Avis relatif à la protection des données à caractère personnel

PwC Luxembourg – qu'il s'agisse de PricewaterhouseCoopers, de PwC Regulated Solutions, de PricewaterhouseCoopers Training Administration Service Centre ou de PricewaterhouseCoopers Academy S.à r.l., chacune de ces entités étant ci-après dénommée PwC Luxembourg – est le premier cabinet de services professionnels au Luxembourg et met l'accent sur les technologies de pointe et sur l'utilisation de l'environnement cloud. PwC Luxembourg s'efforce d'établir un climat de confiance en fournissant des services d'audit, des services fiscaux et des services de conseil de façon à protéger les informations de ses clients, de son personnel ainsi que celles d'autres personnes avec lesquelles le cabinet entretient des relations d'affaires, grâce à la conception de ses produits et la mise en place de mécanismes efficaces de protection de la sécurité de l'information. PwC Luxembourg aspire à promouvoir la transparence au moyen d'initiatives pédagogiques, de principes et de lignes de conduite en matière de protection des données ainsi qu'en fournissant aux personnes concernées des opportunités appropriées quant au choix de leurs données personnelles, à l'accès à celles-ci et à leur correction.

Le présent avis définit la façon dont PwC Luxembourg peut traiter, en conformité avec les lois applicables et pour les finalités définies ci-dessous, les données à caractère personnel recueillies occasionnellement (directement ou indirectement, de façon obligatoire ou volontaire, manuellement ou d'une autre façon) auprès des personnes concernées elles-mêmes ainsi qu'auprès de ses clients, de tiers (tels que des clients potentiels, des sous-traitants, des prestataires ou toute autre partie prenante participant à une mission avec PwC Luxembourg) et/ou, le cas échéant, recueillies auprès de sources à la disposition du grand public.

I. Définitions

- Le terme **Lois applicables** fait référence à toute loi, tout règlement et toute norme ayant trait à la protection, la confidentialité ou la sécurité des données à caractère personnel et applicables à PwC Luxembourg. Les Lois applicables comprennent le règlement général sur la protection des données (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) ;
- Les termes **personnes concernées, données à caractère personnel, traitement, responsable du traitement et sous-traitant** sont entendus au sens qui leur est attribué dans le règlement général sur la protection des données.

II. Finalités du traitement

PwC Luxembourg peut procéder au traitement des données à caractère personnel conformément aux Lois applicables et uniquement pour les finalités suivantes (**la/les « Finalité(s) »**) :

- Afin de fournir des services professionnels comprenant :

  - Services d'audit et d'assurance ;
  - Services ayant trait à la fiscalité, à la comptabilité et au reporting (conseils en fiscalité, respect des obligations fiscales au niveau mondial, fiscalité des personnes physiques, comptabilité, etc.) ; et
  - Services de conseil (Consulting, Corporate Finance, Global Fund Distribution, Forensic, People & Organisation, Regulatory & Compliance, Technology, etc.).

- Afin d'établir et de tenir à jour ses systèmes administratifs et ses systèmes de gestion des relations clients et fournisseurs, comprenant les éléments suivants :

  - Émission d'appels d'offres et rédaction de contrats ;
  - Suivi et gestion des clients, fournisseurs et anciens collaborateurs ;
  - Facturation et paiement des factures ;
  - Publicité, communication et relations publiques ;
  - Organisation de manifestations ;
  - Examens qualité ; et
  - Amélioration de l'expérience client ou utilisateur et personnalisation de la prestation de services (par exemple, par le biais de l'authentification, du suivi de la performance et de l'utilisation d'applications PwC le cas échéant).

- Afin d'appliquer des procédures d'acceptation des clients et de poursuite des relations d'affaires (y compris celles liées à la lutte contre le blanchiment des capitaux, la corruption et le financement du terrorisme) ;
- Afin de faciliter le respect de ses obligations juridiques, réglementaires, professionnelles et/ou contractuelles (y compris les exigences liées à l'indépendance et à l'archivage) ;
- Afin d'entretenir et de protéger ses bâtiments, ses équipements, son infrastructure et ses données informatiques (y compris la gestion et l'authentification des accès, la sécurité et le suivi des performances, etc.) ;
- Afin de garantir la continuité des activités ;
- Afin de gérer les risques et les litiges ;
- Afin de traiter les demandes des personnes concernées ; et/ou
- Afin de gérer ses sites internet.

Les Finalités ci-dessus sont basées sur au moins une des bases légales suivantes :

- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- le traitement est nécessaire au respect d'une obligation légale à laquelle PwC Luxembourg est soumis ;
- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par PwC Luxembourg ou par un tiers (tels que la protection des actifs de PwC Luxembourg, la compréhension des besoins et des attentes de ses clients ou la réalisation de la mission ou de l'intérêt social de PwC Luxembourg) ; et/ou
- la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques.

III. Catégories de données à caractère personnel faisant l'objet d'un traitement

En fonction des finalités et de la base juridique ci-dessus, PwC Luxembourg peut procéder au traitement des catégories de données à caractère personnel suivantes :

- Données relatives à l'identification (par exemple, nom et prénom, photographies et enregistrements audio et vidéo de particuliers, etc.) ;
- Données professionnelles (par exemple, fonction, société, etc.) ;
- Données administratives (par exemple, des documents d'identité, la date de naissance, le genre ou encore les langues parlées par la personne, etc.) ;
- Données financières (par exemple, des données fiscales ou des données transactionnelles, etc.) ;
- Données numériques (par exemple, des rapports d'activité, des adresses IP, etc.) ;
- Données de relation (par exemple, historique de la relation, feuilles de présence, etc.) ; et
- Données relatives à l'environnement (par exemple, état civil, caractéristiques, habitudes, informations liées aux réseaux sociaux).

IV. Catégories de personnes concernées

Les données à caractère personnel traitées par PwC Luxembourg peuvent se rapporter aux personnes concernées suivantes, le cas échéant :

- des clients et des clients potentiels ;
- des employés, stagiaires, bénéficiaires effectifs et membres du conseil d'administration de clients ou de clients potentiels, que ces fonctions soient occupées actuellement, qu'elles l'aient été dans le passé ou qu'elles le soient à l'avenir ;
- des fournisseurs, clients, agents, conseillers et/ou des membres de leur personnel employés par, ayant des relations d'affaires avec ou étant associés d'une autre manière avec un client ou un client potentiel ou intervenant ou pouvant intervenir dans le cadre d'une transaction ou d'un contrat avec un client ou un client potentiel.

V. Catégories de destinataires et transferts de données à caractère personnel

Selon les limites prévues ou exigées par les Lois applicables, PwC Luxembourg peut communiquer les Données à caractère personnel à tout destinataire concerné par la Finalité (les Finalités) et, lorsque ces destinataires traitent les données à caractère personnel au nom de PwC Luxembourg, s'ils sont liés par des engagements essentiellement équivalents à ceux de PwC Luxembourg tels qu'ils sont exprimés dans le présent avis.

Outre les personnes concernées elles-mêmes, les catégories de destinataires sont les suivantes :

- sous-contractants, partenaires commerciaux et experts ;

- sous-traitants et sous-traitants ultérieurs tels que des fournisseurs informatiques (y compris administrateurs systèmes, fournisseurs de services d'informatique en nuage, fournisseurs d'hébergement) ;
- autres entités PwC ;
- conseillers, agents ou auditeurs externes de PwC Luxembourg ;
- personnes morales ou physiques ayant des liens avec les personnes concernées (employeurs, parents et alliés, conseillers, associés existants ou potentiels, etc.) ; et/ou
- organismes de surveillance ou pouvoirs publics.

PwC Luxembourg s'interdit de transmettre les données à caractère personnel à quiconque situé en dehors de l'Espace économique européen (EEE), à moins qu'il ne s'agisse de i) pays offrant un niveau de protection adéquat des données à caractère personnel conformément à une décision de la Commission européenne ou de ii) destinataires ayant conclu un contrat approprié contenant les exigences des Lois applicables s'appliquant à ladite transmission. Une copie des garanties applicables ainsi que des éventuelles mesures additionnelles peut être demandée auprès du délégué à la protection des données de PwC Luxembourg.

VI. Sécurité

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, PwC Luxembourg met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite. Ces mesures comprennent entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité et la disponibilité constantes de ses systèmes de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci en cas d'incident ; ou
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

Des informations supplémentaires quant aux contrôles de sécurité des informations mis en place par PwC Luxembourg figurent à l'Annexe 1.

VII. PwC Luxembourg agissant en qualité de sous-traitant

Lorsque PwC Luxembourg traite des données à caractère personnel pour le compte d'un ou plusieurs responsables de traitement, sans exercer d'influence sur les finalités et les moyens du traitement ou sans

expertise professionnelle (au sens des lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD édité par le Comité européen de la protection des données), elle agit en qualité de sous-traitant. Cette section concerne toute externalisation de processus ou de fonction interne d'un responsable de traitement (paye, audit interne, déclaration fiscale…) vers PwC Luxembourg en tant que prestataire de service.

Dans ce cadre, PwC Luxembourg s'engage à traiter les données à caractère personnel uniquement sur les instructions du responsable du traitement documentée dans les documents contractuels applicables aux services et le présent avis. PwC Luxembourg veille également à ce que ses employés autorisés à accéder les données à caractère personnel soient soumis à une obligation appropriée de confidentialité. Afin d'éviter toute incertitude, le présent avis est destiné à remplir les exigences de l'article 28 du règlement général sur la protection des données.
PwC Luxembourg met à la disposition du responsable du traitement toutes les informations nécessaires afin de démontrer le respect des obligations prévues au présent avis et pour permettre la réalisation d'audits et des inspections selon les limites de ce qui est légalement possible et sous réserve de fournir un préavis raisonnable. Les audits ou les inspections sont effectués pendant les heures de bureau normales au Luxembourg et n'ont pas lieu plus d'une fois par an. PwC Luxembourg informe le responsable du traitement du fait que les audits ou les inspections n'enfreignent pas les obligations légales, réglementaires et contractuelles incombant à PwC Luxembourg, telles que celles ayant trait au secret professionnel. Par conséquent, le responsable du traitement et ses auditeurs potentiels ne se verront pas autoriser à accéder (i) à des données ou des informations d'autres clients de PwC Luxembourg, (ii) à des données appartenant en propre à PwC Luxembourg ou (iii) à toute autre information confidentielle de PwC Luxembourg qui n'est pas pertinente dans le cadre de l'audit ou de l'inspection ou qui ne rentre pas dans le champ clairement défini de l'audit ou de l'inspection.

En fonction de la nature du traitement et dans la mesure du possible, PwC Luxembourg aide le responsable du traitement par des mesures techniques et organisationnelles appropriées à s'acquitter de son obligation de :

- donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits définis au présent avis ;
- réaliser des analyses d'impact relatives à la protection des données et mener des consultations préalables auprès d'une autorité de contrôle ou d'une autre autorité publique, lorsque les Lois applicables l'exigent ;
- notifier une violation de données à caractère personnel à l'autorité de contrôle compétente et/ou aux personnes concernées. Dans ce but, PwC Luxembourg s'engage à notifier le responsable du traitement dans les meilleurs délais de toute faille sécuritaire conduisant à la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel, ou à l'accès non autorisé à de telles données, de manière accidentelle ou illicite ; et
- fournir des informations faisant l'objet de demandes raisonnables émises par le responsable du traitement afin de permettre à ce dernier de remplir ses obligations conformément à la législation applicable en matière de vie privée, lorsque PwC Luxembourg possède ou contrôle lesdites informations et que le responsable du traitement ne dispose pas d'autres moyens raisonnables d'obtenir les informations.

Lorsque PwC Luxembourg engage d'autres sous-traitants pour mener des activités de traitement spécifiques pour le compte du responsable du traitement (**Sous-traitants secondaires**), PwC Luxembourg leur impose les obligations équivalentes en matière de protection des données à celles qui sont énoncées au présent avis, par contrat ou au moyen d'un autre acte juridique au titre du droit de

l'Union Européenne ou du droit d'un État membre. Par la présente, le responsable du traitement donne une autorisation générale à PwC Luxembourg pour l'engagement des sous-traitants secondaires tels que définis dans la Section V ci-dessus. Toute modification envisagée concernant l'ajout ou le remplacement des sous-traitants secondaires sera communiquée au responsable du traitement.

VIII. Obligations des clients

En fonction des Finalités, la mise à disposition de données à caractère personnel constitue une exigence réglementaire et/ou contractuelle ; le défaut de mise à disposition desdites données à caractère personnel pourrait ne pas permettre à PwC Luxembourg de fournir les services.

PwC Luxembourg part du principe que les clients (ainsi que toute partie prenante intervenant dans le cadre d'une mission avec PwC Luxembourg pour laquelle les clients concernés se portent garants) veillent à la garantie des éléments repris ci-dessous. Ceci constitue une condition sine qua non à la réalisation des services.

- les données à caractère personnel qu'ils mettent à disposition de PwC Luxembourg (ou auxquelles ils lui donnent accès) devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour la Finalité spécifique pour laquelle elles sont divulguées et ces données sont sauvegardées de façon adéquate dans leurs systèmes ;
- ils respectent les Lois applicables en rapport avec le traitement des données à caractère personnel par PwC Luxembourg (dont notamment la licéité de la mise à disposition des données ainsi que, le cas échéant, l'obtention du consentement de la personne concernée et la gestion de celui-ci en conséquence) ;
- les personnes concernées sont informées des conditions et des modalités du traitement de leurs données à caractère personnel par PwC Luxembourg, conformément à la description fournie dans le présent avis et sous la forme exigée par les Lois applicables ; et
- ils informent PwC Luxembourg dès que l'une des conditions ci-dessus cesse d'être remplie.

IX. Période de conservation

Les données à caractère personnel seront conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard de chacune des Finalités pour lesquelles elles ont été collectées, nonobstant les sauvegardes informatiques automatiques et les obligations d'archivage légales et réglementaires auxquelles PwC Luxembourg est soumis.

X. Droits des personnes concernées

Selon les limites prévues par les Lois applicables, les personnes concernées disposent du droit de :

- demander l'accès à leurs données à caractère personnel, la rectification ou l'effacement de celles-ci ou une limitation du traitement les concernant ;
- de s'opposer au traitement de leurs données à caractère personnel ; et
- du droit à la portabilité.

Si le traitement des données à caractère personnel des personnes concernées est fondé exclusivement sur le consentement des personnes concernées, les personnes concernées disposent du droit de retirer leur consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci.

Afin d'exercer les droits repris ci-dessus, les personnes concernées sont priées d'envoyer un courriel au délégué à la protection des données de PwC Luxembourg, apportant la preuve de leur identité et précisant le droit qu'elles souhaitent exercer.

Les personnes concernées disposent en outre du droit d'introduire une réclamation auprès de l'autorité de contrôle compétente, l'autorité de contrôle principale compétente pour les données à caractère personnel traitées par PwC Luxembourg étant la Commission nationale pour la protection des données (CNPD).

XI. Droit applicable et validité

Cet avis défini de façon exhaustive les engagements de PwC Luxembourg au regard du traitement des données à caractère personnel nonobstant tout autre engagement par ailleurs.

Afin de respecter les Lois applicables et de refléter adéquatement la façon dont PwC Luxembourg traite les données, le présent avis est mis à jour occasionnellement.

Le présent avis ainsi que l'ensemble des questions qui en découlent ou qui y sont liées sont soumis exclusivement au droit luxembourgeois et à la compétence des tribunaux de Luxembourg-ville.

Annexe 1
Domaines de sécurité concernés et liste des contrôles

PricewaterhouseCoopers a été soumise à une évaluation qui l'a trouvée en conformité avec les exigences en matière de management de la sécurité de l'information imposées par la norme ISO/IEC 27001:2022. Le système de management de la sécurité de l'information couvre l'ensemble des systèmes et processus d'information que PricewaterhouseCoopers utilise pour le stockage et le traitement des données des clients conformément à la Version 3.0 de la déclaration d'applicabilité datée du septembre 2023.

Chacune des sociétés membres du réseau de PwC est tenue de respecter les exigences de la politique en matière de sécurité de l'information définie, mise à jour et auditée par le centre pour la sécurité de l'information du réseau de PwC ou d'aller au-delà desdites exigences. La politique en matière de sécurité de l'information est conforme aux exigences relatives aux contrôles imposées par la Norme ISO/IEC 27002.

La présente annexe résume les engagements de PwC Luxembourg envers l'ensemble des domaines relatifs aux contrôles de sécurité définis par la Norme ISO/IEC 27002. Les contrôles de sécurité ainsi que les initiatives menées dans ce domaine ne sont pas limités aux exemples mentionnés dans le présent document qui a pour but de fournir un aperçu de la maturité de PwC Luxembourg dans le domaine de la sécurité de l'information. Les domaines détaillés ci-dessous sont liés aux objectifs et contrôles détaillés dans la Norme ISO/IEC 27002 relative aux systèmes de management de la sécurité de l'information, certaines adaptations ayant été réalisées afin de correspondre à l'environnement commercial et sécuritaire de PwC Luxembourg.

a. **La politique de sécurité** décrit le besoin de protéger nos ressources d'information et nos biens technologiques afin de garantir le respect des obligations contractuelles et réglementaires ainsi que le respect des politiques et des normes supplémentaires et des politiques en matière de sécurité mises en place au sein de PwC Luxembourg. Les contrôles comprennent notamment :

   - La politique en matière de sécurité de l'information formalisée, répondant aux exigences imposées par la Norme ISO/IEC 27002 ;
   - Un examen annuel de la politique en matière de sécurité de l'information, mené conformément au processus de gouvernance informatique défini par le réseau mondial de PwC ;
   - Un processus continu destiné à développer et à tenir à jour des politiques, normes et lignes de conduite supplémentaires ou plus détaillées établies et mises en place au sein de PwC Luxembourg. Ce processus est développé, examiné, validé et publié. Lesdites politiques, normes et lignes de conduite en matière de sécurité font l'objet d'un examen périodique afin de veiller à la protection et au maintien à jour appropriés des ressources en matière de technologie de l'information.

b. **Organisation de la sécurité de l'information.** Gestion de la sécurité au sein de PwC Luxembourg, comprenant le cadre de la sécurité de l'information applicable à l'ensemble du cabinet, l'accès des tiers à ses ressources et les exigences en matière de sécurité à respecter par les prestataires de services externalisés. Les contrôles comprennent notamment :

   - Une équipe dédiée de spécialistes de la sécurité de l'information ;
   - Un comité dédié de la sécurité de l'information, comprenant des membres clé de la direction ;
   - Un engagement formalisé de la part des cadres supérieurs envers la sécurité de l'information et la fourniture des ressources et des budgets nécessaires au respect de la stratégie en matière de sécurité de l'information ;
   - Établissement d'un diagnostic de sécurité spécifique dans le cadre du processus d'évaluation dès que des données confidentielles doivent être externalisées à des fournisseurs indépendants.

c. Gestion des actifs. Classification et sécurité des ressources et des systèmes d'information, comprenant la classification des données. Les contrôles comprennent notamment :

- Définition d'un dispositif de classification des données, communiqué à l'ensemble du personnel ;
- Établissement et mise à jour d'un inventaire de tous les biens liés aux systèmes d'information ;
- Restriction par logiciel du transfert de fichiers vers des supports amovibles à partir des ordinateurs de la société.

d. Sécurité des ressources humaines. Domaines concernant la sécurité du personnel, tels que les vérifications d'antécédents des employés, les conditions générales d'emploi, les accords de confidentialité et les formations de sensibilisation des utilisateurs. Les contrôles comprennent notamment :

- Existence d'un programme de sensibilisation à la sécurité qui attire l'attention des employés sur leur rôle et leurs responsabilités en matière de sécurité de l'information. Ce programme de sensibilisation à la sécurité comprend la formation de l'ensemble des nouveaux employés, de nombreuses communications de sensibilisation au cours de l'année ainsi que des programmes de sensibilisation particulièrement adaptés à certains rôles au sein de PwC Luxembourg ;
- Définition des responsabilités en matière de sécurité de l'information dans les descriptifs de postes ;
- Vérification des antécédents des employés comprenant leur éducation, leurs qualifications professionnelles ainsi que des vérifications relatives à leurs emplois précédents. Le personnel informatique concerné est informé directement des modifications relatives à la situation des employés (nouveaux employés, transfert/changement de poste, départ, etc.) afin de pouvoir mettre à jour ou révoquer les droits d'accès et afin qu'ils connaissent l'identité des employés tenus de rendre les biens de PwC Luxembourg en leur possession.

e. Sécurité physique et environnementale. Contrôle des accès aux bâtiments, politique en matière de bureau bien rangé, sécurité des ordinateurs portables - le tout visant globalement à garantir la protection adéquate de nos locaux commerciaux ainsi que celle des ressources d'information et des biens technologiques qu'ils contiennent. Les contrôles comprennent notamment :

- L'accès à nos locaux est contrôlé au moyen de cartes d'accès nominatives. L'ensemble des employés de PwC Luxembourg sont tenus de porter en permanence leur badge avec photo d'identité ;
- Les centres de données sont équipés de contrôles d'accès, de systèmes de détection et de suppression d'incendie, de systèmes de refroidissement ainsi que de systèmes d'alimentation électrique de secours ;
- Chaque employé de PwC Luxembourg dispose d'un casier lui étant réservé et pouvant être verrouillé au moyen d'un code de sécurité personnel ;
- Chaque employé de PwC Luxembourg dispose d'un câble de sécurité individuel avec lequel il doit verrouiller son ordinateur afin d'éviter les vols ;
- L'impression des documents est sécurisée au moyen du badge individuel (impression à la demande au moyen de la technologie « follow-me printing »).

f. Gestion des communications et des opérations. Fonctionnement et gestion sécurisés des centres de traitement de l'information. Les contrôles comprennent notamment :

- Séparation nette entre environnements de test et environnements de production ;
- Nous disposons d'un centre de données secondaire, éloigné de notre centre de données principal. Ce centre de données secondaire offre les capacités suivantes :
  - Réplication en temps réel des données avec notre centre de données principal ;
  - Ligne internet de secours ;
  - Redondance des serveurs (en ligne ou en veille, en fonction des exigences en matière de disponibilité).
- Une sauvegarde quotidienne des serveurs est effectuée sur disques et sur bandes. Un jeu des bandes de sauvegarde est encrypté et stocké sur un site distant ;
- Notre architecture internet est basée sur un modèle à 3 niveaux et est protégée par des pare-feu de réseau, des pare-feu d'applications ainsi que par des systèmes de détection et de prévention des intrusions (version réseau et version hôte). Existence d'une redondance à chaque niveau ;
- L'ensemble des ordinateurs (PC portables compris) et des serveurs sont équipés d'un logiciel antivirus géré de façon centralisée et mis à jour au moins une fois par jour (des mises à jour urgentes sont également possibles en temps réel). En outre, chaque ordinateur est équipé d'un pare-feu et d'un système de prévention des intrusions hôtes ;
- Les disques durs des ordinateurs (PC portables compris) sont complètement encryptés ;
- Pour l'échange de fichiers confidentiels, nous utilisons une plate-forme sécurisée de transferts de fichiers permettant l'authentification pour l'accès aux fichiers et le cryptage pendant les transferts de fichiers sur internet.

g. Contrôle des accès. Le contrôle des accès est nécessaire afin de garantir un accès correct et approprié à nos ressources d'information et à nos technologies sur la base d'un système de classification des données et d'attribution de rôles et de responsabilités. Les contrôles comprennent notamment :

- Le contrôle des accès sur la base des rôles des employés est en vigueur à tous les échelons de PwC Luxembourg et les rôles sont définis sur la base des fonctions occupées par les employés. Les modifications des droits d'accès sont soumises à des workflows d'approbation spécifiques, adaptés à la nature des informations pour lesquelles un accès est demandé ;
- Les employés de PwC Luxembourg ne disposent pas d'un accès privilégié sur leurs ordinateurs (ils n'ont pas de droits administrateur) ;
- L'ensemble des accès privilégiés s'effectuent grâce à un système de gestion des utilisateurs privilégiés (PUM, Privileged User Management) et ils sont enregistrés et contrôlés dans le système de gestion des informations de sécurité et des événements de sécurité de PwC (SIEM, Security Information and Event Management) ;
- Une authentification à facteurs multiples (MFA) dynamique est nécessaire pour accéder aux comptes privilégiés ;
- Un accès à distance est uniquement possible à partir des appareils de la société (authentification des appareils au moyen d'un certificat) et par l'intermédiaire d'un canal encrypté (VPN) ;
- L'accès aux applications internes à partir d'appareils mobiles est géré par l'intermédiaire d'un système sécurisé de gestion des appareils mobiles ;
- Les connexions sans fil à notre réseau interne sont uniquement autorisées à partir d'ordinateurs de la société (authentification des appareils au moyen d'un certificat).

h. Acquisition, développement et maintenance des systèmes d'information. Développement et maintenance continue des systèmes d'information afin de veiller à ce que des contrôles de sécurité appropriés soient intégrés à la phase de définition des concepts. Les contrôles comprennent notamment :

- Tout changement relatif à la mise en production est soumis à un processus de validation supervisé par notre comité consultatif sur les changements ;

- Une évaluation des risques en matière de sécurité de l'information est obligatoire dans le cadre de chaque projet informatique. Ces évaluations des risques conduisent à des recommandations de mesures liées à la sécurité et elles sont examinées et validées par le gestionnaire de projet, le directeur informatique, le propriétaire de l'information, le responsable de la sécurité, le sponsor du projet ainsi que, le cas échéant, par un responsable de la gestion des risques ;
- Toute nouvelle application est soumise à un essai d'intrusion préalable à la mise en production, à moins que l'évaluation des risques en matière de sécurité de l'information n'en dispose autrement. Les essais d'intrusion sur les applications web accessibles à partir d'internet et hébergeant des informations confidentielles sont réalisés par un tiers indépendant et sont reconduits chaque année ;
- Des analyses de vulnérabilité sont réalisées mensuellement sur nos serveurs ;
- L'installation de logiciels n'est possible que suite à l'obtention d'une autorisation appropriée. L'utilisation de nouveaux logiciels est soumise à une évaluation de sécurité préalable à leur approbation.
- Les solutions de type logiciel à la demande (SaaS, software-as-a-service) font l'objet d'une analyse de sécurité et les fournisseurs de ces solutions font également l'objet d'une évaluation au moyen d'un processus de gestion des risques tiers.

i. **Gestion des incidents relatifs à la sécurité de l'information.** Contrôles destinés à communiquer les incidents liés à la sécurité de l'information et les faiblesses associées aux systèmes d'information de façon à permettre la prise de mesures correctives dans les temps. Les contrôles comprennent notamment :

- Existence d'outils de détection d'incidents potentiels dans les fichiers de journalisation et présence de notifications automatiques ;
- Conduite d'examens périodiques des fichiers de journalisation des dispositifs de sécurité afin de détecter des incidents potentiels ;
- Établissement de rapports périodiques relatifs aux incidents liés à la sécurité de l'information ; ceci comprend la transmission aux représentants de la gestion des risques de chaque ligne d'activité ;
- Existence de procédures particulières pour la communication interne et externe des incidents.

j. **Gestion de la continuité des activités.** Il s'agit de la planification de la continuité d'exploitation et de la reprise après sinistre sur la base d'accords sur le niveau de service et d'objectifs en matière de délais de rétablissement, le tout visant globalement à minimiser les impacts sur nos activités en cas de sinistre. Les contrôles comprennent notamment :

- Des mesures de redondance sont en place pour l'ensemble de nos systèmes et de nos applications, en fonction des exigences commerciales ;
- Des tests périodiques sont réalisés afin de garantir l'efficacité de nos mesures de redondance ;
- Nous disposons d'un centre de données secondaire et distant qui contient une réplication de nos données et de nos systèmes ;
- Nos plans de continuité d'exploitation et nos plans de reprise après sinistre font l'objet d'un examen et d'une mise à jour périodiques ainsi qu'après chaque changement important.

k. **Conformité.** Il s'agit des contrôles destinés à mesurer et à surveiller le respect par PwC Luxembourg et par ses systèmes des politiques de PwC ainsi que d'autres normes de sécurité pertinentes. Les contrôles comprennent notamment :

- Nos politiques, procédures, processus et systèmes font l'objet d'un audit régulier par le centre pour la sécurité de l'information du réseau de PwC ;
- Notre équipe d'avocats et de juristes spécialisés intervient dans le cadre de l'examen des contrats conclus avec des tiers et de celui des politiques et procédures appropriées.

Avertissement

Annexe 1
Domaines de sécurité concernés et liste des contrôles

PwC désigne le réseau des sociétés membres de PwC International Limited, chacune d'elles constituant une entité juridique autonome. Pour de plus amples renseignements sur PwC, veuillez consulter www.pwc.com/structure. Le présent document vise uniquement à fournir un aperçu très succinct des mesures en matière de sécurité des systèmes d'information mises en place afin de contribuer à protéger tant les informations que l'infrastructure et les applications informatiques de PwC Luxembourg.

1 PwC Luxembourg

PricewaterhouseCoopers
Une société coopérative de droit luxembourgeois
2, rue Gerhard Mercator, B.P. 1443, L-1014 Luxembourg
T : +352 494848 1, www.pwc.lu

Cabinet de révision agréé. Expert-comptable (autorisation gouvernementale n°10028256)
R.C.S. Luxembourg B 65 477 - TVA LU25482518

PwC Regulated Solutions
Une société à responsabilité limitée de droit luxembourgeois
2, rue Gerhard Mercator, B.P. 1443, L-1014 Luxembourg
T : +352 494848 1, https://www.pwc.lu/en/pwc-regulated-solutions.html

R.C.S. Luxembourg B 47205 - capital social : 500 000 € - TVA LU15947475
Professionnel du secteur financier - autorisation d'établissement n° 08/17
Professionnel du secteur de l'assurance

PricewaterhouseCoopers Training Administration Service Centre
A Luxembourg société à responsabilité limitée
rue Gerhard Mercator, B.P. 1443, L-1014 Luxembourg
T : +352 494848 1, www.pwc.lu

PricewaterhouseCoopers Academy S.à r.l.
2 rue Gerhard Mercator, B.P. 1443, L-1014 Luxembourg
T : +352 494848-4040, www.pwcacademy.lu

Organisme de formation professionnelle continue (autorisation gouvernementale n°123773)
R.C.S. Luxembourg B 66 026 - capital social : 12 500 € - TVA LU17613706

2 Délégué à la protection des données

PwC Luxembourg a désigné un délégué à la protection des données qui peut être contacté à l'adresse suivante : lu-data-protection-office@pwc.lu

L'adresse suivante est disponible pour faciliter l'exercice des droits des personnes concernées en vertu des articles 15 à 22 du règlement général sur la protection des données : www.pwc.lu/dataprotection-contact.