002, lequel comprend :

- Une gestion appropriée des directives, normes, lignes directrices et programmes
- D'excellents contrôles de sécurité technologique
- Un programme de conformité en matière de sécurité prévoyant des examens de la sécurité, des certifications et des audits
- Une stratégie et une feuille de route en matière de sécurité bien définies prenant en compte les aspects suivants :
  - La protection des données : exigences légales, réglementaires et procédurales
  - Les activités d'entreprise : procédures et exigences prescrites
  - Les technologies : directives, normes et procédures
  - Les menaces externes : évolution du contexte dans lequel s'inscrivent les menaces d'atteinte à la sécurité
- Un programme de gestion des incidents de sécurité axé sur le contrôle et le règlement efficaces des incidents liés à la sécurité, y compris le programme d'intervention à l'égard des vulnérabilités critiques en matière de cyberdéfense

Conformité et audit

Les équipes d'EY ont mis en place des programmes de protection des données et de sécurité de l'information à l'échelle mondiale. Nous maintenons une fonction gouvernance efficace et procédons à des examens de la conformité dans le cadre d'exercices d'audit en bonne et due forme. Nous assurons le respect des obligations de protection des données et de sécurité de l'information au moyen des examens et programmes indiqués ci-après.

Processus de certification de la sécurité
Préalablement à leur mise en œuvre, toutes les applications et tous les systèmes sont soumis à notre processus de certification de la sécurité, qui permet d'obtenir la confirmation qu'ils ont été développés conformément à nos directives en matière de sécurité de l'information et aux normes de développement d'applications sécuritaires.

Le processus de certification de la sécurité comprend une évaluation des risques, des examens de la documentation et des analyses des vulnérabilités. Toute application ou tout système servant à créer, stocker ou gérer de l'information en notre nom doit y être soumis. Ce processus nous permet de préserver la confidentialité, l'intégrité et la disponibilité de notre information et de celle de nos clients.

Analyses d'impact sur la protection et la confidentialité des données
Les équipes d'EY qui élaborent ou mettent en œuvre des systèmes ou des outils qui traitent des données à caractère personnel ou des informations des clients doivent communiquer avec les équipes de la protection des données afin qu'elles procèdent à une analyse d'impact sur la protection et la confidentialité des données. Une analyse d'impact consiste à examiner le système ou l'outil concerné en fonction de normes mondiales et, lorsqu'il y a lieu, à prodiguer des conseils visant à atténuer les risques d'atteinte à la confidentialité et à la protection des données.

Après la réalisation d'une analyse d'impact sur la protection et la confidentialité des données, une liste de recommandations est préparée à l'intention de tous les utilisateurs et administrateurs des systèmes ou outils concernés. Cette analyse détaillée comporte un examen de tous les transferts de données transfrontaliers, qui vise à confirmer que ceux-ci répondent aux exigences légales et réglementaires applicables.

Nous utilisons un ensemble exhaustif de directives et de lignes directrices qui facilitent le déploiement des systèmes et des outils conformément aux normes et exigences de protection des données applicables.

Évaluations de l'efficacité des contrôles
Pour nous assurer de l'efficacité de la mise en place et du fonctionnement des contrôles, nous soumettons ceux-ci à divers types d'évaluation :

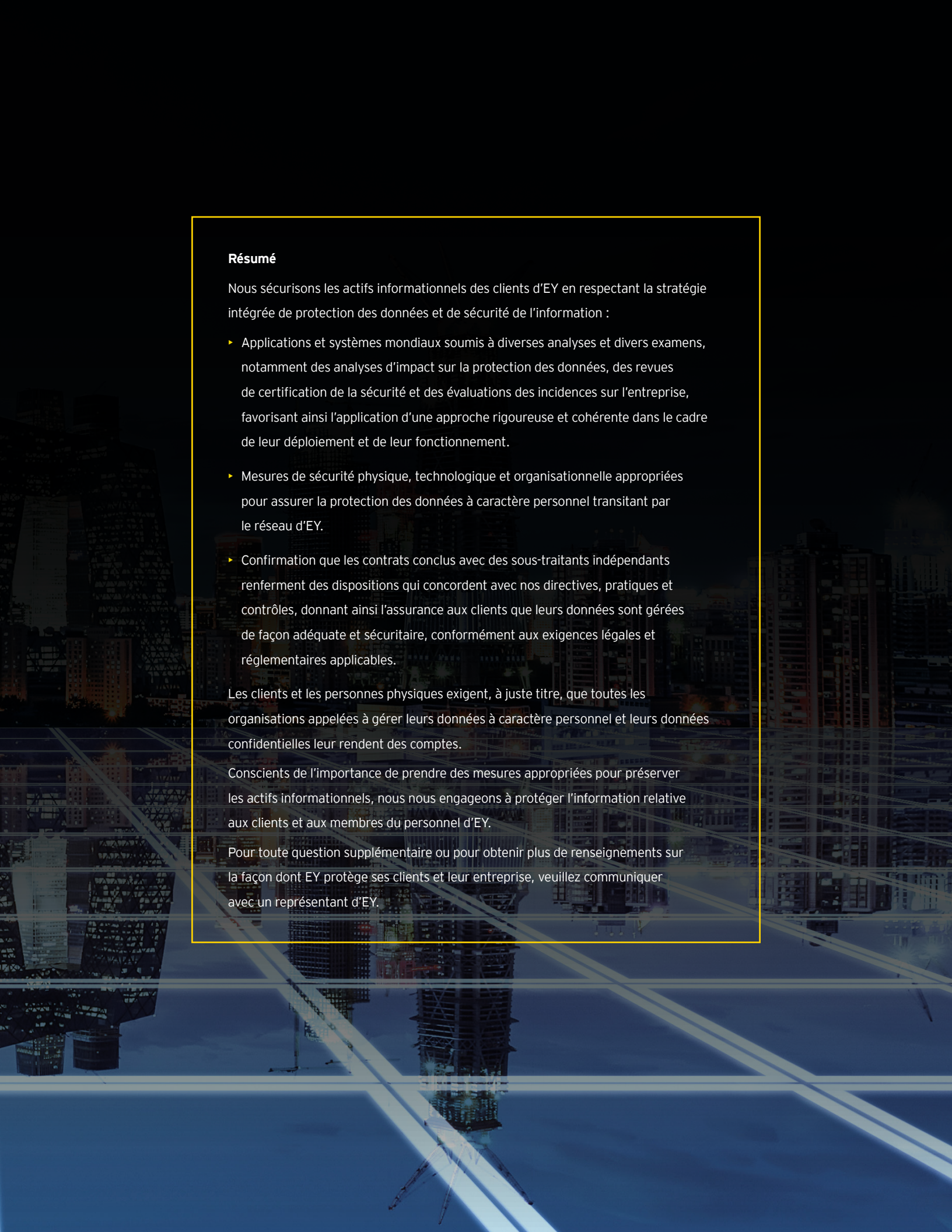
- Évaluation des vulnérabilités des réseaux et applications axée sur les aspects techniques de la directive mondiale en matière de sécurité de l'information, tels que la gestion des correctifs et la sécurité des applications et des infrastructures
- Évaluation de l'efficacité opérationnelle axée sur l'examen des contrôles techniques et l'établissement de processus relatifs à des composantes telles que les systèmes d'exploitation, les bases de données et les infrastructures
- Surveillance opérationnelle continue de l'efficacité des contrôles de sécurité pour en valider la mise en place et la configuration adéquates

Audits de la sécurité de l'information
Afin de permettre aux équipes d'EY d'obtenir un portrait plus complet de la conformité aux exigences de sécurité de l'information, les produits technologiques, services et centres de données d'EY à l'échelle mondiale sont soumis à des audits. Les équipes d'EY procèdent à divers types d'audits :

- Audits de la conformité des tiers indépendants à la norme ISO 27001 pour la certification du système de gestion de la sécurité de l'information utilisé dans nos trois centres de données mondiaux, aux États-Unis, en Allemagne et à Singapour, ainsi que dans nos salles de données locales
- Audits de la conformité des tiers indépendants à la norme ISO 27017 pour la certification des contrôles de sécurité de l'information dans l'environnement informatique de la plateforme technologique cliente EY Fabric hébergée dans l'infrastructure infonuagique d'un tiers
- Audit de la conformité des tiers indépendants à la norme ISO 22301, qui comprend les éléments du système mondial de gestion de la continuité des activités d'EY
- Réalisation par un auditeur tiers indépendant d'une attestation annuelle de type 2 selon la norme SOC 2, qui englobe les principes de sécurité, de confidentialité et de disponibilité et vise nos trois centres de données mondiaux aux États-Unis, en Allemagne et à Singapour, nos salles de données locales ainsi que la plateforme technologique cliente EY Fabric hébergée dans l'infrastructure infonuagique d'un tiers
- Réalisation d'une attestation annuelle de type 2 selon la norme ISAE 3402/SOC 1 aux fins de laquelle nos contrôles de sécurité mis en place dans nos trois centres de données mondiaux aux États-Unis, en Allemagne et à Singapour, dans nos salles de données locales ainsi que sur la plateforme EY Fabric hébergée dans l'infrastructure infonuagique d'un tiers sont testés et vérifiés par un tiers indépendant
- Balayages des vulnérabilités des réseaux axés sur les aspects techniques de la directive mondiale d'EY en matière de sécurité de l'information, tels que la gestion des correctifs et la sécurité des applications et des infrastructures
- Audits fondamentaux axés sur l'examen des contrôles techniques et des processus de production de composants tels que les systèmes d'exploitation, les bases de données et les infrastructures
- Audits sur le terrain comprenant des entretiens avec les principaux dirigeants, des tests de cheminement détaillés, des examens de la documentation et des balayages des vulnérabilités des réseaux – le type d'audit le plus important et le plus détaillé, qui consiste à évaluer la conformité à tous les aspects de la directive mondiale d'EY en matière de sécurité de l'information

Les constatations issues de l'audit de la conformité aux exigences de sécurité de l'information sont compilées et validées par la haute direction. S'il y a lieu, des plans de mesures correctrices sont élaborés et acceptés.

Dérogations aux exigences de sécurité de l'information
Si un problème ne peut pas être réglé dans le cadre d'un plan de mesures correctrices, un processus d'attribution de dérogations permet d'examiner les risques connexes et de trouver des solutions de rechange. Cette démarche comprend un processus d'approbation structuré, des examens réguliers de chaque dérogation et une évaluation de la sécurité donnant lieu à l'attribution d'une cote de risque. Les dérogations approuvées s'accompagnent généralement de contrôles compensatoires qui contribuent à atténuer adéquatement les risques pouvant découler de la modification. Ce processus d'attribution de dérogations permet de confirmer que les dérogations et toutes les mesures correctrices subséquentes sont adéquatement documentées, gérées et réexaminées au moins une fois l'an.



Résumé

Nous sécurisons les actifs informationnels des clients d'EY en respectant la stratégie intégrée de protection des données et de sécurité de l'information :

- Applications et systèmes mondiaux soumis à diverses analyses et divers examens, notamment des analyses d'impact sur la protection des données, des revues de certification de la sécurité et des évaluations des incidences sur l'entreprise, favorisant ainsi l'application d'une approche rigoureuse et cohérente dans le cadre de leur déploiement et de leur fonctionnement.
- Mesures de sécurité physique, technologique et organisationnelle appropriées pour assurer la protection des données à caractère personnel transitant par le réseau d'EY.
- Confirmation que les contrats conclus avec des sous-traitants indépendants renferment des dispositions qui concordent avec nos directives, pratiques et contrôles, donnant ainsi l'assurance aux clients que leurs données sont gérées de façon adéquate et sécuritaire, conformément aux exigences légales et réglementaires applicables.

Les clients et les personnes physiques exigent, à juste titre, que toutes les organisations appelées à gérer leurs données à caractère personnel et leurs données confidentielles leur rendent des comptes.

Conscients de l'importance de prendre des mesures appropriées pour préserver les actifs informationnels, nous nous engageons à protéger l'information relative aux clients et aux membres du personnel d'EY.

Pour toute question supplémentaire ou pour obtenir plus de renseignements sur la façon dont EY protège ses clients et leur entreprise, veuillez communiquer avec un représentant d'EY.

EY | Travailler ensemble pour un monde meilleur

La raison d'être d'EY est de contribuer à un monde meilleur, en créant de la valeur à long terme pour ses clients, pour ses gens et pour la société, et en renforçant la confiance à l'égard des marchés financiers.

Les équipes diversifiées d'EY, réparties dans plus de 150 pays, renforcent la confiance grâce à l'assurance que leur permettent d'offrir les données et la technologie, et aident les clients à croître, 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 encore de leurs services transactionnels ou juridiques, les équipes d'EY posent de meilleures questions pour trouver de nouvelles réponses aux enjeux complexes du monde d'aujourd'hui.

4568042

ey.com/ca/fr