ADDENDA SUR LA SÉCURITÉ DES DONNÉES DE NETSUITE CPQ

En ce qui concerne le service infonuagique de NetSuite CPQ fourni dans le Formulaire d'estimation ou de commande applicable, 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 infonuagique NetSuite CPQ 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 pour le personnel de sécurité Oracle qui prend en charge le service infonuagique NetSuite CPQ.

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 infonuagique NetSuite CPQ, 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 de données. 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 d'Oracle à un incident est décrit plus en détail dans le rapport SOC 1 / ISAE 3402 Type II et dans le rapport SOC 2 Type II d'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 des informations qui ont un impact sur la sécurité des informations.

7. Systèmes d'exploitation de serveurs. Les serveurs Oracle utilisent une mise en œuvre de système d'exploitation, renforcée et personnalisée pour le service infonuagique NetSuite CPQ. 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. 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.

[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.

10. Exigences de sécurité de la connectivité du réseau. Oracle protège son infrastructure par de multiples niveaux de périphériques réseau sécurisés .

11. 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 d'Oracle est décrit plus en détail dans le rapport SOC 1 / ISAE 3402 Type II et dans le rapport SOC 2 Type II d'Oracle. 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.

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

13. Gestion des données personnelles. 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. Lors de la gestion et du traitement des données personnelles, 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 données personnelles ou un accès non autorisé aux données personnelles.

14. Utilisation des services. Le service infonuagique NetSuite CPQ ne peut pas être livré à des utilisateurs au Venezuela ou faire l'objet d'un accès par ceux-ci; et le service infonuagique NetSuite CPQ 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 « **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 « **données personnelles** » a le même sens que le terme « informations 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.