

Avenant relatif au traitement des données (dénommé auparavant avenant SaaS)

Le présent Avenant relatif au traitement des données (ci-après « Data Processing Addendum » ou « **DPA** ») est incorporé au contrat de logiciel et/ou au contrat de services (le « **Contrat** ») entre le Fournisseur et le Client pour l'achat de certaines licences de Logiciel SaaS et/ou de Services de maintenance et/ou services professionnels (aux fins du présent DPA, ci-après dénommés les « **Services** »). Ce DPA n'est pas un contrat distinct et fait partie d'un contrat écrit (y compris sous forme électronique) convenu entre le Fournisseur et le Client. Tous les termes commençant par une majuscule non définis dans les présentes auront la signification indiquée dans le Contrat.

1. **Définitions.** Les termes commençant par une majuscule qui ne sont pas définis dans le contexte ou dans le Contrat auront la signification qui leur est attribuée ci-dessous :

- a) « **Responsable du traitement** » désigne une personne physique ou morale, une autorité publique, une agence ou un autre organisme, qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des Données personnelles.
- b) « **Loi sur la protection des données** » désigne toutes les lois et réglementations applicables au traitement des données personnelles du client en vertu du Contrat, y compris, le cas échéant : (i) la California Consumer Privacy Act, telle que modifiée par la California Privacy Rights Act, et toute réglementation contraignante promulguée dans le cadre de celle-ci « **CCPA** », (ii) le Règlement Général sur la Protection des Données (Règlement (UE) 2016/679) (« **RGPD UE** » ou « **RGPD** »), (iii) la loi fédérale suisse sur la protection des données (« **LPD** »), (iv) le RGPD UE telue appliqué dans le droit applicable de l'Angleterre et du Pays de Galles en vertu de l'article 3 de la loi de 2018 sur l'Union européenne (retrait) (le « **UK GDPR** ») et (v) le UK Data Protection Act 2018; pour chacune des lois, telle que mise à jour, modifiée ou remplacée.
- c) « **Personne concernée** » désigne la personne physique identifiée ou identifiable à laquelle se rapportent les Données personnelles du Client.
- d) « **Données personnelles** » désigne des informations sur une personne physique identifiée ou identifiable ou qui constituent autrement des « données personnelles », des « informations personnelles », des « informations personnellement identifiables » ou des termes similaires tels que définis dans les Lois sur la protection des données.
- e) « **Violation de données personnelles** » désigne une destruction accidentelle ou illégale, une perte, une altération, une divulgation non autorisée des données personnelles du Client traitées par le Fournisseur ou l'accès non autorisé d'un tiers à celles-ci, dans chaque cas pour lequel un Responsable du traitement est tenu, en vertu de la Loi sur la protection des données, d'avertir les autorités compétentes en matière de protection des données ou les Personnes concernées.
- f) « **Traitement** » désigne toute opération effectuée sur les Données personnelles, telle que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou l'altération, la récupération, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou la mise à disposition, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction, par des moyens automatisés ou non.
- g) « **Sous-traitant** » désigne une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui traite des Données personnelles pour le compte du Responsable du traitement.
- h) « **Clauses contractuelles types** » désigne les clauses contractuelles types approuvées par la Commission européenne dans le cadre de la décision 2021/914.
- i) « **Sous-traitant ultérieur** » désigne les Sociétés affiliées du Fournisseur et les tiers engagés par le Fournisseur (ou par les Sociétés affiliées du Fournisseur) pour la fourniture de tout ou partie des Services et qui traite les Données personnelles du Client conformément au présent DPA.

2. Traitement des données personnelles du Client

Le Fournisseur peut traiter les données personnelles du Client en vertu du Contrat en qualité de sous-traitant agissant pour le compte du Client, qui est Responsable du traitement (ou, selon le cas, en qualité de sous-traitant ultérieur pour le compte du Client qui est alors lui-même Sous-traitant). Le Fournisseur s'engage à traiter les Données personnelles dans le seul but d'exécuter ses obligations envers le Client en vertu et conformément (i) au présent DPA et au Contrat, et (ii) aux instructions écrites du Client ou (iii) aux Lois sur la protection des données, sous réserve de toute exigence de notification, requise en vue de se conformer à ses obligations en vertu des lois applicables. Les détails de l'objet du traitement, sa durée, sa nature et son objectif, ainsi que le type de Données personnelles du Client et les Personnes concernées, sont tels que spécifiés dans le Contrat ou, à défaut, , seront tels qu'énoncés à l'annexe 1 de ce DPA. Le Client et le Fournisseur acceptent de se conformer à leurs obligations respectives en vertu des Lois sur la protection des données applicables aux Données personnelles qui sont traitées dans le cadre des Services. Le Client est seul responsable du respect des Lois sur la protection des données concernant le traitement de ses Données personnelles avant la divulgation, la transmission ou la mise à disposition d'une quelconque autre manière des Données personnelles au Fournisseur. Ce dernier informera le Client sans délai dès lors qu'il juge que les instructions du Client sont contraires aux Lois sur la protection des données.

3. Sécurité du traitement

- a) **Politiques générales de sécurité.** Le Fournisseur mettra en œuvre et maintiendra des mesures, procédures et pratiques techniques et organisationnelles, adaptées à la nature des Données personnelles du Client, lesquelles sont conçues pour protéger la sécurité, la confidentialité, l'intégrité et la disponibilité des Données personnelles du Client et les protéger contre les violations de Données personnelles, conformément aux mesures de sécurité du Fournisseur référencées dans le Contrat et décrites de manière plus approfondie à l'adresse suivante: <https://www.oneidentity.com/legal/security.aspx> (collectivement le « **Site de sécurité** »), qui comprend les éléments suivants :
 - La Politique de sécurité de l'information,
 - La déclaration des mesures techniques et organisationnelles,
 - La Politique de réponse aux Violations de données, et
 - La politique de confidentialité.

Le Fournisseur peut modifier son Site de sécurité tant que cela ne diminue pas de manière significative le niveau global de protection fourni.

- b) **Confidentialité.** Le Fournisseur protégera les Données personnelles du Client conformément à ses obligations de confidentialité telles qu'énoncées dans le Contrat. Le Fournisseur s'assurera que les membres de son personnel qui traitent les Données personnelles du Client ont conclu des accords de confidentialité écrits. Il doit s'assurer que ces obligations de confidentialité survivront à la cessation d'emploi de ces membres du personnel. Il formera régulièrement les personnes ayant accès aux Données personnelles du Client aux exigences et aux principes de sécurité et de confidentialité des données.

4. Demandes des Personnes concernées.

À la demande du Client, le Fournisseur coopérera de manière raisonnable avec celui-ci afin de l'aider à se conformer à ses obligations en vertu des Lois sur la protection des données pour répondre aux demandes de personnes physiques souhaitant exercer leurs droits en vertu des Lois sur la protection des données, dès lors que le Client ne puisse pas (raisonnablement) répondre à ces demandes de manière autonome (y compris par l'utilisation des Services). Si le Fournisseur reçoit une demande d'une Personne concernée au sujet des Données personnelles traitées en vertu des présentes, il informera la Personne concernée (lorsque celle-ci a fourni des informations permettant d'identifier le Client) de d'adresser sa demande directement auprès du Client.

5. Droits d'audit.

- a) **Dossiers fournisseur en général.** Le Fournisseur conservera des dossiers de son Traitement conformément aux Lois sur la protection des données et, sur demande écrite du Client, mettra à la disposition de ce dernier, tous les documents raisonnablement nécessaires pour prouver qu'il respecte ses obligations en vertu du présent DPA et des Lois sur la protection des données applicables.
- b) **Programme de conformité tiers.** Le Fournisseur décrira ses programmes d'audit et de certification tiers (le cas échéant) et mettra à la disposition du Client des copies des synthèses de ses rapports d'audit (chacun, un « **Rapport d'audit** ») sur demande écrite du Client (sous réserve des obligations de confidentialité énoncées dans le Contrat). Le Client peut partager une copie des Rapports d'audit avec les autorités gouvernementales compétentes si nécessaire.
- c) **Audit client.** Le Client peut, à ses frais, effectuer un audit conformément à un plan convenu d'un commun accord qui est conforme aux paramètres d'audit ci-dessous (un « **Audit** »). Le Client peut exercer ses droits d'Audit (1) dans la mesure où la Fourniture d'un rapport d'audit par le Fournisseur ne fournit pas suffisamment d'informations au Client pour vérifier la conformité du Fournisseur avec le présent DPA ou la conformité avec les Lois sur la protection des données ; ou (2) si l'Audit est nécessaire pour que le Client réponde à un audit d'une autorité gouvernementale, ou (3) dans le cadre d'une Violation des données personnelles.

Chaque Audit doit (1) être mené par un tiers indépendant qui aura conclu un accord de confidentialité avec le Fournisseur, (2) être limité dans sa portée aux questions raisonnablement requises pour que le Client évalue la conformité du Fournisseur avec le présent DPA ainsi que la conformité des parties avec Les lois sur la protection des données, (3) avoir lieu à une date et une heure convenues d'un commun accord entre les parties et uniquement pendant les heures normales d'ouverture du Fournisseur, (4) être limité à un par an (sauf si cela est requis en vertu des Lois sur la protection des données ou en relation avec une Violation des données personnelles), (5) couvrir uniquement les installations contrôlées par le Fournisseur, (6) limiter l'inspection uniquement aux Données personnelles du Client et (7) traiter l'ensemble des résultats comme étant des informations confidentielles dans les limites autorisées par les Lois sur la protection des données.

6. Sous-traitants ultérieurs et Transferts internationaux.

- a) **Utilisation de Sous-traitants ultérieurs.** Le Client autorise le Fournisseur à engager des Sous-traitants ultérieurs dans le cadre de la fourniture des Services. Le Fournisseur signera les accords écrits appropriés avec les Sous-traitants ultérieurs conformément aux dispositions du présent DPA et aux instructions visées aux présentes convenues entre le Client et le Fournisseur. Ce dernier est responsable de toute violation de ce DPA causée par des Sous-traitants ultérieurs qu'il aurait lui-même engagés.
- b) **Liste des Sous-traitants ultérieurs.** Le Fournisseur tient à jour des listes de Sous-traitants ultérieurs par Produit, y compris leurs fonctions et localisations, dont le Client peut disposer, moyennant une inscription, à l'adresse <https://support.oneidentity.com/subprocessor>. Au moins trente (30) jours avant d'autoriser tout nouveau Sous-traitant ultérieur à accéder aux Données personnelles, le Fournisseur mettra à jour la liste des Sous-traitants ultérieurs et informera le Client par e-mail lors de l'inscription.
- c) **Objection aux nouveaux Sous-traitants ultérieurs.** Si le Client n'approuve pas un nouveau Sous-traitant ultérieur, le Client peut résilier tout abonnement au Logiciel SaaS applicable en adressant, avant la fin de la période de préavis, une demande écrite de résiliation expliquant les motifs pour lesquels il n'approuve pas le choix du Fournisseur.
- d) **Transferts internationaux.** Pour le transfert de données personnelles européennes et/ou britanniques à un Sous-traitant ultérieur situé dans un pays tiers qui n'offre pas une protection adéquate des Données personnelles, le Fournisseur et le Sous-traitant ultérieur concerné ont conclu les Clauses contractuelles types afin de fournir des garanties appropriées pour le transfert desdites Données personnelles conformément aux Lois européennes et britanniques sur la protection des données.

7. Notification de violation de données personnelles.

Outre les obligations décrites sur le Site de sécurité, le Fournisseur s'engage à informer le Client sans délai indu après avoir pris connaissance d'une Violation de données à caractère personnel et à fournir les informations raisonnables en sa possession pour aider le Client à remplir ses obligations de signalement d'une Violation de données à caractère personnel, comme l'exige la Loi sur la protection des données. Le Fournisseur peut fournir ces informations par étapes, au fur et à mesure qu'elles sont disponibles. Le Fournisseur s'engage à déployer des efforts de bonne foi pour identifier la cause de ladite Violation de données à caractère personnel et à prendre les mesures qu'il juge nécessaires et raisonnables pour remédier à

la cause de la Violation de données à caractère personnel dans la mesure où la réparation est sous le contrôle raisonnable du Prestataire.

8. Suppression des Données personnelles du Client.

Sauf notification adressée par le Client au Fournisseur au moins trente (30) jours avant le terme des Services, après la résiliation ou l'expiration du Contrat, le Fournisseur supprimera de ses systèmes toutes les Données personnelles du Client. Il effectuera la suppression conformément aux pratiques de suppression sécurisée standard du secteur. Nonobstant ce qui précède, le Fournisseur peut conserver les Données personnelles du Client : (i) conformément aux Lois sur la protection des données ou (ii) conformément à ses politiques standard de sauvegarde ou de conservation des dossiers, à condition que, dans les deux cas, le Fournisseur (1) préserve la confidentialité et respecte les dispositions applicables du présent DPA en ce qui concerne les Données personnelles du client conservées et (2) ne traite pas ultérieurement les Données personnelles du client conservées, sauf en vue de ces motifs et selon la durée prévue par les Lois sur la protection des données applicables.

9. Évaluation de l'impact de la protection des données.

Le Fournisseur coopérera avec le Client et l'aidera de manière raisonnable, selon les besoins, à satisfaire à l'obligation qui incombe au Client en vertu des Lois sur la protection des données de réaliser une évaluation d'impact sur la protection des données ou une évaluation des risques similaires liés à l'utilisation des Services par le Client.

ANNEXE AU DPA

Cette annexe fait partie du DPA.

ANNEXE I – Objet et détails du Traitement

A. LISTE DES PARTIES

Le Contrat entre le Client en qualité de Responsable du traitement et le Fournisseur en tant que Sous-traitant contient une description de toutes les informations requises, telles que :

- nom, adresse, nom du contact,
- poste et coordonnées,
- activités pertinentes pour les données transférées en vertu des présentes Clauses, et
- signature et date.

B. DESCRIPTION DU TRAITEMENT

1. **Catégories de Personnes concernées dont les Données personnelles sont traitées**

Sauf disposition contraire du Client, les Données personnelles traitées concernent les catégories suivantes de Personnes concernées :

- employés, sous-traitants, prestataires de services, partenaires commerciaux du Client.

2. **Catégories de Données personnelles traitées**

Le Client détermine les catégories de données en fonction de son utilisation des Services. Les Données Personnelles Traitées concernent généralement les catégories de données suivantes :

- les détails de l'emploi (qui peuvent inclure le nom et l'adresse de l'entreprise, le titre du poste, le grade, les données démographiques et de localisation) relatifs aux employés du Client ou d'autres tiers dont les informations personnelles sont fournies par ou au nom du Client ;
- les systèmes d'information liés aux systèmes du Client ou aux systèmes fournis au Fournisseur par le Client et liés aux Services achetés dans le cadre du Contrat et requis pour la fourniture des Services (qui peuvent inclure l'identifiant et le mot de passe de l'utilisateur, l'ordinateur et le nom de domaine, l'adresse IP, le numéro GUID ou l'emplacement de l'ordinateur ou de tout autre dispositif utilisé).

Les Données personnelles du Client traitées en vertu des présentes peuvent concerner des partenaires commerciaux passés, présents et potentiels ou d'autres personnes liées à ces partenaires commerciaux.

3. **Données sensibles traitées (le cas échéant)**

Le Client ne doit pas fournir de catégories spéciales de Données personnelles (données sensibles), sauf si elles sont identifiées au cas par cas et uniquement dans la mesure où les parties conviennent que ces données de catégorie spéciale doivent être couvertes par la fourniture des Services.

4. **La fréquence du Traitement (par exemple, si les données sont traitées de manière ponctuelle ou continue)**

De manière continue pendant toute la durée d'utilisation des Services.

5. **Nature du Traitement**

- a) Dans le cadre des Services de maintenance : le Fournisseur ou ses Sous-traitants ultérieurs fournissent une assistance et soutien technique lorsqu'un Client soumet une demande d'assistance parce que le Logiciel n'est pas disponible ou ne fonctionne pas comme il se devrait. Le Fournisseur répond aux appels téléphoniques, effectuent des dépannages de base et gèrent les tickets d'assistance dans un système de suivi.
- b) Dans le cadre des services Professionnels : le Fournisseur ou ses Sous-traitants ultérieurs fournissent des Services soumis à la Commande portant sur des services professionnels.
- c) Dans le cadre du Logiciel SaaS : Fourniture du Logiciel SaaS souscrit par le Client.

6. **Finalité(s) du transfert de données et Traitement ultérieur**

Les Données personnelles du Client traitées par le Fournisseur seront soumises aux activités de Traitement de base suivantes :

- a) utilisation des Données personnelles pour fournir les Services du Fournisseur et, le cas échéant, pour fournir l'accès et les avantages du Logiciel SaaS conformément au Contrat ainsi que pour fournir une assistance technique à la demande du Client et conformément aux exigences spécifiques du Client, le cas échéant, le tout conformément aux instructions décrites ci-dessous ;
- b) stockage des Données personnelles ;
- c) traitement informatique des Données personnelles pour la transmission de données ;
- d) amélioration continue des caractéristiques et fonctionnalités de service fournies dans le cadre des Services du Fournisseur, y compris l'automatisation, le traitement des transactions et l'apprentissage automatique (machine learning) ;
- e) exécution des instructions du Client conformément au Contrat.

Les activités de Traitement supplémentaires suivantes s'appliquent à toutes les Données personnelles stockées dans le Logiciel SaaS :

- a) stockage des Données Personnelles dans des centres de traitement des données (architecture multi-locataires) ;
- b) sauvegarde et restauration des Données personnelles du Client stockées dans le Logiciel SaaS ;
- c) le traitement informatique des Données personnelles, y compris la transmission et la récupération de données ainsi que l'accès à celles-ci ;
- d) communication aux utilisateurs du Client ;
- e) publication, développement et chargement de tout correctif ou mise à niveau du Logiciel SaaS ;
- f) accès au réseau pour permettre le transfert de Données personnelles ;
- g) surveillance, dépannage et administration de l'infrastructure et la base de données sous-jacentes du Logiciel SaaS ;
- h) surveillance de la sécurité, prise en charge de la détection d'intrusion basée sur le réseau, tests d'intrusion ; et
- i) dans la mesure nécessaire pour répondre aux demandes des Personnes concernées, le cas échéant, et conformément aux instructions décrites ci-dessous.

Le Fournisseur peut utiliser des données anonymisées (qui ne sont pas des Données personnelles du Client mais qui peuvent être dérivées des Données personnelles du Client) à des fins liées à l'amélioration des produits et au développement de nouveaux Produits et Services du Fournisseur.

De plus amples détails sur ce que sont les fonctions du Logiciel SaaS, la manière dont il traite les Données personnelles ainsi que l'emplacement du stockage des données sont indiqués dans la Documentation du Produit et le Guide de sécurité applicables.

- 7. La durée pendant laquelle les Données personnelles seront conservées ou, si cela n'est pas possible, les critères utilisés pour déterminer cette durée**
Les Données personnelles seront traitées pendant l'utilisation par le Client des Services conformément aux termes du Contrat et sous réserve de l'article 8 du présent DPA
- 8. Pour les transferts aux Sous-traitants ultérieurs, précisez également l'objet, la nature et la durée du Traitement**
En ce qui concerne les Clauses contractuelles types, les transferts aux Sous-traitants ultérieurs seront effectués sur la même base que celle énoncée dans le présent DPA.
- 9. Instructions, Engagements Client et Fournisseur**
Le Fournisseur suivra les instructions écrites et documentées reçues du Client portant sur les Données personnelles du Client, sauf si, selon le Fournisseur, ces instructions (1) sont légalement interdites ou susceptibles d'entraîner une violation de la Loi sur la protection des données applicable, (2) nécessitent des modifications importantes des Services du Fournisseur, et/ou (3) sont incompatibles avec les conditions du Contrat ou la Documentation du Fournisseur concernant les Services vendus en vertu du Contrat. Dans une telle hypothèse, le Fournisseur informera immédiatement le Client de son incapacité à suivre ces instructions. Toute description du Traitement dans le Contrat, le présent DPA et toute Documentation associée du Fournisseur sera considérée comme des instructions par le Client.

ANNEXE II - Déclaration des mesures techniques et organisationnelles

Le Fournisseur mettra en œuvre les mesures techniques et organisationnelles appropriées définies sur le Site de sécurité (tel que défini à l'article 3 (a) du DPA) dans le cadre du Traitement des Données personnelles du Client par le Fournisseur en vertu des présentes. Le Fournisseur peut modifier les mesures prises pour protéger les Données personnelles du Client tant que cela ne diminue de manière significative le niveau global de protection des données tel que convenu dans les présentes.