REMARQUE : le texte ci-dessous a été généré par traduction automatique à des fins de commodité. La qualité de cette traduction automatique ne correspond pas à celle d'une traduction réalisée de manière professionnelle, le texte peut donc contenir des erreurs. Cette traduction est fournie « EN L'ÉTAT », sans aucune garantie de son exactitude ni de son intégralité ou de sa fiabilité. Si des incohérences apparaissent entre la version anglaise du présent Contrat et sa traduction, seule la version anglaise prévaudra.

AVENANT RELATIF AU TRAITEMENT DES DONNÉES

Date de révision : 18 décembre 2022

Si cet Avenant relatif au traitement des données (« Avenant ») est expressément incorporé par référence dans le Contrat principal (comme défini à la clause 2) entre Sophos Limited, une société immatriculée en Angleterre et au Pays de Galles sous le numéro 2096520, dont le siège social est situé à l'adresse The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni («Fournisseur») et un client du fournisseur («Client»), cet Avenant fait partie du Contrat principal et est en vigueur entre le fournisseur et le client.

Les termes en majuscules utilisés dans cet Avenant sont définis comme indiqué dans la clause 2 ci-dessous. Sur demande, nous pouvons fournir une copie de cet Avenant dans une autre langue. En cas de conflit, la version anglaise de l'Avenant prévaut.

1. PRÉAMBULE

1.1. Les parties ont conclu le Contrat principal concernant la fourniture par le fournisseur au client de certains produits et/ou services (collectivement, les «Produits»).

1.2. Si le Contrat principal est un Contrat MSP de la même forme que le Contrat MSP situé à l'adresse https://www.sophos.com/fr-fr/legal/sophos-msp-partner-terms-and-conditions («Contrat MSP»), le client est un fournisseur de services gérés («MSP»). Si le Contrat principal est une Contrat OEM en vertu de laquelle le client est autorisé à distribuer, concéder en sous-licence ou mettre à la disposition de tiers produits fournisseurs en combinaison avec les produits du client dans le cadre d'une unité groupée («Contrat OEM»), le client est un fabricant d'équipement d'origine («OEM»). Sinon, le client est un utilisateur final («Utilisateur final»).

1.3. La fourniture des produits peut inclure la collecte, l'utilisation et le traitement des données personnelles du contrôleur par le fournisseur au nom du client. Le présent Avenant énonce les obligations des parties en ce qui concerne ce traitement et complète les conditions générales du Contrat principal.

1.4. Nonobstant toute autre condition de la Contrat ou du présent Avenant, les parties conviennent que les Données personnelles du contrôleur ne doivent pas inclure les coordonnées, les informations de paiement ou de facturation, ni d'autres données personnelles concernant les contacts professionnels et les administrateurs du client, y compris le nom, l'adresse e-mail et les coordonnées, Quel fournisseur collecte et traite en son propre nom afin de gérer ses relations avec ses clients, de communiquer avec ses clients et partenaires commerciaux actuels, anciens et potentiels, et d'administrer ses relations commerciales (« données CRM »).

1.4.1. Le fournisseur est un contrôleur des données CRM et traitera les données CRM conformément à ses obligations en vertu de la loi sur la protection des données applicable et de la Politique de confidentialité du Groupe fournisseur .

1.4.2. Sauf en ce qui concerne la Section 1.4.1, les obligations du fournisseur en vertu du présent Avenant ne s'appliquent pas aux données CRM.

1.5. Le Contrat principal, le présent Avenant et les documents expressément mentionnés dans le Contrat principal et le présent Avenant constituent l'intégralité du Contrat entre les parties en relation avec les données personnelles collectées, traitées et utilisées par le fournisseur pour le compte du client en relation avec le Contrat principal,et remplace tous les accords, arrangements et ententes antérieurs entre les parties à l'égard de cet objet.

2. DÉFINITIONS

2.1. Dans cet Avenant, les termes suivants ont la signification suivante :

«Lois applicables en matière de protection des données » désigne, dans la mesure applicable : (a) le Règlement 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données ou «RGPD»);(b la directive e-Privacy (directive 2002/58/ce de l'UE); et (c) toute législation nationale applicable en matière de protection des données, y compris la législation adoptée en vertu des points (a) ou (b); dans chaque cas, elle peut être modifiée ou remplacée de temps à autre.

«Bénéficiaire» a la signification qui lui est donnée dans la Contrat du MSP.

« CCPA » désigne la California Consumer Privacy Act telle que modifiée par la California Privacy Rights Act de 2020), codifiée au Cal. Civ. Code §§ 1798.100 - 1798.199.100 et le Règlement de la California Consumer Privacy Act qui y est publié, Cal. Registres de code tit. 11, div. 6, ch. 1, chacune modifiée;

Les «Clauses» ont le sens qui leur est attribué dans les SCC.

« Contrôleur » signifie soit: (a) le client, si le client est un utilisateur final ; (b) le bénéficiaire, si le client est un MSP ; ou (c) le client final, si le client est un OEM.

« Données personnelles du contrôleur » désigne les données personnelles que le fournisseur traite pour le compte du contrôleur conformément aux Services.

« Clauses du contrôleur au processeur » désigne le module deux clauses aux SCC. « Données CRM » désigne les informations de contact, de paiement ou de facturation, ou d'autres données personnelles concernant les contacts professionnels et les administrateurs du client, y compris le nom, l'adresse e-mail et les informations de contact, Que le fournisseur collecte et traite en son propre nom afin de gérer ses relations avec ses clients, de communiquer avec ses clients et partenaires commerciaux actuels, anciens et potentiels, et d'administrer ses relations commerciales.

« Objet des données » désigne la personne à qui les données personnelles Sophos sont liées.

« Demandes de sujets de données » désigne toute demande émanant de sujets de données exerçant des droits conformément aux lois applicables en matière de protection des données, y compris leurs droits d'accès, de suppression et de correction.

"EEE" désigne l'espace économique européen, y compris a) les États membres de l'espace économique européen ("EEE") et b) le Royaume-Uni.

«Client final» a la signification qui lui est donnée dans le Contrat OEM.

"Europe" (et "européenne") signifie a) les États membres de l'espace économique européen ("EEE") et b) le Royaume-Uni.

« produits hébergés» désigne les produits énumérés à l'Annexe 3.

« ICO » désigne le Bureau du Commissaire à l'information établi au Royaume-Uni

« Contrat principal » désigne, collectivement, le ou les contrats écrits, y compris et les pièces, addenda et modifications y afférentes, en vertu desquels le fournisseur fournit certains Services au client.

« Données personnelles » désigne toute information qui identifie, pourrait être utilisée pour identifier, est liée ou peut être raisonnablement liée à une personne ou un ménage particulier, ainsi que toute information définie comme « données personnelles », « informations personnelles » ou un terme équivalent selon les lois et réglementations applicables en matière de protection des données.

«Violation des données personnelles» désigne une violation de la sécurité (autre que celles causées par le client ou ses utilisateurs) qui entraîne la destruction, la perte, la modification, la divulgation non autorisée ou l'accès aux Données personnelles du contrôleur traitées par le fournisseur en vertu du présent Avenant.

« Processeur » désigne une personne ou une entité qui traite des données personnelles pour le compte et selon les instructions du contrôleur, y compris toute entité agissant en tant que « fournisseur de services » conformément à la CCPA.

« Transfert restreint » désigne un transfert de données personnelles du contrôleur par le client vers le fournisseur, où ce transfert serait interdit par les lois de protection des données applicables en l'absence des clauses contractuelles standard applicables et, le cas échéant, de l'Avenant britannique.

« Données sensibles » signifie « catégories spéciales de données personnelles », « données personnelles sensibles », « données sensibles », et terme équivalent tel que défini dans les lois applicables en matière de protection des données.

« Services » désigne tous les produits et/ou services fournis par le fournisseur conformément aux Contrat principal.

« clauses contractuelles types » ou « SCC » les clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers conformément au règlement (UE) 2016/679 du

Parlement européen et du Conseil approuvé par la Commission européenne dans sa décision d'application (UE) 2021/914 du 4 juin 2021;

« Sous-traitant » désigne toute personne ou entité (à l'exclusion de tout employé du fournisseur) ou entité nommée par ou au nom du fournisseur et qui traite les données personnelles du contrôleur.

« Autorité de surveillance » désigne l'autorité de régulation compétente en ce qui concerne les lois et règlements applicables en matière de protection des données, y compris, le cas échéant, une autorité de surveillance telle que définie dans le RGPD.

« Avenant Royaume-Uni » désigne l'Avenant international de transfert de données aux clauses contractuelles types de la Commission européenne, émis par l'ICO, tel que modifié ou remplacé de temps à autre par une autorité de surveillance compétente en vertu des lois sur la protection des données applicables du Royaume-Uni

2.2. Dans le présent Avenant, les termes minuscules «contrôleur», «processeur», «sujet des données», «données personnelles» et «traitement» (ainsi que leurs dérivés) ont la signification donnée dans la loi sur la protection des données applicable.

3. PORTÉE

3.1. L'objet et la durée du traitement des Données personnelles du contrôleur par le fournisseur, y compris la nature et l'objet du traitement, les types de Données personnelles du contrôleur à traiter et les catégories de sujets de données, doivent être décrits dans : (a) le présent Avenant ; (b) le Contrat principal ; (c) les instructions de l'Annexe 1 (instructions de traitement des données) ; et (d) les instructions du client émises conformément à la clause 4 ci-dessous.

3.2. Il incombe au client de s'assurer (a) que le contrôleur dispose d'une base légale pour le traitement des données personnelles du contrôleur qui seront effectuées par le fournisseur pour le compte du client, Et (b) que le contrôleur a obtenu tous les consentements nécessaires de la part des sujets de données qui peuvent être requis pour le traitement des données personnelles du contrôleur par le client et le fournisseur (y compris, mais sans s'y limiter, en ce qui concerne les données sensibles) ; Et (c) qu'elle est autrement conforme aux lois applicables en matière de protection des données et qu'elle veille à ce que ses instructions au fournisseur pour le traitement des données personnelles du contrôleur soient conformes à tous les égards.

3.3. Les parties conviennent que le fournisseur est un processeur ou un sous-processeur pour les données personnelles du contrôleur, et que le client est (a) le contrôleur où le client est un utilisateur final, ou (b) un processeur ((pour un contrôleur tiers) où le client est un MSP ou un OEM.

4. INSTRUCTIONS DU CLIENT

4.1. Le client demande au fournisseur de traiter les données personnelles du contrôleur comme étant raisonnablement nécessaires pour fournir et exécuter les Services et comme stipulé dans les présentes et dans les Contrat principal. Le fournisseur doit traiter les données personnelles du contrôleur conformément aux instructions de traitement documentées du client, comme indiqué dans le présent document, sauf (a) en cas d'accord écrit entre le fournisseur et le client ; Ou (b)

lorsque la loi le demande (auquel cas le fournisseur doit informer le client de cette obligation légale avant le traitement, sauf si cette loi interdit la fourniture de telles informations).

4.2. Si le fournisseur se rend compte que les instructions de traitement du client enfreignent les lois applicables en matière de protection des données (sans imposer aucune obligation au fournisseur de surveiller activement la conformité du client), il en informera rapidement le client et suspendra le traitement des Données personnelles du contrôleur.

4.3. Sans limiter l'absence, dans la mesure où la Loi sur la protection des renseignements personnels des consommateurs de la Californie («**CCPA**») s'applique aux données personnelles du contrôleur, le fournisseur convient également que :

4.3.1. Le fournisseur n'utilisera, ne divulguera ou ne traitera pas les données personnelles du contrôleur, sauf dans le but spécifique d'exécuter les Services, conformément aux termes du présent Avenant et du Contrat principal, et conformément aux lois applicables. Nonobstant ce qui précède :

a. Le fournisseur peut engager les sous-processeurs pour traiter les données personnelles du contrôleur, sous réserve des conditions de la Section 7 ;

b. Le fournisseur ne traitera pas les données personnelles du contrôleur en dehors de la relation commerciale directe entre le client et le fournisseur ou à des fins commerciales propres au fournisseur ; Nonobstant ce qui précède, les Parties conviennent que, dans la mesure où la LPA s'applique, le fournisseur ne traitera les données personnelles du contrôleur qu'aux fins commerciales spécifiques énoncées dans la Contrat principal et le présent Avenant ou à une autre fin expressément autorisée en vertu des règlements de la CCPA.

c. Le fournisseur ne « partagera » ni ne « vendra » (comme ces conditions sont définies dans la CCPA) aucune donnée personnelle du contrôleur ;

d. Le fournisseur (et s'assurera que chaque sous-transformateur se conformera à ses obligations en vertu de la CCPA et fournira le même niveau de protection de la vie privée que celui exigé par la CCPA; et

e. Si le fournisseur estime qu'il ne sera pas en mesure de se conformer aux conditions du présent Avenant ou aux lois applicables en matière de protection des données, Le fournisseur avisera rapidement le client et lui accordera le droit de prendre des mesures raisonnables et appropriées pour s'assurer que les données personnelles du contrôleur sont traitées de manière conforme aux obligations du contrôleur en vertu de la CCPA.

f. Le fournisseur ne conservera pas les données personnelles du contrôleur à l'expiration ou à la résiliation du Contrat principal, sauf comme stipulé dans la section **Error! Reference source not found.**;

5. OBLIGATIONS DU FOURNISSEUR

5.1. Tout le personnel du fournisseur qui traite les Données personnelles du contrôleur doit être correctement formé en ce qui concerne ses obligations en matière de protection, de sécurité et

de confidentialité des données et doit être soumis à des obligations écrites ou légales de maintien de la confidentialité.

5.2. Le fournisseur mettra en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité approprié au risque et pour protéger les Données personnelles du contrôleur contre une violation des données personnelles. Ces mesures prendront en compte l'état de la technique, les coûts de mise en œuvre et la nature, la portée,contexte et objectifs du traitement ainsi que le risque de variation de la probabilité et de la gravité des droits et libertés des personnes physiques afin d'assurer un niveau de sécurité approprié au risque. En particulier, les mesures prises par le fournisseur doivent inclure celles décrites à l'Annexe 2 du présent Avenant. Le fournisseur peut modifier ou modifier les mesures techniques et organisationnelles décrites à l'Annexe 2 sans le consentement écrit préalable du client, à condition que le fournisseur conserve un niveau de protection au moins équivalent. À la demande du client, le fournisseur fournira une description mise à jour des mesures techniques et organisationnelles sous la forme présentée à l'Annexe 2.

5.3. Le fournisseur doit respecter les exigences spécifiées à la clause 7 ci-dessous pour engager tout sous-traitant à traiter les données personnelles du contrôleur.

5.4. Le fournisseur doit respecter les exigences spécifiées dans la clause 8 ci-dessous pour aider le client à répondre aux demandes de renseignements émanant de tiers, y compris toute demande émanant de sujets de données d'exercer ses droits en vertu des lois applicables sur la protection des données.

5.5. Après avoir confirmé la survenue d'une violation de données personnelles, le fournisseur doit informer le client sans délai indu et doit fournir toutes les informations et la coopération nécessaires en temps opportun pour que le client puisse raisonnablement exiger pour le client (et, si le client est un MSP ou un OEM, son contrôleur)Pour remplir ses obligations de signalement des violations de données en vertu (et conformément aux délais requis par) de la loi sur la protection des données applicable. Le fournisseur prendra en outre les mesures et actions raisonnablement nécessaires pour remédier ou atténuer les effets de la violation des données personnelles et tiendra le client informé de tous les développements liés à la violation des données personnelles.

5.6. Le fournisseur doit fournir au client (ou, si le client est un MSP ou un OEM, son contrôleur) une assistance raisonnable et opportune en tant que client (ou, le cas échéant, le contrôleur) Peut exiger une évaluation de l'impact sur la protection des données ou toute autre évaluation requise par les lois applicables en matière de protection des données et, si nécessaire, consulter son autorité compétente en matière de protection des données. Cette assistance sera fournie aux frais du client.

5.7. Sauf disposition contraire de la loi en vigueur, le fournisseur doit supprimer les données personnelles du contrôleur dans un délai raisonnable après la résiliation ou l'expiration du présent Avenant, sauf si la loi en vigueur l'interdit. Sur demande, le fournisseur confirmera au client que ces données personnelles du contrôleur ont été supprimées conformément au présent Avenant. Si le fournisseur est tenu par les lois applicables de conserver les données personnelles du

contrôleur, il doit prendre des mesures pour assurer la confidentialité et la sécurité continues des données personnelles du contrôleur tant qu'elles sont conservées.

6. DROITS D'AUDIT DU CLIENT

6.1. Le client reconnaît que le fournisseur fait régulièrement l'objet d'un audit par des auditeurs tiers indépendants en fonction des normes SSAE 18 SOC 2. Sur demande raisonnable, le fournisseur doit fournir une copie de son rapport d'audit SOC 2 au client, qui est soumis aux dispositions de confidentialité du Contrat principal en tant qu'informations confidentielles du fournisseur. Le fournisseur doit également répondre à toute question d'audit raisonnable écrite soumise par le client, à condition que le client n'exerce pas ce droit plus d'une fois par an.

6.2. Si, de l'avis raisonnable du client, les matériaux fournis en vertu de la clause 6.1 sont insuffisants pour démontrer la conformité du fournisseur à cet Avenant, le client peut demander par écrit et sous réserve de la clause 6.2 (a) - (d) des présentes, Que le fournisseur met à la disposition du client toutes les informations raisonnablement nécessaires pour démontrer le respect des obligations énoncées dans le présent Avenant (y compris les clauses contractuelles standard dans la mesure applicable) et permettre et contribuer aux audits, y compris les inspections, par le client ou par le client indépendant, Auditeur tiers qui n'est pas un concurrent du fournisseur des activités de traitement couvertes par le présent Avenant.

a. Avant de demander un examen ou un audit conformément à la présente clause 6.2, le client tiendra compte des certifications et audits tiers du fournisseur concernés décrits à la clause 6.1 ;

b. Le client doit donner au processeur un préavis raisonnable, au moins 60 jours à l'avance, d'une demande d'audit ou d'inspection en vertu de la présente clause 6.2, et prendra (et veillera à ce que chacun de ses auditeurs prenne) des mesures raisonnables pour éviter et prévenir tout dommage ou blessure et minimiser toute interruption de cet audit ou de cette inspection ;

c. Un audit ou une inspection ne sera pas effectué plus d'une fois par an, sauf si une autorité de surveillance ou les lois applicables en matière de protection des données l'exigent ; et

d. Le client doit assumer la totalité des coûts d'un tel audit et rembourser le fournisseur pour les coûts et dépenses raisonnables engagés par le fournisseur dans le cadre de ces audits, y compris tout temps passé par le fournisseur, ses filiales ou ses sous-traitants pour un tel audit ou inspection aux tarifs de services professionnels actuels du fournisseur, Qui sera mis à la disposition du client sur demande.

7. SOUS-PRODUITS

7.1. Le client consent à utiliser les sous-processeurs existants du fournisseur à la date du présent Avenant, qui sont répertoriés à l'adresse https://www.sophos.com/fr-fr/legal(« liste des sous-processeurs »), ainsi que les filiales du fournisseur. Le client consent expressément à ce que le fournisseur engage des sous-traitants tiers supplémentaires (chacun étant un « nouveau sous-traitant ») sous réserve des conditions énoncées dans la présente clause 7. Le fournisseur fournira

au client un préavis de trente (30) jours avant l'ajout de tout nouveau sous-traitant, lequel peut être donné en affichant les détails de cet ajout à la liste des sous-traitants.

7.2. Si le client ne s'oppose pas par écrit à la nomination d'un nouveau sous-traitant par le fournisseur (pour des raisons raisonnables relatives à la protection des Données personnelles du contrôleur) dans les 30 jours suivant l'ajout du nouveau sous-traitant à la liste des sous-traitants,Le client accepte qu'il soit réputé avoir consenti à ce nouveau sous-processeur. Si le client présente une telle objection écrite au fournisseur, le fournisseur informera le client par écrit dans un délai de 30 jours : (a) le fournisseur n'utilisera pas le nouveau sous-processeur pour traiter les Données personnelles du contrôleur; ou (b) le fournisseur ne peut pas ou ne souhaite pas le faire. Si la notification au paragraphe (b) est donnée, le client peut, dans les 30 jours suivant cette notification,Choisir de mettre fin au présent Avenant et au Contrat principal concernant le traitement concerné sur notification écrite adressée au fournisseur et le fournisseur devra s'en prévaloir pour les clients situés dans l'espace économique européen et au Royaume-Uni uniquement,autoriser un remboursement ou un crédit au prorata des frais prépayés pour la période restant après la résiliation. Toutefois, si aucun avis de résiliation n'est fourni dans ce délai, le client sera réputé avoir consenti au nouveau sous-processeur. Le fournisseur imposera des conditions de protection des données aux nouveaux sous-processeurs qui imposent des protections équivalentes pour les données personnelles du contrôleur, comme le prévoit le présent Avenant. Le fournisseur restera entièrement responsable de l'exécution des obligations de chaque sous-traitant.

8. DEMANDES DE RENSEIGNEMENTS DE TIERS

8.1. Le fournisseur doit informer le client de toute demande de confidentialité, correspondance, demande ou plainte qu'il reçoit d'un sujet de données, d'un organisme de réglementation ou d'un autre tiers en rapport avec le traitement des données personnelles du contrôleur, en fournissant tous les détails de ces données, mais ne doit pas répondre directement au sujet de données, sauf si la loi l'exige autrement.

8.2. Dans la mesure nécessaire, le fournisseur fournira une assistance raisonnable et opportune au client (ou, si le client est un MSP ou un OEM, le contrôleur), aux frais du client, pour permettre au client (ou, si le client est un MSP ou un OEM, le contrôleur) de répondre à : (a) une demande émanant d'une donnée soumise à l'exercice de ses droits en vertu de la loi sur la protection des données applicable (y compris, le cas échéant, ses droits d'accès, de correction, d'objection, d'effacement et de portabilité des données, et (b) une demande reçue d'un organisme de réglementation ou d'un autre tiers en relation avec le traitement des données personnelles du contrôleur.

9. TRANSFERTS INTERNATIONAUX DE DONNÉES

9.1. Certains produits peuvent permettre au client de sélectionner l'emplacement d'hébergement des données personnelles du contrôleur pour ces produits, y compris dans les centres de données situés en dehors de la juridiction d'origine des données. Ces emplacements peuvent inclure (a) l'espace économique européen, (b) le Royaume-Uni, (c) les États-Unis d'Amérique, ou un autre emplacement tel que spécifié dans le Contrat principal (« emplacement de stockage central »).

Cette sélection a lieu au moment de l'installation du Produit, de la création de compte ou de la première utilisation du produit concerné. Une fois sélectionné, l'emplacement de stockage central ne peut pas être modifié à une date ultérieure.

9.2. Le client reconnaît et consent expressément, quel que soit l'emplacement de stockage central sélectionné (le cas échéant), aux transferts restreints, sous réserve du respect des obligations énoncées dans la présente clause 9.

9.3. En ce qui concerne les transferts restreints :

9.3.1. Les SCC et l'Avenant Royaume-Uni sont expressément incorporés aux présentes et font partie intégrante de cet Avenant ;

9.3.2. Sous réserve des dispositions de la Section 9.3.3 et de l'Annexe 4 des présentes, le client et le fournisseur s'engagent à : (i) les SCC, qui s'appliquent dans la mesure d'un transfert restreint des données personnelles du contrôleur au fournisseur ; Et (ii) l'Avenant Royaume-Uni, qui s'applique aux SCC, les modifie et les complète en ce qui concerne tout transfert restreint de données personnelles du contrôleur soumis aux lois et règlements sur la protection des données du Royaume-Uni ; et

9.3.3. Le module 2 des SCC s'applique, sous réserve des dispositions de l'Annexe 4 aux présentes.

9.4. L'Annexe des SCC doit être complété comme indiqué à l'Annexe 4 ci-dessous.

10. DURÉE

10.1. Le présent Avenant commence à (a) l'exécution par les deux parties de la Contrat principal ou (b) la date à laquelle la Contrat principal prend effet, si elle est ultérieure, et se poursuit jusqu'à la première de : (i) l'expiration du droit du client d'utiliser et de recevoir les produits, comme indiqué dans le Contrat principal ou sur tout droit de licence associé ; et (ii) la résiliation du Contrat principal.

11. AUTRES RÈGLEMENTS

11.1. Les modifications et les modifications apportées à cet Avenant nécessitent le formulaire écrit. Cela s'applique également aux modifications apportées à la présente clause11.1.

11.2. En aucun cas, la responsabilité du fournisseur envers le client en relation avec un problème découlant ou lié au présent Avenant ne peut dépasser les limites de responsabilité du fournisseur énoncées dans le Contrat principal. Les limitations de responsabilité du fournisseur énoncées dans le Contrat principal s'appliquent globalement à la fois au Contrat principal et au présent Avenant, de sorte qu'une seule limitation de responsabilité s'applique à la fois au Contrat principal et au présent Avenant.

11.3. Le présent Avenant (à l'exclusion des SCC) est régi et interprété conformément aux lois de l'Angleterre et du pays de Galles, sans égard aux principes de conflit de lois. Dans la mesure permise par la loi en vigueur, les tribunaux d'Angleterre auront compétence exclusive pour déterminer tout litige ou toute réclamation qui peut résulter de, en vertu ou en relation avec le présent Avenant.

11.4. En cas de conflit avec les termes de la présente Annexe sur le traitement des données et les termes de tout SCC conclu par les parties, les termes des SCC applicables (y compris les annexes), ont préséance.

12. MODIFICATIONS DE LA LOI

12.1. Si une modification du présent Avenant est requise à la suite d'une modification des lois applicables en matière de protection des données, l'une ou l'autre des parties peut fournir un avis écrit à l'autre partie de ce changement de loi. Les parties discuteront et négocieront de bonne foi les éventuelles modifications nécessaires au présent Avenant pour y remédier. Les parties ne refuseront pas, de manière déraisonnable, de consentir ou d'approuver la modification du présent Avenant conformément à la présente Section 12 ou autre.

12.2. Dans le cas où les clauses contractuelles standard ou l'Avenant au Royaume-Uni sont remplacées, mises à jour ou remplacées par une nouvelle version (« nouvelles clauses »), le client accepte que le fournisseur puisse, sur notification écrite préalable au client, mettre à jour cet Avenant si nécessaire pour incorporer ces nouvelles clauses, En tant que modification ou remplacement des clauses contractuelles standard précédentes ou de l'Avenant au Royaume-Uni.

Pièce 1

DESCRIPTION DU TRAITEMENT

La présente pièce 1 décrit le traitement que le fournisseur effectuera pour le compte du client.

(a) Objet, nature et objet des opérations de traitement

Les Données personnelles du contrôleur seront soumises aux activités de traitement de base suivantes (veuillez préciser) :

- Fourniture des produits achetés par le client dans le cadre et conformément à la Contrat principale
- Fournir des services de gestion de compte et d'assistance technique à la clientèle

Le fournisseur fournit des produits conçus pour détecter, prévenir et gérer ou aider le fournisseur à détecter, prévenir et gérer les menaces de sécurité au sein ou contre des systèmes, réseaux, appareils, fichiers et autres données mis à disposition par le client. Le contenu de toute information contenue dans ces systèmes, réseaux, appareils, fichiers et autres données est déterminé uniquement par le client et non par le fournisseur.

(b) Durée des opérations de traitement :

Les Données personnelles du contrôleur seront traitées pendant la durée suivante (veuillez préciser) :

Durée spécifiée dans le Contrat principal (ou pour la durée du Contrat principal, si elle n'est pas spécifiée autrement).

(c) Sujets de données

Les Données personnelles du contrôleur concernent les catégories de sujets de données suivantes (veuillez préciser) :

- Personnel et utilisateurs finaux des clients
- Autres sujets de données dont les données personnelles sont traitées pour le compte du client en rapport avec les produits Sophos

(d) Types de données personnelles

Les Données personnelles du contrôleur concernent les catégories de données suivantes (veuillez préciser) :

- Noms d’utilisateur et autres identifiants
- Informations sur le réseau et l'activité du réseau
- Autres informations pouvant être transmises ou traitées en relation avec les produits Sophos

(e) Catégories spéciales de données (le cas échéant)

Les Données personnelles du contrôleur concernent les catégories spéciales de données suivantes (veuillez préciser) :

Sauf indication contraire, les produits du fournisseur ne sont pas conçus pour traiter des catégories spéciales de données.

Pièce 2

MESURES TECHNIQUES ET ORGANISATIONNELLES

Certaines de ces mesures ne peuvent être pertinentes ou applicables qu'aux produits hébergés.

1. Contrôle d'accès physique.
   (a) Sophos a une politique de contrôle d'accès physique ;
   (b) tout le personnel porte des ID / badges d'accès ;
   (c) les entrées des installations sont protégées par des badges ou des clés d'accès ;
   (d) les installations sont divisées en (i) zones d'accès public (telles que les zones de réception), (ii) zones d'accès général du personnel, Et (iii) les zones d'accès restreint auxquelles seul le personnel ayant un besoin commercial explicite peut accéder ;
   (e) les badges et les clés d'accès contrôlent l'accès aux zones restreintes de chaque installation en fonction des niveaux d'accès autorisés d'une personne ;
   (f) les niveaux d'accès des personnes sont approuvés par les membres du personnel supérieur et vérifiés sur une base trimestrielle ;
   (g) le personnel de réception et/ou de sécurité est présent aux entrées des sites plus importants ;
   (h) les installations sont protégées par des alarmes ;
   (i) les visiteurs sont préenregistrés et les registres des visiteurs sont conservés.

2. Contrôle d'accès au système.
   (a) Sophos a une stratégie de contrôle d'accès logique ;
   (b) le réseau est protégé par des pare-feu à chaque connexion Internet ;
   (c) le réseau interne est segmenté par des pare-feu en fonction de la sensibilité des applications ;
   (d) IDS et autres contrôles de détection et de blocage des menaces exécutés sur tous les pare-feu ;
   (e) le filtrage du trafic réseau repose sur des règles qui appliquent le principe du « moindre accès » ;
   (f) les droits d'accès ne sont accordés qu'au personnel autorisé dans la mesure et la durée nécessaires à l'exécution de ses fonctions et sont révisés trimestriellement ;
   (g) l'accès à tous les systèmes et applications est contrôlé par une procédure de connexion sécurisée ;
   (h) les individus ont des ID utilisateur et des mots de passe uniques pour leur propre usage ;
   (i) les mots de passe sont testés et les modifications sont appliquées aux mots de passe faibles ;
   (j) les écrans et les sessions se verrouillent automatiquement après une période d'inactivité ;
   (k) les produits de protection contre les programmes malveillants Sophos sont installés en standard ;
   (l) des analyses de vulnérabilité régulières sont effectuées sur les adresses IP et les systèmes ;

(m) les systèmes sont corrigés sur un cycle régulier avec un système de hiérarchisation pour un suivi rapide des correctifs urgents.

3. Contrôle d'accès aux données.
   (a) Sophos dispose d'une stratégie de contrôle d'accès logique ;
   (b) les droits d'accès ne sont accordés qu'au personnel autorisé dans la mesure et pendant la durée nécessaires à l'exécution de ses fonctions et sont révisés trimestriellement ;
   (c) l'accès à tous les systèmes et applications est contrôlé par une procédure de connexion sécurisée ;
   (d) les utilisateurs disposent d'ID utilisateur et de mots de passe uniques pour leur propre usage ;
   (e) les mots de passe sont testés et les modifications sont appliquées aux mots de passe faibles ;
   (f) les écrans et les sessions se verrouillent automatiquement après une période d'inactivité ;
   (g) les ordinateurs portables sont cryptés à l'aide des produits Sophos chiffrement ;
   (h) les expéditeurs doivent prendre en compte le fichier chiffrement avant d'envoyer un e-mail externe.

4. Contrôle d'entrée.
   (a) l'accès à tous les systèmes et applications est contrôlé par une procédure de connexion sécurisée ;
   (b) les individus ont des ID utilisateur et des mots de passe uniques pour leur propre utilisation ;
   (c) les produits Sophos Central utilisent la couche de transfert chiffrement pour protéger les données en transit ;
   (d) la communication entre le logiciel client et le système Sophos principal est effectuée via HTTPS pour sécuriser les données en transit, établissant une communication sécurisée via des certificats et la validation du serveur.

5. Contrôle du sous-traitant.
   (a) les sous-traitants ayant accès aux données entreprennent une procédure de vérification de la sécurité INFORMATIQUE avant l'intégration et comme requis par la suite ;
   (b) les contrats contiennent des obligations appropriées en matière de confidentialité et de protection des données, fondées sur les devoirs du sous-traitant.

6. Contrôle de disponibilité.
   (a) Sophos protège ses locaux contre les risques d'incendie, d'inondation et autres risques environnementaux ;
   (b) des générateurs de secours sont disponibles pour entretenir les alimentations en cas de coupure de courant ;
   (c) les centres de données et les salles de serveurs utilisent les contrôles et la surveillance de la température ;
   (d) le système Sophos Central est équilibré en charge et dispose d'un basculement entre

trois sites, chacun exécutant deux instances du logiciel, dont chacune est capable de fournir le service complet.

7. Contrôle de la ségrégation.
   (a) Sophos maintient et applique un processus de contrôle qualité pour le déploiement de nouveaux produits clients ;
   (b) les environnements de test et de production sont séparés ;
   (c) les nouveaux logiciels, systèmes et développements sont testés avant leur mise en production.

8. Contrôle organisationnel.
   (a) Sophos dispose d'une équipe dédiée à la sécurité INFORMATIQUE ;
   (b) l'équipe de gestion des risques et de la conformité gère les contrôles et rapports internes sur les risques, notamment les rapports sur les risques clés pour la direction ;
   (c) un processus de réponse aux incidents identifie et corrige les risques et les vulnérabilités en temps opportun ;
   (d) chaque nouvel employé entreprend une formation sur la protection des données et la sécurité INFORMATIQUE ;
   (e) le département SÉCURITÉ INFORMATIQUE mène des campagnes trimestrielles de sensibilisation à la sécurité.

Pièce 3

PRODUITS HEBERGES

(a) Sophos Central
(b) Sophos Cloud Optix
(c) Central Device Encryption
(d) Central Endpoint Protection
(e) Central Endpoint Intercept X
(f) Central Endpoint Intercept X Advanced
(g) Central Mobile Advanced
(h) Central Mobile Standard
(i) Central Phish Threat
(j) Central Intercept X Advanced for Server
(k) Central Server Protection
(l) Central Mobile Security
(m) Central Web Gateway Advanced
(n) Central Web Gateway Standard
(o) Central Email Standard
(p) Central Email Advanced
(q) Central Wireless Standard
(r) Tout autre produit Sophos administré et utilisé avec Sophos Central

Pièce 4

CONDITIONS SUPPLÉMENTAIRES POUR LES TRANSFERTS RESTREINTS

La présente pièce jointe inclut des conditions supplémentaires applicables aux transferts restreints effectués par ou au nom du client vers le fournisseur, conformément à l'addendum, ainsi que les informations nécessaires pour compléter les annexes (annexes I à III) aux SCC applicables.

En acceptant l'Avenant, les Parties conviennent d'exécuter les SCC dans toutes les parties pertinentes, sous réserve de la Section **Error! Reference source not found.** de l'Avenant et des termes de la présente Annexe.

1. Les termes en majuscules utilisés mais non définis dans la présente Annexe ou dans l'Avenant ont la signification qui leur est attribuée en vertu des SCC et de l'Avenant au Royaume-Uni, le cas échéant.

2. Le module 2 des SCC s'applique, sous réserve des termes de la présente Annexe et l'Annexe des SCC doit être remplie en référence à l'Annexe A aux présentes.

3. Pour les besoins des SCC (module 2) :

3.1. Clause 7 : la clause facultative d'amarrage ne s'applique pas;

3.2. Clause 9(a) : L'option 2 (autorisation générale) s'applique et l'importateur de données avise l'exportateur de données par écrit au moins 30 jours à l'avance de toute modification envisagée.

3.3. Clause 11 : la langue facultative ne s'applique pas.

3.4. Aux fins de l'alinéa 13 a), l'autorité de surveillance compétente s'applique comme suit :

3.4.1. Lorsque l'exportateur de données est établi dans un État membre de l'UE, l'autorité de surveillance est l'autorité de surveillance compétente pour la juridiction dans laquelle l'exportateur de données est établi;

3.4.2. Lorsque l'exportateur de données est établi au Royaume-Uni ou que le transfert restreint est soumis aux lois et règlements sur la protection des données du Royaume-Uni, l'autorité de surveillance compétente est le bureau du commissaire à l'information du Royaume-Uni;

3.4.3. Lorsque l'exportateur de données est établi en Suisse ou que le transfert restreint est soumis aux lois et règlements sur la protection des données de Suisse, le commissaire fédéral suisse à la protection des données et à l'information agit en qualité d'autorité de surveillance compétente; et

3.4.4. Lorsque l'exportateur de données n'est pas établi dans un État membre de l'UE, au Royaume-Uni ou en Suisse, Mais relève du champ d'application territorial du règlement (UE) 2016/679 conformément à son article 3, paragraphe 2, l'autorité de surveillance sera l'autorité de surveillance compétente pour la juridiction

dans laquelle le représentant de l'exportateur de données est établi, à savoir le commissaire à la protection des données de l'Irlande.

4. Aux fins de la Clause 17 et de la Clause 18(b), respectivement, les SCC sont régies par les lois de la République d'Irlande les litiges seront réglés devant les tribunaux irlandais, à l'exception de ce qui suit : (i) lorsque l'exportateur de données est établi en Suisse ou que le transfert restreint est soumis aux lois et règlements de la Suisse sur la protection des données, les SCC sont régies par les lois de la Suisse et les litiges sont réglés devant les tribunaux de la Suisse ; Et (ii) lorsque l'exportateur de données est établi au Royaume-Uni ou que le transfert restreint est soumis aux lois et règlements sur la protection des données du Royaume-Uni, les SCC sont régies par les lois du Royaume-Uni et les litiges sont réglés devant les tribunaux du Royaume-Uni.

5. **Conditions supplémentaires pour la Suisse**. Lorsque l'exportateur de données est établi en Suisse ou que le transfert restreint est soumis aux lois et règlements sur la protection des données de la Suisse : (i) les références dans les SCC à «Union européenne», «Union» ou «État membre» désignent la Suisse; (ii) les références au RGPD comprennent également la référence aux dispositions équivalentes de la loi fédérale suisse sur la protection des données (telle que modifiée ou remplacée); Et (iii) les SCC s'appliquent également au transfert d'informations relatives à une entité juridique identifiée ou identifiable dans la mesure où ces informations sont protégées en tant que données personnelles en vertu des lois et réglementations applicables en matière de protection des données de la Suisse.

6. **Conditions supplémentaires pour le Royaume-Uni** . Lorsque l'exportateur de données est établi au Royaume-Uni ou que le transfert restreint est soumis aux lois et règlements sur la protection des données du Royaume-Uni :

6.1. Les SCC doivent être lues conformément aux dispositions de la partie 2 (clauses obligatoires) de l'Avenant au Royaume-Uni et réputées modifiées par celles-ci ; et

6.2. Aux fins de la partie un, les tableaux 1 et 2 sont remplis avec référence aux annexes A et B (le cas échéant) de la présente pièce, le tableau 3 est rempli avec référence aux renseignements de la présente pièce, Aux fins du tableau 4, l'importateur de données peut mettre fin à l'addendum du Royaume-Uni, tel qu'il est défini à la section 19 de l'addendum du Royaume-Uni.

Annexe A à la pièce 4

ANNEXE AUX SCC (MODULE 2) : TRANSFERTS RESTREINTS ENTRE LE CONTROLEUR ET LE PROCESSEUR

ANNEXE I

A. LISTE DES PARTIES

1. Exportateur(s) de données : [*identité et coordonnées de l'exportateur(s) de données et, le cas échéant, de son responsable de la protection des données et/ou de son représentant dans l'Union européenne]*

Nom	Fourni au fournisseur en vertu du Contrat principal
Adresse	Fourni au fournisseur en vertu du Contrat principal
Autres informations nécessaires pour identifier l'Organisation	Fourni au fournisseur en vertu du Contrat principal
Nom de la personne à contacter : Position : Coordonnées :	Fourni au fournisseur en vertu du Contrat principal
Activités relatives aux données transférées en vertu des présentes SCC	Comme indiqué à la clause 3 de l'Avenant ci-dessus
Rôle	Contrôleur

Signature et date de l'exportateur de données : Les SCC (module 2), ainsi que la présente annexe et les annexes du présent document, sont exécutés dans le cadre de l'addendum.

2. **Importateur(s) de données :** [*identité et coordonnées du ou des importateurs de données, y compris toute personne de contact responsable de la protection des données]*

Nom	Sophos Limited (pour et pour le compte de ses filiales européennes et suisses)
Adresse	The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni

Autres informations nécessaires pour identifier l'Organisation	Numéro d'enregistrement 2096520
Nom de la personne à contacter : Position : Coordonnées :	Conseiller en matière de confidentialité dataprotection@sophos.com
Activités relatives aux données transférées en vertu des présentes SCC	Conformément à la Contrat

Signature et datede l'importateur de données : Les SCC (module 2), ainsi que la présente annexe et les annexes du présent document, sont exécutés dans le cadre de l'addendum.

B. DESCRIPTION DU TRANSFERT

1.1. Catégories de *sujets de données dont les données personnelles sont transférées.*

Tel qu'énoncé à l'annexe 1, partie A.

1.2 Catégories de *données personnelles transférées.*

Tel qu'énoncé à l'annexe 1, partie A.

Données sensibles transférées (le cas échéant) et application de restrictions ou de mesures de protection qui tiennent pleinement compte de la nature des données et des risques encourus, comme par exemple la limitation à des fins strictes, les restrictions d'accès (y compris l'accès uniquement pour le personnel ayant suivi une formation spécialisée), la tenue d'un registre d'accès aux données,restrictions relatives aux transferts ou mesures de sécurité supplémentaires.

Aucune.

La fréquence du transfert (par exemple, si les données sont transférées de manière ponctuelle ou continue).

Continu.

Nature *du traitement*

Fournir les services acquis par Sophos dans le cadre et conformément à la Contrat.

But(s) du transfert de données et du traitement ultérieur

Le fournisseur traitera les données personnelles du contrôleur si nécessaire pour exécuter les Services conformément à la Contrat et conformément aux instructions de Sophos dans son utilisation des Services.

La période pour laquelle les données personnelles seront conservées ou, si cela n'est pas possible, les critères utilisés pour déterminer cette période

Sous réserve de la Section 10 de l'Avenant, le fournisseur traitera les données personnelles pendant toute la durée du Contrat, sauf accord écrit contraire.

Pour les transferts aux (sous-) transformateurs, préciser également l'objet, la nature et la durée du traitement

Le fournisseur est autorisé à utiliser les sous-processeurs comme notifié par le fournisseur à Sophos au moment de l'exécution de la Contrat ou de l'Avenant.

C. AUTORITÉ DE SURVEILLANCE COMPÉTENTE

Comme indiqué à la section 3.4 de l'annexe 4 de l'addenda.

ANNEXE II - MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À ASSURER LA SÉCURITÉ DES DONNÉES

Comme indiqué à l'Annexe 2 de l'Avenant.

ANNEXE III – LISTE DES SOUS-PROCESSEURS

Sans objet (les parties ont accepté l'option 2 (autorisation générale) en ce qui concerne l'alinéa 9 a) des SCC).