La traduction ci-dessous est fournie à titre d'information uniquement. En cas de divergence, d'incohérence ou de conflit entre cette traduction et la dernière version en anglais mise à jour (y compris en raison de délais de traduction), la version anglaise prévaudra.

POLITIQUE DE SÉCURITÉ DES PRESTATAIRES D'AMAZON

Dernière mise à jour : septembre 11, 2024

1. **CHAMP D'APPLICATION.** Le Fournisseur se conformera à ces exigences en matière de sécurité (la « Politique de sécurité »). La présente Politique de sécurité ne limite aucune autre obligation contractuelle ou légale du Prestataire. En cas de conflit entre la présente Politique de sécurité et d'autres accords entre le Prestataire et Amazon, le Prestataire se conformera aux exigences plus restrictives qui protègent mieux les Informations Amazon.

2. **MISES À JOUR.**

2.1 Amazon peut apporter des mises à jour commercialement raisonnables à la présente Politique de sécurité de temps à autre, qui entreront en vigueur 30 jours après la date de « Dernière mise à jour » de la présente Politique de sécurité. Le Prestataire accepte d'être lié par la Politique de sécurité mise à jour une fois que les mises à jour entrent en vigueur.

2.2 Si le Prestataire souhaite recevoir un préavis desdites mises à jour avant qu'elles ne prennent effet, il peut s'abonner pour recevoir des notifications de mise à jour en utilisant le formulaire d'abonnement fourni sur la page Web de la présente Politique de sécurité. Le Prestataire veillera à ce que toutes ses coordonnées fournies pour l'abonnement à l'avis de mise à jour soient mises à jour et exactes à tout moment. Le Prestataire sera réputé avoir reçu tout avis de mise à jour lorsqu'il est envoyé par courrier électronique, qu'il ait ou non effectivement reçu l'avis de mise à jour.

3. **FINALITÉ AUTORISÉE.**

3.1 **Autorisation expresse**. Le Prestataire ne peut traiter que les Informations Amazon expressément autorisées en vertu du Contrat et uniquement aux fins de fournir les produits ou services prévus par le Contrat (l'« Objectif autorisé »).

3.2 **Conservation des données.** Le Prestataire conservera les Informations Amazon uniquement aux fins de la Finalité autorisée, et aussi longtemps que nécessaire pour celle-ci.

3.3 **Limitations expresses**. Le Prestataire s'abstiendra autrement : (a) de traiter toute Information Amazon, même si elle est anonymisée ; (b) de transférer, louer, troquer, échanger, vendre, prêter, louer à bail ou distribuer de toute autre manière ou mettre à la disposition d'un tiers les Informations d'Amazon, même anonymisées ; ou (c) de développer, former ou améliorer tout modèle d'Intelligence artificielle (IA) ou d'Apprentissage automatique (ML) à l'aide des Informations Amazon, même anonymisées.

4. **EXIGENCES DE SÉCURITÉ MINIMALES**. Le Prestataire maintiendra des mesures de protection physiques, administratives et techniques conformes aux meilleures pratiques du secteur (y compris les normes 27001 et 27002 de l'Organisation internationale de normalisation (« ISO »), le Cadre de cybersécurité de l'Institut national des normes et de la technologie (« NIST »), ou d'autres
des normes similaires). Les garanties maintenues par le Prestataire incluront les exigences minimales décrites ci-dessous dans les Sections 4.1 à 4.18.

4.1 **Programme écrit concernant la sécurité des informations.** Le Prestataire disposera d'un programme écrit de sécurité des informations qui : (a) comprend des politiques, des procédures et des normes appropriées répondant aux exigences énoncées dans la présente Politique de sécurité ; (b) désigne un point de contact en matière de sécurité responsable de la communication et de la gestion des problèmes de sécurité (y compris les incidents de sécurité) ; (c) est revu au moins une fois par an et mis à jour si nécessaire ; et (d) s'applique au Personnel. Le Prestataire surveillera et fera appliquer son programme de sécurité des informations et traitera les violations.

La traduction ci-dessous est fournie à titre d'information uniquement. En cas de divergence, d'incohérence ou de conflit entre cette traduction et la dernière version en anglais mise à jour (y compris en raison de délais de traduction), la version anglaise prévaudra.

4.2 **Gestion des correctifs**. Le Prestataire tiendra les Systèmes d'information couverts à jour avec les dernières mises à niveau, mises à jour, corrections de bogues et nouvelles versions. Le Prestataire mettra en œuvre des mesures d'atténuation pour les actifs inopérables.

4.3 **Enregistrement**. Le Prestataire collectera, gérera et conservera les journaux d'audit, d'événements et de sécurité, y compris : (a) les données de journal concernant toute utilisation (autorisée ou non) des comptes d'Amazon ou des informations d'identification transmises au Prestataire à des fins autorisées, et (b) les données de journal concernant toute usurpation d'identité ou tentative d'usurpation d'identité du personnel d'Amazon ou du personnel ayant accès aux Informations d'Amazon ou aux Systèmes d'information couverts. Ces journaux contiendront suffisamment de données pour identifier chaque événement enregistré : (i) le Personnel ou le compte à l'origine de l'événement, (ii) l'heure de l'événement, et (iii) le système, les données ou toute autre ressource affectée. Le Prestataire analysera régulièrement ces journaux afin de détecter, d'enquêter et de se remettre d'une activité non autorisée.

4.4 **Défenses contre les logiciels malveillants.** Le Prestataire (a) déploiera un logiciel anti-malware ou un contrôle de sécurité équivalent sur tous les Systèmes d'information couverts ; (b) maintiendra les mises à jour, signatures et configurations du logiciel anti-malware ou du contrôle de sécurité équivalent ; et (c) configurera les systèmes pour détecter, prévenir et corriger l'installation, la propagation et l'exécution de code malveillant ou non autorisé.

4.5 **Programme de gestion des risques.** Le Prestataire disposera d'un programme écrit de gestion des risques liés à la sécurité des informations, qui définit les processus d'analyse, de traitement et d'acceptation des risques, ainsi que les exceptions.

4.6 **Formation de sensibilisation à la sécurité.** Le Prestataire dispensera une formation sur la sécurité des informations et la confidentialité des données au Personnel lors de l'embauche et au moins une fois par an par la suite. Le Prestataire veillera également à ce que le Personnel soit informé en temps opportun des mises à jour des politiques de sécurité et de confidentialité des données du Prestataire.

4.7 **Inventaire des données** . Le Prestataire documentera et conservera les informations concernant (a) les Informations d'Amazon qu'il traite et (b) comment et où lesdites Informations d'Amazon sont traitées (par ex., dans un diagramme d'architecture à jour). À la demande d'Amazon, le Prestataire fournira ces informations à Amazon.

4.8 **Tests de sécurité.**

4.8.1 Le Prestataire effectuera des tests annuels pour s'assurer qu'il répond aux exigences de la présente Politique de sécurité.

4.8.2 Le Prestataire effectuera des tests de pénétration des défenses de sécurité du Prestataire au moins une fois par an. Les tests de pénétration comprendront : (a) des tests à l'intérieur et à l'extérieur du réseau du Prestataire, (b) des tests d'ingénierie sociale (par exemple, des simulations d'hameçonnage), et (c) des tests de sécurité pour les réseaux sans fil. Le Prestataire traitera les vulnérabilités identifiées dans le cadre de son programme de gestion dans ce domaine. À la demande d'Amazon, le Prestataire lui fournira les résultats de ces tests de pénétration et de la correction des vulnérabilités.

4.9 **Sécurité réseau.** Le Prestataire protégera tous les Systèmes d'information couverts en limitant l'accès non autorisé au réseau, en particulier depuis les réseaux externes. Le Prestataire maintiendra et configurera des pare-feu ou d'autres contrôles de sécurité équivalents pour protéger les systèmes contre tout accès non autorisé et examinera les ensembles de règles de pare-feu au moins une fois par an pour s'assurer qu'il existe des cas commerciaux valides et documentés pour toutes les règles.

4.10 **Environnement approprié**. Le Prestataire traitera les Informations Amazon uniquement dans un environnement adapté à son objectif et ne traitera pas lesdites Informations Amazon dans un environnement de test, à moins que cela ne soit autorisé en vertu du Contrat.

La traduction ci-dessous est fournie à titre d'information uniquement. En cas de divergence, d'incohérence ou de conflit entre cette traduction et la dernière version en anglais mise à jour (y compris en raison de délais de traduction), la version anglaise prévaudra.

4.11 **Chiffrement**. Le Prestataire chiffrera toutes les Informations Amazon au repos et en transit sur les réseaux externes conformément aux meilleures pratiques du secteur. Si les Informations Amazon sont transmises sur les réseaux internes des Prestataires, elles seront transmises par le biais d'un protocole chiffré qui répond aux meilleures pratiques du secteur. Le Prestataire gérera et sécurisera les clés de chiffrement conformément aux meilleures pratiques du secteur.

4.12 **Utilisation contrôlée des privilèges administratifs.** Le Prestataire gérera les fonctions administratives conformément au Cadre de cybersécurité du NIST ou à la norme ISO 27002. Le Prestataire séparera, au minimum, les comptes administratifs des comptes standard et limitera les comptes administratifs aux seules capacités nécessaires à l'exécution des fonctions administratives. Le Prestataire enregistrera toutes les actions administratives du compte d'une manière attribuable à un utilisateur individuel. Les capacités administratives fournies à un compte standard seront basées sur le principe du moindre privilège et consignées d'une manière attribuable à un utilisateur individuel.

4.13 **Contrôle d'accès.**

4.13.1 **Identifiants uniques**. Le Prestataire attribuera des identifiants individuels et uniques au Personnel ayant accès aux Informations Amazon ou aux Systèmes d'information couverts, y compris les comptes ayant un accès administratif.

4.13.2 **« Besoin de savoir » uniquement.** Le Prestataire limitera l'accès aux Informations Amazon et aux Systèmes d'informations couverts au seul Personnel ayant un « besoin de savoir » à des fins autorisées.

4.13.3 **Examen de l'accès utilisateur**. Le Prestataire examinera, au moins une fois tous les 90 jours, la liste des Personnels et des services ayant accès aux Informations Amazon et Systèmes d'informations couverts, et supprimera l'accès aux comptes qui n'en ont plus besoin.

4.13.4 **Authentification unique (Single Sign-On, SSO).** Tous les services du Prestataire qui nécessitent une authentification du personnel Amazon doivent s'intégrer à un fournisseur d'identité Amazon (par ex., Amazon Federate) pour fournir cette authentification. Ces services ne doivent pas utiliser d'informations d'identification fournies ou gérées par le Prestataire pour l'authentification.

4.14 **Gestion des mots de passe.**

4.14.1 **Mots de passe forts**. Le Prestataire n'utilisera pas les valeurs par défaut fournies par le fabricant pour les mots de passe système et autres paramètres de sécurité sur les Systèmes d'information couverts. Le Prestataire mandatera et veillera à l'utilisation de « mots de passe forts » imposés par le système conformément aux meilleures pratiques décrites dans NIST SP 800-63B sur tous les Systèmes d'information couverts. Le Prestataire exigera que tous les mots de passe et identifiants d'accès restent confidentiels et ne soient pas partagés entre les membres du Personnel.

4.14.2 **Verrouillage**. Le Prestataire maintiendra et appliquera le « verrouillage de compte » en désactivant les comptes ayant accès aux Informations Amazon ou aux Systèmes d'information couverts lorsqu'un compte dépasse plus de dix (10) tentatives consécutives de mot de passe incorrect.

4.15 **Accès à distance ; Authentification multifacteur**. Le Prestataire mettra en œuvre une authentification multifacteur (c.-à-d., nécessitant au moins deux facteurs pour authentifier un utilisateur) pour l'accès à distance à tout réseau, système, application ou autre actif du Prestataire.

4.16 **Accès « en masse »**. Aux fins de la présente section, l'accès « en masse » signifie le fait d'accéder aux données au moyen d'une requête de base de données, d'une génération de rapports ou de tout autre transfert de masse de données.

La traduction ci-dessous est fournie à titre d'information uniquement. En cas de divergence, d'incohérence ou de conflit entre cette traduction et la dernière version en anglais mise à jour (y compris en raison de délais de traduction), la version anglaise prévaudra.

4.16.1 Sauf autorisation expresse du Contrat ou autre disposition écrite d'Amazon, le Prestataire n'accédera pas et n'autorisera pas l'accès aux Informations Amazon « en masse », que les Informations Amazon soient dans une base de données contrôlée par le Prestataire ou Amazon ou stockées de toute autre manière, y compris le stockage dans des archives basées sur des fichiers (par exemple, des fichiers plats), etc.

4.16.2 Lorsque Amazon autorise un accès « en masse », le Prestataire : (a) limitera cet accès uniquement au Personnel spécifié ayant un « besoin de savoir », et (b) exigera une autorisation explicite et un enregistrement de cet accès conformément aux exigences de la Section 4.3. Sur demande d'Amazon
, en coordination avec les contrôles de sécurité visés à la Section 10 ou les incidents de sécurité visés à la Section 11, le Prestataire fournira à Amazon tous les registres relatifs à l'accès « en masse » mentionnés dans la présente section.

4.17 Séparation des données. Le Prestataire séparera physiquement ou logiquement les Informations Amazon des informations du Prestataire et de tout tiers à tout moment. Si la séparation n'est pas possible, le Prestataire s'assurera que les Informations Amazon puissent être différenciées des autres informations à des fins d'enregistrement, de suppression et d'intervention en cas d'incident.

4.18 **Sécurité du personnel du Prestataire.**

4.18.1 Le Prestataire prendra toutes les précautions raisonnables pour s'assurer que le Personnel autorisé à accéder aux Informations Amazon en préserve la confidentialité et ne les utilise qu'à des fins autorisées. Ces précautions doivent inclure le respect de la confidentialité par le biais d'un accord de non-divulgation ou d'une politique des Prestataires.

4.18.2 Pour tout membre du Personnel qui (a) n'a plus besoin d'accéder aux Informations Amazon ou (b) n'est plus qualifié en tant que Personnel du Prestataire, ce dernier mettra fin à l'accès aux Informations Amazon et aux Systèmes d'information couverts dans un délai de 24 heures. Si un membre du Personnel conserve l'accès aux Informations d'Amazon ou aux Systèmes d'information couverts plus de 24 heures après la survenance des points (a) ou (b), le Prestataire informera Amazon de cet accès continu dans les 24 heures après en avoir pris connaissance en envoyant un e-mail à security@amazon.com.

5. **EXIGENCES DE SÉCURITÉ DE PAIEMENT**. Si le Prestataire a accès aux données des titulaires de cartes de paiement ou les traite, il se conformera à la dernière version de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS).

6. **SOUS-TRAITANTS.**

6.1 Le Prestataire ne sous-traitera ni ne déléguera aucune de ses obligations en vertu de la présente Politique de sécurité à un tiers (collectivement, les « sous-traitants ») sans l'accord écrit préalable d'Amazon. Nonobstant l'existence ou les conditions de tout contrat de sous-traitance ou toute délégation, le Prestataire demeurera responsable de l'exécution complète de ses obligations en vertu de la présente Politique de sécurité. Les conditions générales de la présente Politique de sécurité seront contraignantes pour les Sous-traitants et le Personnel du Prestataire.

6.2 Si le Prestataire utilise des Systèmes d'information couverts du Sous-traitant, ledit Prestataire effectuera un examen de sécurité des Systèmes d'information couverts du Sous-traitant et de leurs contrôles de sécurité et, à la demande d'Amazon, fournira à Amazon des rapports périodiques sur les contrôles de sécurité des Systèmes d'information couverts du Sous-traitant dans le format demandé par Amazon (par ex., Déclaration sur les normes pour les engagements d'attestation n° 16 (SSAE 16)).

7. ACCÈS AUX SYSTÈMES D'INFORMATION GÉRÉS PAR AMAZON. Amazon peut accorder au Prestataire le droit de Traiter les Informations Amazon via des portails Web ou d'autres sites Web ou extranets non publics

La traduction ci-dessous est fournie à titre d'information uniquement. En cas de divergence, d'incohérence ou de conflit entre cette traduction et la dernière version en anglais mise à jour (y compris en raison de délais de traduction), la version anglaise prévaudra.

(chacun, un « Système d'information géré par Amazon ») uniquement aux fins autorisées. Si Amazon autorise le Prestataire à accéder à toute Information Amazon à l'aide d'un Système d'information géré par Amazon, le Prestataire doit se conformer aux exigences suivantes :

7.1 **Comptes.** Le Prestataire s'assurera que le Personnel du prestataire utilise uniquement le ou les compte(s) du Système d'information géré par Amazon désignés pour chaque personne et exigera du Personnel du prestataire qu'il préserve la confidentialité de ses identifiants d'accès et ne les partage pas.

7.2 **Systèmes**. Le Prestataire et son Personnel utiliseront les Systèmes d'information gérés par Amazon uniquement par le biais de systèmes informatiques ou de traitement ou d'applications (a) exécutant des systèmes d'exploitation gérés par le Prestataire et utilisant un cryptage complet du disque, et (b) répondant aux exigences des Sections 4.2 (Gestion des correctifs), 4.4 (Défenses contre les logiciels malveillants) et 4.9 (Sécurité du réseau).

7.3 **Restrictions**. Sauf autorisation écrite préalable d'Amazon, le Prestataire et son Personnel ne téléchargeront, ne mettront en miroir ni ne stockeront de façon permanente aucune Information Amazon à partir d'un Système d'information géré par Amazon sur quelque support que ce soit.

7.4 **Résiliation de compte**. Pour tout membre du Personnel du prestataire qui (a) n'a plus besoin d'accéder au Système d'information géré par Amazon ou (b) ne répond plus aux critères du Personnel du prestataire (par ex., la personne quitte l'emploi du Prestataire), le Prestataire mettra immédiatement fin à l'accès au Système d'Information géré par Amazon (dans un délai maximum de 24 heures) ou informera Amazon de la suppression de cet accès.

8. **DOMAINES OU URL AMAZON.** Tout domaine ou URL que le Prestataire fournit pour le seul usage d'Amazon ne doit pas être délivré par le Prestataire à un tiers ni réutilisé par celui-ci pendant au moins cinq ans après la résiliation du Contrat.

9. RETOUR ET SUPPRESSION DES DONNÉES ; DESTRUCTION MÉDICO-LÉGALE.

9.1 **Retour et suppression des données**. À la demande d'Amazon, le Prestataire retournera rapidement (mais dans un délai maximum de 72 heures) à Amazon et supprimera de façon permanente et sécurisée toutes les Informations Amazon conformément à l'avis d'Amazon exigeant le retour et/ou la suppression. Le Prestataire supprimera également de manière permanente et sécurisée toutes les instances en cours (en ligne ou accessibles par le réseau) des Informations Amazon dans les 30 jours suivant la réalisation de la Finalité autorisée ou la résiliation ou l'expiration du présent Contrat. Si Amazon le demande, le Prestataire certifiera par écrit que toutes les Informations Amazon ont été détruites. Pour plus de clarté, cette section ne s'appliquera pas aux copies d'archives conformément à la section 9.3.

9.2 **Nettoyage des données**. Toutes les informations Amazon supprimées par le Prestataire le seront conformément aux recommandations minimales de nettoyage contenues dans le document NIST SP 800-88 Revision 1, Guidelines for Media Sanitization (18 décembre 2014, annexe A) pour la purge du type d'appareil concerné. En l'absence de directives dans le NIST SP 800-88 pour le type d'appareil concerné, le Prestataire détruira l'appareil contenant des Informations Amazon de l'une des manières suivantes : (a) en le purgeant comme défini dans le NIST SP 800-88, (b) en le détruisant comme défini dans le NIST SP 800-88, ou (c) en appliquant d'autres normes qu'Amazon peut exiger en fonction de la classification et de la sensibilité des Informations Amazon.

9.3 **Copies d'archives.** Si le Prestataire est tenu par la loi de conserver des copies archivées des Informations Amazon, il n'utilisera pas les Informations Amazon archivées à d'autres fins et
restera lié par toutes les obligations qui lui incombent en vertu de la présente Politique de sécurité. Toute Information Amazon archivée doit être cryptée et stockée lorsque le Système d'information couvert hébergeant ou stockant les Informations Amazon cryptées n'a pas accès à une copie de la ou des clé(s) utilisée(s) pour le cryptage. Toute sauvegarde « froide » ou hors ligne (c.-à-d. non disponible pour une utilisation immédiate ou interactive) doit être stockée dans une installation physiquement sécurisée.

La traduction ci-dessous est fournie à titre d'information uniquement. En cas de divergence, d'incohérence ou de conflit entre cette traduction et la dernière version en anglais mise à jour (y compris en raison de délais de traduction), la version anglaise prévaudra.

9.4 **Destruction médico-légale**. Avant de se débarrasser de tout matériel, logiciel ou autre support contenant, ou ayant contenu à un moment quelconque, des Informations Amazon, le Prestataire procédera à une destruction médico-légale complète du matériel, du logiciel ou de tout autre support conformément à la norme NIST SP 800-88, annexe A. Cette exigence de destruction ne s'appliquera pas aux supports de stockage auxquels le Prestataire n'a pas accès physiquement ou qu'il ne contrôle pas. Dans de tels cas, le Prestataire veillera à ce que les Informations Amazon soient supprimées en toute sécurité lorsqu'elles ne sont plus nécessaires conformément aux meilleures pratiques du secteur.

> 9.4.1 À moins que le Prestataire ne reçoive le consentement écrit préalable exprès d'Amazon, il ne vendra, ne revendra, ne donnera, ne rénovera ou ne transférera autrement aucun matériel, logiciel ou autre support ayant contenu à tout moment des Informations Amazon, à moins qu'il n'ait été détruit de manière irréfutable
> conformément à la présente Section.

10. **EXAMENS DE SÉCURITÉ.** À la demande d'Amazon, le Prestataire devra : (a) réaliser une évaluation des risques d'Amazon, (b) fournir les preuves demandées par Amazon pour valider le respect de la présente Politique de sécurité par le Prestataire, (c) permettre à Amazon ou à un tiers désigné en son nom d'effectuer un examen du respect de la présente Politique de sécurité par le Prestataire, et/ou (d) fournir à Amazon tous les journaux référencés à la section 4.3 au format Open Cybersecurity Schema Framework (OCSF). Si le Prestataire exige qu'une preuve soit examinée en personne ou dans le cadre d'une inspection sur place plutôt que de fournir cette preuve à Amazon pour examen à distance, Il prendra à sa charge les frais de déplacement et autres dépenses liées à cette inspection sur place. Si une évaluation ou un examen donne lieu à des constatations, le Prestataire prendra rapidement, à ses frais exclusifs, toutes les mesures raisonnables nécessaires pour remédier à ces constatations, à la satisfaction raisonnable d'Amazon et dans un délai convenu.

11. **INCIDENTS DE SÉCURITÉ.**

11.1 **Avis d'incident de sécurité**. Le Prestataire informera Amazon dès que possible, et au plus tard dans les 24 heures, après qu'il aura appris ou raisonnablement cru qu'il y a eu un accès non autorisé, une collecte, une acquisition, une utilisation, une transmission, une divulgation, une corruption ou une perte des Informations Amazon ou d'un Système d'Information Couvert (un « Incident de Sécurité »). Le Prestataire enverra les notifications d'incident de sécurité à security@amazon.com.

11.2 **Plan d'intervention en cas d'incident.** Le Prestataire maintiendra un plan d'intervention en cas d'incident écrit et en fournira une copie à Amazon sur demande. Le Prestataire remédiera à chaque Incident de sécurité en temps opportun en suivant le plan écrit d'intervention en cas d'incident et les meilleures pratiques du secteur. Le Prestataire examinera, testera et (si nécessaire) mettra à jour le plan au moins une fois par an.

11.3 **Coopération avec Amazon.** Le Prestataire (a) assistera Amazon dans son enquête sur l'incident de sécurité ; (b) facilitera les entretiens avec le Personnel et les autres personnes impliquées dans l'incident de sécurité ou la réponse ; (c) conservera par écrit les détails de l'enquête et de la réponse que le Prestataire a apportées à l'incident de sécurité ; et (d) mettra à la disposition d'Amazon tous les enregistrements, journaux, fichiers, rapports de données, rapports médico-légaux, rapports d'enquête et autres documents pertinents demandés par Amazon.

11.4 **Notifications de tiers.** Sauf disposition contraire de la loi, le Prestataire obtiendra le consentement écrit préalable d'Amazon avant : (a) d'informer tout tiers (y compris toute autorité réglementaire ou tout client) de tout Incident de sécurité ; ou (b) d'identifier Amazon dans toute notification ou déclaration publique concernant tout Incident de sécurité. Sauf disposition contraire de la loi, Amazon aura le droit de déterminer si la notification d'un Incident de sécurité doit être fournie à un tiers ainsi que la forme, le calendrier et le contenu de cette notification.

12. **AVIS DE PROCESSUS JURIDIQUE**. Avis de procédure judiciaire. Sauf si la loi l'interdit, si les Informations Amazon sont recherchées dans le cadre d'une procédure judiciaire ou d'une autre loi applicable, le Prestataire en

La traduction ci-dessous est fournie à titre d'information uniquement. En cas de divergence, d'incohérence ou de conflit entre cette traduction et la dernière version en anglais mise à jour (y compris en raison de délais de traduction), la version anglaise prévaudra.

informera Amazon suffisamment à l'avance pour lui permettre d'obtenir une ordonnance de protection ou toute autre mesure appropriée.

13. **DÉFINITIONS.**

13.1 « **Accord** » signifie tout accord qui fait référence à la présente Politique de sécurité.

13.2 « **Amazon** » désigne Amazon.com, Inc. et ses sociétés affiliées.

13.3 « **Informations Amazon** » signifie, individuellement et collectivement : (a) tous les Informations confidentielles d'Amazon (telles que définies dans un accord de confidentialité ou tout autre accord entre les parties) ; (b) toutes les données, enregistrements, fichiers, contenus ou informations, sous quelque forme que ce soit, acquis, consultés, collectés, reçus, stockés ou conservés par le Prestataire ou ses sociétés affiliées, de la part ou pour le compte d'Amazon, ou autrement en relation avec l'Accord ; et (c) les informations dérivées des points (a) ou (b), même si elles sont anonymisées.

13.4 « **Anonymiser** » signifie traiter toute donnée ou information (y compris les Informations Amazon) d'une manière ou sous une forme qui n'identifie pas, ne permet pas d'identifier et n'est pas autrement attribuable à Amazon, ou à tout utilisateur, identificateur d'appareil, source, produit, service, contexte ou marque de celui-ci.

13.5 « **Systèmes d'information couverts** » désigne tous les systèmes que le Prestataire utilise pour traiter les Informations Amazon.

13.6 « **Personnel** » désigne les employés, agents, Sous-traitants et autres utilisateurs autorisés du Prestataire ou du Sous-traitant de ses systèmes et ressources réseau.

13.7 « **Traiter** » désigne toute opération sur les données, telle que l'accès, l'utilisation, la collecte, la réception, le stockage, l'altération, la transmission, la diffusion ou toute autre forme de mise à disposition, l'effacement ou la destruction.

13.8 « **Prestataire** » désigne chaque Prestataire, Fournisseur ou Sous-traitant défini dans un Accord et tout autre prestataire soumis à un Accord.