ADDENDA SUR LA SÉCURITÉ DES DONNÉES DU SERVICE OPENAIR

En ce qui concerne le service infonuagique fourni dans le Formulaire d'estimation ou de commande applicable (le « service OpenAir »), Oracle maintient des protections administratives commercialement raisonnables conçues pour la protection, la confidentialité et l'intégrité des données du client. Toutes ces protections sont proportionnelles à l'importance des données du client étant protégées, mais en aucun cas elles ne sont moindres que les protections utilisées par Oracle pour protéger ses propres renseignements ou données d'importance similaire, ou selon les exigences de la loi en vigueur. À la date d'entrée en vigueur du Formulaire d'estimation ou de commande applicable, lesdites protections sont décrites ci-dessous dans le présent addenda[1]; dans la mesure cependant où le client reconnaît et accepte que lesdites protections décrites dans le présent addenda ne sont pas complètes et qu'elles peuvent changer pendant la durée du Formulaire d'estimation de commande applicable, car les vérifications de sécurité de tiers, les normes de conformité et/ou les certifications applicables évoluent dans le temps, dans la mesure où lesdits changements aux protections ne réduisent pas de manière importante la sécurité générale du service OpenAir pendant la durée du Formulaire d'estimation ou de commande applicable. En ce qui concerne la durée de la convention, Oracle se conforme à toutes les obligations concernant les données du client en vertu du Formulaire d'estimation ou de commande applicable, y compris, sans s'y limiter, les obligations d'Oracle concernant le maintien de protections commercialement raisonnables, comme fournies aux présentes.

1. Politique de sécurité. Oracle possède et gère une politique de sécurité pour son organisation de sécurité, qui exige une formation sur la sécurité et sur la confidentialité dans le cadre d'un groupe de formations destinées au personnel de sécurité Oracle, comme l'indique la documentation de certification ISO 27001 d'Oracle.
2. Organisation de la sécurité Oracle. Oracle possède et continue à posséder une organisation dédiée à la sécurité responsable de la surveillance continue de l'infrastructure de sécurité Oracle, de l'examen des produits et services Oracle et des réponses à des incidents de sécurité.
3. Stockage et gestion des données. Le support de stockage ou tout équipement ayant une capacité de stockage, y compris les supports mobiles utilisés pour stocker les données du client, sont sécurisés et renforcés conformément aux pratiques standards du secteur. Le maintien par Oracle d'une politique raisonnable de gestion des biens pour gérer le cycle de vie (mise en service, exploitation, entretien, gestion, modification, réparation et mise hors service/élimination) des supports en question. Les supports mis hors service, qui contiennent des données du client, sont détruits conformément au NIST 800-88 au niveau modéré de sensibilité (ou selon une norme similaire de destruction des données).
4. Transmission de données. Oracle utilise des protocoles robustes de cryptographie et de sécurité conformes aux normes du secteur, comme indiqué dans la documentation des Guides de l'utilisateur pour le service.
5. Gestion des modifications. Oracle maintient une politique de gestion des modifications pour assurer le contrôle des modifications de l'organisation, des processus commerciaux, des installations et des systèmes de traitement des informations qui ont un impact sur la sécurité des informations.
6. Systèmes d'exploitation de serveurs. Les serveurs Oracle utilisent une mise en œuvre de systèmes d'exploitation, renforcée et personnalisée pour le service. Oracle gère une politique de protection des correctifs établissant des priorités basées sur le risque.
7. Gestion des privilèges et du contrôle de l'accès. Oracle utilise des systèmes et des processus pour limiter l'accès physique et logique en fonction de privilèges minimaux et de la séparation des tâches pour assurer un accès aux données critiques uniquement par le personnel Oracle autorisé.
8. Comptes d'utilisateurs. Le client contrôle la création, la suppression et la suspension des rôles d'utilisateurs dans le service, comme l'indique la documentation des Guides de l'utilisateur du service.
9. Politique de mot de passe. Comme indiqué dans les Guides de l'utilisateur pour le service, le client peut appliquer ses propres mots de passe et politiques d'authentification par l'entremise de paramètres de politique configurables du service et lorsqu'il utilise une fonctionnalité de signature unique dans le service.
10. Exigences de sécurité de la connectivité du réseau. Oracle protège son infrastructure par de multiples niveaux de périphériques réseau sécurisés.
11. Vérifications et certifications. Les vérifications et certifications de sécurité suivantes sont pertinentes pour le service OpenAir, comme indiqué ci-dessous :
    a. Attestation du rapport SOC. L'American Institute of CPAs (AICPA) a établi des cadres de travail pour les contrôles de l'organisation et du système (SOC ou System and Organization Controls) afin d'évaluer et de produire des rapports sur l'efficacité des contrôles d'un organisme de service qui répondent aux besoins particuliers d'un utilisateur. En ce qui concerne le service OpenAir, Oracle doit assurer la production de rapports annuels d'attestation par des tiers conformément à l'AICPA et à l'IFAC Standards for Assurance Engagements :

[1]Pour éviter toute confusion, les protections indiquées dans le présent addenda ne s'appliquent à aucune application de tiers et à aucun service facultatif commandé ou activé ultérieurement par le client et qui sont assujettis à des conditions différentes.

i. Oracle doit assurer la production d'un rapport annuel SOC 1 / ISAE 3402 Type II.

ii. Oracle doit assurer la production d'un rapport annuel SOC 2 Type II pour les attributs de sécurité, de disponibilité et de confidentialité.

iii. Tout résultat important qui entraîne une opinion avec réserve dans les rapports SOC fera l'objet d'une réponse rapide avec développement et mise en œuvre d'un plan de mesures correctives par la direction d'Oracle.

b. ISO 27001. ISO 27001 est une norme internationale dominante publiée par l'Organisation internationale de normalisation (ISO) et la Commission électronique internationale (IEC) pour la mesure de systèmes de gestion de la sécurité de l'information (ISMS ou information security management systems). Cette norme précise les exigences d'établissement, de mise en œuvre, d'exploitation, de surveillance, de revue, de gestion et d'amélioration d'un ISMS documenté.

Oracle doit assurer l'exécution d'une vérification de certification par un tiers de l'ISMS d'Oracle par rapport aux exigences de la norme ISO 27001.

c. Jusqu'à une fois par année, le client peut soumettre à Oracle une demande de copie finale des rapports suivants : a) SOC 1 / ISAE 3402 Type II; b) SOC 2 Type II; et (c) certificat et déclaration d'applicabilité (SOA) ISO 27001. Tous les rapports, certificats et documents connexes fournis par Oracle en lien avec la présente section sont réputés être des renseignements confidentiels d'Oracle.

d. Si des vérifications, des normes et/ou des certifications de tiers similaires sont proposées à l'avenir, Oracle peut choisir de les exécuter et/ou d'obtenir une certification de telles normes établies dans le secteur, selon le choix d'Oracle, au lieu de celles indiquées dans la présente section.

12. Environnement du centre de données et sécurité physique. Les informations qui suivent présentent une description générale des divers environnements de centre de données Oracle et des efforts visant à assurer leur sécurité physique.

a. Personnel affecté à la sécurité physique. Chaque centre de données Oracle est doté de personnel de sécurité sur place et est surveillé par un organisme de sécurité responsable des fonctions continues de la sécurité physique.

b. Procédures d'accès de sécurité physique. Des procédures formelles d'accès sont en place pour permettre un accès physique aux centres de données.

c. Dispositifs de sécurité physique. Les centres de données utilisent des systèmes de contrôle d'accès électronique liés à un système d'alarme. Les activités non autorisées et les tentatives d'accès ayant échoué sont consignées par le système de contrôle de l'accès et font l'objet d'une enquête selon le cas.

d. Redondance. Les centres de données Oracle sont conçus pour la résilience et la redondance. La redondance vise à minimiser l'impact des défaillances communes de l'équipement et des risques environnementaux. Les systèmes d'infrastructure ont été conçus pour éliminer les points de défaillance unique. En outre, Oracle a mis en place une procédure de récupération des données du client et de rétablissement du service vers un centre de données secondaire dans le cas où le centre de données principal est déclaré par Oracle comme inopérable à la suite d'une catastrophe.

e. Alimentation électrique. Les systèmes d'alimentation électrique du centre de données sont conçus pour permettre une redondance et un entretien complets, sans interruption des opérations continues. Une alimentation électrique de réserve est fournie par plusieurs mécanismes, y compris l'utilisation de batteries et de groupes électrogènes. L'alimentation électrique de réserve est conçue pour fournir une protection d'alimentation fiable et cohérente, pendant les réductions de tensions pour l'entretien, les pannes d'électricité, les surtensions, les sous-tensions et les conditions de dépassement des limites de tolérance de fréquence.

13. Évaluation des risques. Oracle effectue chaque année une évaluation des risques du service OpenAir. Cette évaluation inclut une évaluation des risques dans les domaines de la confidentialité, de l'intégrité et de l'accessibilité des données du client qui résident dans le service OpenAir, de même qu'un plan, documenté dans sa politique de sécurité, pour corriger ou atténuer ces risques.

14. Utilisation des services. Le service OpenAir ne peut pas être livré à des utilisateurs au Venezuela ou faire l'objet d'un accès par ceux-ci; et le service OpenAir ou tout résultat des services ne peuvent pas être utilisés pour l'avantage de toute personne ou entité au Venezuela y compris, sans s'y limiter, le gouvernement du Venezuela.

15. Définitions.

Le terme « **centre de données principal** » désigne le centre de données principal dans lequel sont stockées les données du client.

Le terme « **protections** » désigne les protections physiques et techniques.

Le terme « **incidents de sécurité** » désigne une divulgation non autorisée effective ou un doute raisonnable d'Oracle selon lesquels une divulgation non autorisée des données du client, qui contiennent des renseignements personnels non cryptés, a eu lieu pour une personne ou une entité non autorisée.

[1]Pour éviter toute confusion, les protections indiquées dans le présent addenda ne s'appliquent à aucune application de tiers et à aucun service facultatif commandé ou activé ultérieurement par le client et qui sont assujettis à des conditions différentes.