MESURES TECHNIQUES ET ORGANISATIONNELLES

(POUR LES CLIENTS)

Ces Mesures techniques et organisationnelles (les « **MTO** ») font partie intégrante de l'Accord/Avenant/Pièce jointe/Programme/Section relatif(ve) au Traitement des Données à caractère personnel (ou tout autre document équivalent, selon le cas) entre Avaya (y compris ses filiales internationales) et le Client (y compris ses filiales internationales, le cas échéant), qui les intègrent par renvoi.

1. Contrôle de l'accès aux locaux

Avaya empêchera l'accès physique à l'équipement de traitement des Données à caractère personnel par des personnes non autorisées comme suit :

1.1. Avaya mettra en place et maintiendra des mesures de sécurité physiques afin d'éviter tout accès non autorisé. Cette protection sera assurée par les mesures suivantes :

1.1.1. un système de contrôle d'accès électronique avec une durée de conservation des journaux de 90 jours ;

1.1.2. un enregistrement vidéo 24 heures/24 et 7 jours/7 avec une durée de conservation des journaux de 30 jours ; et

1.1.3. des alarmes antivol et de détection des intrusions, ou le recours à des agents de sécurité dans les locaux.

1.2. Avaya limitera l'accès aux différentes zones de ses locaux selon les fonctions, et renouvellera régulièrement la validité d'accès des titulaires.

1.3. Avaya mettra en place des mesures de sécurité destinées au personnel et aux visiteurs afin d'éviter tout accès non autorisé, assurées par les moyens suivants :

1.3.1. Le personnel doit présenter une pièce d'identité ;

1.3.2. Les visiteurs doivent s'enregistrer ;

1.3.3. Les visiteurs doivent être accompagnés par un membre du personnel dans les limites du raisonnable ; et

1.3.4. Les visiteurs doivent porter un badge permettant de les identifier facilement en tant que visiteurs.

2. Contrôle de l'accès à l'utilisation du système

Afin d'éviter tout accès logique à son équipement de traitement des Données à caractère personnel par des personnes non autorisées, Avaya mettra en place et maintiendra les mesures suivantes :

2.1. Avaya n'accordera l'accès à l'équipement de traitement des Données à caractère personnel qu'aux personnes en mesure de

2.1.1. présenter un identifiant d'utilisateur unique autorisant l'accès avec un processus d'autorisation formel, et

2.1.2. un mot de passe unique comportant les caractéristiques suivantes :

2.1.2.1. un mot de passe complexe, composé de huit caractères et de trois types de caractères sur quatre ;

2.1.2.2. une durée de vie maximale du mot de passe de quatre-vingt-dix jours ; et

2.1.2.3. un verrouillage du compte en cas d'échec des tentatives.

2.2. Avaya accordera l'accès aux personnes sur la base de leur fonction en respectant les critères suivants :

2.2.1. accès selon le poste ;

2.2.2. accès selon le principe du moindre privilège ; et

2.2.3. accès sur la base du « besoin de savoir » uniquement.

2.3. L'écran des points de terminaison sera automatiquement verrouillé après 20 minutes d'inactivité.

2.4. Avaya consignera l'accès à l'équipement de traitement des données.

2.5. Avaya utilisera une authentification multi-facteurs pour le réseau privé virtuel (VPN) d'Avaya dans le cas de l'accès à distance.

2.6. Avaya mettra en place et maintiendra une administration centralisée des utilisateurs.

2.7. Avaya chiffrera les points de terminaison fournis par la société elle-même.

3. Contrôle de l'accès aux Données à caractère personnel

Avaya empêchera tout accès logique aux Données à caractère personnel par des personnes non autorisées, en mettant en place et en maintenant des mesures adéquates destinées à éviter toute lecture, copie, modification ou suppression non autorisées des supports contenant les Données à caractère personnel, tout enregistrement non autorisé dans la mémoire, et toute lecture, modification ou suppression des Données à caractère personnel enregistrées. Cette protection sera assurée par les mesures suivantes :

3.1. Avaya n'accordera l'accès aux Données à caractère personnel qu'aux personnes en mesure de présenter :

3.1.1. un identifiant d'utilisateur unique autorisant l'accès avec un processus d'autorisation formel, et

3.1.2. un mot de passe unique comportant les caractéristiques suivantes :

3.1.2.1. un mot de passe complexe, composé de huit caractères et de trois types de caractères sur quatre ;

3.1.2.2. une durée de vie maximale du mot de passe de quatre-vingt-dix jours ; et

3.1.2.3. un verrouillage du compte en cas d'échec des tentatives.

3.2. Avaya accordera l'accès aux Données à caractère personnel sur la base de la fonction des employés, en respectant les critères suivants :

3.2.1. accès selon le poste ;

3.2.2. accès selon le principe du moindre privilège ; et

3.2.3. accès sur la base du « besoin de savoir » uniquement.

3.3. L'écran des points de terminaison sera automatiquement verrouillé après 20 minutes d'inactivité.

3.4. Avaya consignera l'accès à l'équipement de traitement des données.

3.5. Avaya conservera des listes de contrôle d'accès (LCA).

3.6. Avaya réalisera des sauvegardes et des extractions de données à l'aide de supports de stockage pour les sauvegardes sécurisés et les tests sur les sauvegardes.

3.7. Avaya mettra en place et maintiendra un programme de gestion des modifications du contrôle d'accès formel.

3.8. Avaya mettra en place et maintiendra des normes et des politiques internes, notamment en matière de sécurité, au niveau de l'entreprise comme de l'unité opérationnelle.

3.9. Avaya réalisera des formations obligatoires régulières sur le thème de la protection des données à caractère personnel, et surveillera et imposera la participation à ces formations.

3.10. Avaya mettra en place et maintiendra des programmes antivirus, suivis et mis à jour de façon centralisée, et réalisera des scans antivirus réguliers.

3.11. Avaya réalisera une suppression et/ou une élimination sécurisée des données.

4. Contrôle de la transmission

Avaya empêchera tout accès non autorisé aux Données à caractère personnel, en mettant en place des canaux de communication sécurisés et des enregistrements comme suit :

4.1. Avaya utilisera un VPN avec une authentification multi-facteurs pour l'accès à distance.

4.2. Avaya utilisera des pare-feu présentant les fonctionnalités et processus suivants :

4.2.1. une inspection d'état ;

4.2.2. la mise en œuvre de règles d'accès paramétrées sur un refus par défaut, sauf dans le cas d'une validation explicite des règles d'accès ;

4.2.3. un accès selon le poste et le principe du moindre privilège, sur la base du « besoin de savoir » ;

4.2.4. un enregistrement et une alerte lors de l'accès ; et

4.2.5. une révision annuelle des règles du pare-feu.

4.3. Avaya utilisera un e-mail chiffré si le Client a également activé cette fonction, en utilisant le protocole Sécurité de la couche transport (TLS).

4.4. Avaya mettra en place et maintiendra des normes et des politiques de sécurité au niveau de l'entreprise comme de l'unité opérationnelle.

5. Contrôle des saisies

Avaya garantira la possibilité de vérifier et de déterminer si les Données à caractère personnel ont été ajoutées, modifiées ou supprimées de l'équipement de traitement des Données à caractère personnel, et la personne qui en est à l'origine, comme suit :

5.1. Les personnes jouissant d'un accès aux données à caractère personnel auront besoin d'un identifiant utilisateur unique et d'une autorisation d'accès.

5.2. Avaya mettra en place et maintiendra des normes et des politiques de sécurité au niveau de l'entreprise comme de l'unité opérationnelle.

5.3. L'équipement de traitement des Données à caractère personnel disposera de fonctionnalités d'enregistrement.

5.4. Avaya n'accordera l'accès aux Données à caractère personnel que selon la fonction des employés, en respectant les critères suivants :

5.4.1. accès selon le poste ;

5.4.2. accès selon le principe du moindre privilège ; et

5.4.3. accès sur la base du « besoin de savoir ».

6. Contrôle de l'organisation

6.1. Avaya veillera à ce que, dans le cas d'un traitement des données commandité, les Données à caractère personnel soient traitées en se conformant strictement aux instructions du Client.

6.2. Le Client fournira des instructions claires à Avaya concernant la portée du traitement des Données à caractère personnel et Avaya veillera à respecter ces instructions.

7. Contrôle de la disponibilité

Avaya évitera toute destruction ou perte accidentelle des Données à caractère personnel, en mettant en place les mesures adéquates comme suit :

7.1. Avaya mettra en place et maintiendra un système d'alimentation sans coupure, des détecteurs de fumée et alarmes incendie, des dispositifs d'extinction des incendies, des générateurs, des systèmes de refroidissement et un sol surélevé.

7.2. Avaya mettra en place et maintiendra un plan de reprise d'activité, et en effectuera la révision et le test chaque année.

7.3. Avaya mettra en place et maintiendra une stratégie et des procédures de sauvegarde.

7.4. Avaya mettra en place et maintiendra des programmes antivirus ainsi que des systèmes de pare-feu.

8. Contrôle de la séparation des données

Avaya mettra en place et maintiendra les mesures adéquates afin de permettre un traitement distinct des données collectées à différentes fins, comme suit :

8.1. Avaya séparera les Données à caractère personnel de ses différents clients en enregistrant les Données à caractère personnel dans des bases de données séparées au niveau logique.

8.2. Avaya séparera également les données de test et les données réelles.

- FIN DES MTO -