ADDENDA SUR LA SÉCURITÉ DES DONNÉES DU SERVICE NETSUITE

En ce qui concerne le service infonuagique fourni dans le Formulaire d'estimation ou de commande applicable (le « service NetSuite »), 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. En ce qui concerne 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 ou de commande applicable, car les vérifications de sécurité par des tiers, les normes de conformité et/ou les certifications applicables évoluent et changent au cours du temps, dans la mesure où lesdits changements aux protections ne réduisent pas de façon importante la sécurité générale du service NetSuite pendant la durée du Formulaire d'estimation ou de commande applicable. En ce qui concerne la durée de la convention, Oracle respecte 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 en matière de gestion des protections commercialement raisonnables, comme indiqué 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 des certifications ISO 27001 et PCI DSS 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 et 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, comme :

    a. 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.

    b. Les supports mis hors service, qui contiennent des données du client, sont détruits conformément au NIST 800-88 révision 2 au niveau modéré de sensibilité (ou selon une norme similaire de destruction des données).

    c. Les données du client sont segmentées de manière logique par rapport aux données d'Oracle et à celles d'autres clients d'Oracle.

    d. Dans le service NetSuite, les champs de bases de données désignés pour des renseignements sur les données de carte de crédit et les numéros de sécurité sociale sont cryptés et Oracle ne traite pas de telles données du client dans des tests, pour un développement ou dans des environnements de non-production.

4. Transmission des données. L'accès du client au service NetSuite a lieu par l'entremise d'un protocole de communication sécurisé spécifié par Oracle. Oracle utilise une cryptographie robuste et des protocoles de sécurité conformes aux normes du secteur, comme indiqué dans la documentation des Guides de l'utilisateur pour le service NetSuite.

5. Réponse à un incident. Oracle surveille plusieurs canaux de communication pour y détecter des incidents connus et l'équipe de sécurité Oracle réagit promptement à ces incidents. Si un incident de sécurité survient, Oracle : (i) avise le client conformément aux obligations d'Oracle en vertu de la loi en vigueur ou des exigences réglementaires, dans la mesure où une loi en vigueur sur la violation de sécurité s'applique à cet incident de sécurité; et (ii) effectue un test de pénétration après avoir mis en œuvre des mesures correctives, le cas échéant, avec un sommaire des résultats de test qui est fourni au client, et ces résultats sont réputés être des renseignements confidentiels d'Oracle.

    Le plan de réponse aux incidents d'Oracle est décrit plus en détail et vérifié dans le rapport SOC 1 / ISAE 3402 Type II d'Oracle et dans le rapport SOC 2 Type II, et il est vérifié plus avant dans le processus de revue de certification annuelle ISO 27001 s'appliquant au service NetSuite. Les incidents liés aux renseignements personnels sont gérés conformément aux dispositions indiquées dans la Convention sur le traitement des données Oracle.

6. 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 les informations qui ont un impact sur la sécurité des informations.

[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.

7. Systèmes d'exploitation de serveurs. Les serveurs Oracle utilisent une mise en œuvre de système d'exploitation, renforcée et personnalisée pour le service NetSuite. Oracle gère une politique de gestion des correctifs établissant des priorités basées sur le risque.

8. 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.

9. Comptes d'utilisateurs. Le client contrôle la création, la suppression et la suspension des rôles d'utilisateurs dans le service NetSuite, comme l'indique la documentation des Guides de l'utilisateur du service NetSuite. Le service NetSuite permet au client d'effectuer des fonctions administratives.

10. Contrôles des responsabilités et de la politique d'Oracle. Oracle met en œuvre des mesures pour assurer que le traitement des données du client est exécuté uniquement selon les instructions fournies par le client.

11. Politique de mot de passe. Comme indiqué dans les Guides de l'utilisateur pour le service NetSuite, le client peut appliquer ses propres mots de passe et politiques d'authentification par l'entremise de paramètres de politique configurables du service NetSuite et lorsqu'il utilise une fonctionnalité de signature unique dans le service NetSuite.

12. Exigences de sécurité de la connectivité du réseau. Oracle protège son infrastructure par de multiples niveaux de périphériques réseau sécurisés. Tout accès à distance aux environnements des services NetSuite par le personnel d'Oracle ayant accès aux données du client, doit être effectué par une ou par plusieurs des méthodes suivantes : réseau privé virtuel, authentification à facteurs multiples, authentification mutuelle, cote de confiance du client, ou d'autres méthodes d'authentification qui permettent un niveau de sécurité égal ou supérieur.

13. Vérifications et certifications. Les vérifications et certifications de sécurité suivantes sont pertinentes pour le service NetSuite, comme indiqué ci-dessous :

    a. PCI DSS. Les Normes de sécurité des données de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard ou PCI DSS) sont des normes de sécurité des renseignements à l'échelle mondiale pour les organisations qui gèrent des cartes de crédit de marque comme Visa, Master Card, American Express, etc. Les normes de la PCI sont mandatées par les marques de cartes et gérées par le Payment Card Industry Security Standards Council. Pendant la durée, Oracle maintient la conformité à la PCI DSS au niveau 1 du niveau de prestataire de service pour les parties du service NetSuite Oracle qui stocke, traite et transmet des données de carte de crédit. (Tous les changements effectués aux services Oracle par ou au nom du client peuvent avoir une incidence sur la conformité du client aux exigences de la PCI DSS et le client assume l'entière responsabilité de s'assurer que tous ces changements soient conformes aux exigences de la PCI DSS.)

    b. 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 NetSuite, 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 :

        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.

    c. ISO 27001. ISO 27001 est une norme internationale dominante publiée par l'Organisation internationale de normalisation (ISO) et la Commission électronique internationale (IEC) qui mesure les 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.

    d. 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.

[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.

e. 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.

f. Si le client a fait l'acquisition de NetSuite New Starter Edition, toute cette section ne s'applique pas à l'achat par le client de ces services NetSuite New Starter Edition.

14. 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. Le plan de reprise après sinistre préparé par Oracle est décrit dans le rapport SOC 1 / ISAE 3402 Type II d'Oracle et vérifié plus à fond dans le rapport SOC 2 Type II d'Oracle et dans le processus d'évaluation de certification annuelle ISO 27001. Les centres de données 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. 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. Oracle met en œuvre des mesures pour assurer la protection des données du client contre une destruction ou une perte accidentelle.

    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, sans interruption 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.

15. Évaluation des risques. Oracle effectue chaque année une évaluation des risques du service NetSuite. 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 NetSuite, de même qu'un plan, documenté dans sa politique de sécurité, pour corriger ou atténuer ces risques.

16. Gestion des renseignements personnels. Oracle traite les données personnelles dans le cadre d'une disposition de ses services conformément à sa convention sur les services conclue avec le client et assume la responsabilité de se conformer à ses obligations respectives en vertu des lois en vigueur sur la protection des données. Gestion et traitement internes des renseignements personnels. Oracle met en œuvre et gère des mesures de sécurité organisationnelles et techniques pertinentes conçues pour prévenir la destruction accidentelle ou illégale, la perte, la modification, la divulgation non autorisée de renseignements personnels ou un accès non autorisé à ces renseignements.

17. Utilisation des services. Le service NetSuite ne peut pas être livré à des utilisateurs au Venezuela ou faire l'objet d'un accès par ceux-ci; et le service NetSuite 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.

18. 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 « incident de sécurité » désigne une divulgation non autorisée actuelle ou un doute raisonnable d'Oracle selon lesquels une divulgation non autorisée des données du client, qui contiennent des renseignements non cryptés, a eu lieu pour une personne ou une entité non autorisée.

Le terme « **renseignements personnels** » a le même sens que le terme « données personnelles », « renseignements permettant d'identifier une personne » ou un terme équivalent employé dans la législation en vigueur sur la protection des données.

[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.