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 document et sa traduction, seule la version anglaise prévaudra.

ADDENDA RELATIF AU TRAITEMENT DES DONNÉES

Date de révision : 20 janvier 2022.

Si cet addenda relatif au traitement des données («**Addenda**») est expressément incorporé par référence dans un contrat (« **Contrat principal** ») 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 addenda fait partie du Contrat principal et est en vigueur entre le fournisseur et le client.

1. PREAMBULE

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.aspx («**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, le traitement et l'utilisation des données du contrôleur par le fournisseur pour le client. Le présent addendum énonce les obligations des parties en ce qui concerne ce traitement de données et complète les conditions générales du Contrat principal.

1.4 Le Contrat principal, le présent Addendum et les documents expressément mentionnés dans le Contrat principal et le présent Addendum 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. DEFINITIONS

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

«**Lois applicables en matière de protection des données**» désigne (i) 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**»);(ii) la directive e-Privacy (directive 2002/58/ce de l'UE); et (iii) toute législation nationale applicable en matière de protection des données, y compris la législation adoptée en vertu des points (i) ou (ii); 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.

"**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 du contrôleur**» désigne toutes les données personnelles pour lesquelles le contrôleur est le contrôleur en vertu des lois applicables en matière de protection des données.

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

«**Europe**» (et «**Europe**») signifie (i) les États membres de l'espace économique européen («**EEE**»), et (ii) avec effet immédiat après la date à partir de laquelle le droit de l'Union européenne ne s'applique plus au Royaume-Uni, au Royaume-Uni.

« clauses contractuelles types de l'UE » ou « CSC de l'UE » 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;

« clauses du contrôleur à l'organisme de traitementde l'UE » désigne le module deux clauses aux CSC de l'UE;

« clauses du processeur à processeur de l'UE» désigne le module trois clauses des CSC de l'UE.

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

«**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 à,Données du contrôleur traitées par le fournisseur en vertu du présent addendum.

«**UK Addendum**» désigne l'addendum aux CSC de l'UE figurant dans l'Annexe, le cas échéant.

2.2 Dans le présent addenda, 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. **PORTEE**

3.1 L'objet et la durée du traitement des données du contrôleur par le fournisseur, y compris la nature et l'objet du traitement, les types de données du contrôleur à traiter et les catégories de sujets de données, doivent être décrits dans : (i) le présent addendum; (ii) le Contrat principal; (iii) les instructions figurant **à la pièce 1**;Et (v) les instructions du client publiées conformément à la Clause 4.

3.2 Il incombe au client de s'assurer (i) que le contrôleur dispose d'une base légale pour le traitement des données du contrôleur qui seront effectuées par le fournisseur en son nom,Et (ii) 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 du contrôleur par le client et le fournisseur (y compris, mais sans s'y limiter, en ce qui concerne des catégories spéciales de données) ;Et (iii) qu'il est autrement conforme aux lois applicables en matière de protection des données et qu'il s'assurera que ses instructions au fournisseur pour le traitement des données du contrôleur sont conformes à tous les égards.

3.3 Les autres dispositions du présent Addenda décrivent les obligations respectives des parties en ce qui concerne les données du contrôleur pour lesquelles : (i) le client est le

contrôleur et le fournisseur est le processeur, si le client est un utilisateur final ; ou (ii) le client est le processeur d'un contrôleur tiers, et le fournisseur est le sous-processeur, si le client est un MSP ou un OEM.

4. INSTRUCTIONS DU CLIENT

4.1 Le fournisseur doit traiter les données du contrôleur conformément aux instructions de traitement documentées du client, telles que définies exclusivement dans l'Article 3.1 , sauf :

(a) Si le fournisseur et le client en ont convenu autrement par écrit ; ou

(b) Lorsque la loi l'exige (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 du contrôleur.

5. OBLIGATIONS DU FOURNISSEUR

5.1 tout le personnel du fournisseur qui traite les données 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 de maintien de la confidentialité.

5.2 le fournisseur mettra en œuvre, à ses frais, les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité approprié au risque et pour protéger les données 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 Addendum. 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 pour engager tout sous-processeur à traiter les données du contrôleur.

5.4 le fournisseur doit respecter les exigences spécifiées à la Clause 8 pour aider le client à répondre aux demandes de renseignements émanant de tiers, y compris les demandes émanant de sujets de données d'exercer leurs droits en vertu des lois sur la protection des données applicables.

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 toutes les mesures et actions 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) toute l'assistance raisonnable et opportune dont le client (ou, le cas échéant, le contrôleur) peut avoir besoin pour effectuer une évaluation de l'impact sur la protection des données et, si nécessaire,consultez son autorité de protection des données. Cette assistance sera fournie aux frais du client.

5.7 le fournisseur doit supprimer les données du contrôleur dans un délai raisonnable suivant la résiliation ou l'expiration du présent Addendum, dans chaque cas si et dans la mesure permise par la législation européenne applicable.

5.8 le fournisseur doit respecter les exigences spécifiées dans la clause 6 pour fournir au client (et, si le client est un MSP ou un OEM, son contrôleur) les informations nécessaires pour démontrer le respect par le fournisseur des obligations énoncées dans le présent Addendum.

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, 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 client reconnaît et accepte que l'auditeur tiers qui a rédigé un tel rapport («**auteur**») n'accepte aucune responsabilité envers le client ou les auditeurs du client, sauf si le client conclut un Contrat de diligence distinct avec l'auteur. Le fournisseur doit également répondre à toute question d'audit écrite soumise par le client, à condition que le client n'exerce pas ce droit plus d'une fois par an.

7. SOUS-PRODUITS

7.1 le client consent aux sous-processeurs existants du fournisseur à la date du présent Addendum, qui sont énumérés à l'adresse https://www.sophos.com/en-us/legal («**liste des sous-processeurs**»). Le fournisseur ne sous-traite pas le traitement des données du contrôleur à des sous-processeurs tiers supplémentaires (chacun étant un «**nouveau sous-processeur**») sans notification préalable au client. Le fournisseur doit fournir un avis préalable de l'ajout de tout nouveau sous-traitant (y compris les détails généraux du traitement qu'il effectue ou qu'il effectuera), lequel avis peut être donné en publiant les détails de cet ajout dans la liste des sous-traitants. 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 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 : (i) le fournisseur n'utilisera pas le nouveau sous-processeur pour traiter les données du contrôleur ; ou (ii) le fournisseur ne peut pas ou ne souhaite pas le faire. Si la notification au paragraphe (ii) est donnée, le client peut, dans les 30 jours suivant cette notification,Choisir de mettre fin au présent Addendum 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-traitants afin de protéger les données du contrôleur conformément aux normes prévues par le présent Addendum et le fournisseur restera entièrement responsable de toute violation de cet Addendum causée par un tel sous-processeur.

8. DEMANDES DE RENSEIGNEMENTS DE TIERS

8.1 le fournisseur doit fournir toute l'assistance raisonnable et en temps opportun au client (ou, si le client est un MSP ou un OEM, le contrôleur), aux frais du client, pour lui permettre de répondre à : (i) toute demande émanant d'une donnée soumise à l'exercice de l'un de ses droits en vertu de la loi sur la protection des données applicable (y compris ses droits d'accès, de correction, d'objection, d'effacement et de portabilité des données, le cas échéant) ;Et (ii) toute autre correspondance, enquête ou plainte reçue d'un sujet de données, d'un organisme de réglementation ou d'un autre tiers en relation avec le traitement des données du contrôleur. Si une telle demande, correspondance, demande ou plainte est faite directement au fournisseur, le fournisseur doit en informer rapidement le client en fournissant tous les détails.

9. TRANSFERTS INTERNATIONAUX DE DONNÉES

9.1 certains produits permettent au client de choisir d'héberger les données du contrôleur de ces produits dans des centres de données situés dans (i) l'espace économique européen, (ii) le Royaume-Uni ou (iii) les États-Unis d'Amérique («**emplacement de stockage central**»). Cette sélection a lieu au moment de l'installation, 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 accepte que, quel que soit l'emplacement de stockage central sélectionné (le cas échéant), les données du contrôleur peuvent être exportées vers d'autres juridictions (à l'intérieur et/ou à l'extérieur du Royaume-Uni et de l'espace économique européen) : (i) à l'équipe mondiale de techniciens et d'ingénieurs de Sophos pour les programmes malveillants, les menaces de sécurité et l'analyse des faux positifs, ainsi qu'à des fins de recherche et de développement, (ii) afin de fournir une assistance technique et client, la gestion de compte, la facturation et d'autres fonctions auxiliaires, et (iii) comme décrit expressément dans la documentation référencée à la Clause 3.1.

9.3 le fournisseur ne doit pas transférer les données du contrôleur (ni autoriser le traitement des données du contrôleur à partir ou à l'entrée)Un pays en dehors de l'Europe, sauf si le transfert est effectué dans un pays jugé adéquat par les lois sur la protection des données en vigueur ou si le fournisseur prend les mesures nécessaires pour s'assurer que le transfert est conforme aux lois sur la protection des données en vigueur, y compris, par exemple, mais sans s'y limiter,Par l'utilisation des CSC de l'UE (telles que modifiées de temps à autre).

9.4 la restriction de transfert décrite à la clause 9.3 s'applique également aux transferts de données de contrôleur de l'espace économique européen vers le Royaume-Uni si et lorsque le Royaume-Uni cesse d'être soumis au droit de l'Union européenne.

9.5 si la clause 9.3 s'applique parce que le fournisseur ou une filiale du fournisseur traitera les données du contrôleur dans un pays en dehors du Royaume-Uni ou de l'EEE, dans ce cas (et uniquement dans la mesure où pour tout transfert de données du contrôleur,Aucune autre mesure reconnue en vertu des lois de protection des données applicables pour permettre de tels transferts n'est disponible (par exemple, sans s'y limiter,Transfert à un destinataire dans un pays considéré comme fournissant une protection adéquate des données personnelles en vertu des lois applicables sur la protection des données ou transfert à un destinataire ayant obtenu une autorisation obligatoire conformément aux lois applicables sur la protection des données) pour tout transfert de données du contrôleur,les parties conviennent que :

(A) pour les transferts de l'EEE, les clauses du contrôleur de l'UE vers le processeur s'appliquent et ces CSC de l'UE sont incorporés par renvoi dans le présent Addendum;

(b) pour les transferts depuis le Royaume-Uni, les clauses du contrôleur de l'UE vers le processeur s'appliquent (et ces CSC de l'UE sont par la présente incorporées par

référence dans le présent Addendum) à condition que ces clauses du contrôleur de l'UE vers le processeur soient soumises à l'Addendum du Royaume-Uni.

9.6 si la clause 9.3 s'applique parce que le fournisseur ou une filiale du fournisseur traitera les données du contrôleur dans un pays en dehors du Royaume-Uni ou de l'EEE, dans ce cas (et uniquement dans la mesure où pour tout transfert de données du contrôleur,Aucune autre mesure reconnue en vertu des lois de protection des données applicables pour permettre de tels transferts n'est disponible (par exemple, sans s'y limiter,Transfert à un destinataire dans un pays considéré comme fournissant une protection adéquate des données personnelles en vertu des lois applicables en matière de protection des données ou transfert à un destinataire ayant obtenu une autorisation de règles d'entreprise contraignantes conformément aux lois applicables en matière de protection des données)) lorsque(Conformément à la clause 3.3(ii)) le client est le responsable de la gestion d'un contrôleur tiers et le fournisseur est le sous-responsable, les parties conviennent que :

(A) pour les transferts de l'EEE, les clauses de l'UE relatives aux processeurs s'appliquent et ces CSC de l'UE sont incorporés par renvoi dans le présent Addendum;

(b) pour les transferts en provenance du Royaume-Uni, les clauses de l'Union européenne relatives aux processeurs s'appliquent (et ces CSC de l'Union européenne sont par la présente incorporées par référence dans le présent Addendum) à condition que ces clauses de l'Union européenne relatives aux processeurs soient soumises à l'Addendum du Royaume-Uni.

9.7 l'Annexe des CSC de l'UE doit être complété comme indiqué à la pièce 4 ci-dessous.

9.8 Pour chaque module des CSC de l'UE, le cas échéant :

(a) La clause d'arrimage facultative de la clause 7 ne s'applique pas;

(b) L'option 2 de la clause 9 s'applique. L'importateur de données notifie à l'exportateur de données, 30 jours à l'avance, toute modification prévue (par ajout ou remplacement) à la liste des sous-transformateurs.

(c) À l'article 11, la langue facultative ne s'applique pas;

(d) Pour l'application des articles 13(a) :

- Lorsque l'exportateur de données est établi dans un État membre de l'UE: L'autorité de surveillance chargée d'assurer le respect par l'exportateur de données du règlement (UE) 2016/679 en ce qui concerne le transfert de données est l'autorité de surveillance compétente lorsque l'exportateur de données est établi et agit en tant qu'autorité de surveillance compétente.

(e) Aux fins de la clause 17, les CSC de l'UE sont régies par le droit de l'État membre de l'UE dans lequel l'exportateur de données est établi;

(f) Aux fins de la clause 18(b), les litiges seront réglés devant les tribunaux de l'État membre de l'UE dans lequel l'exportateur de données est établi.

10. DURÉE

10.1 le présent addendum commence à l'exécution par les deux parties du Contrat principal (ou à la date à laquelle le Contrat principal prend effet, le cas échéant) 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 Addendum nécessitent le formulaire écrit. Cela s'applique également aux modifications apportées à la présente clause 11.1.

11.2 en aucun cas, la responsabilité du fournisseur envers le client en relation avec un problème découlant ou lié au présent Addendum 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 à l'addendum principal et au présent addendum, de sorte qu'une seule limitation de responsabilité s'applique à la fois au Contrat principal et au présent addendum.

11.3 le présent Addendum 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 Addendum.

11.4 en cas de conflit avec les termes de la présente Annexe sur le traitement des données et les termes de toute CSC conclue par les parties, les termes des CSC de l'UE applicables prévalent.

Pièce 1
Instructions de traitement des données

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

1. Fourniture des produits achetés par le client dans le cadre et conformément à la Contrat principale
2. 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 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 du contrôleur concernent les catégories de sujets de données suivantes (veuillez préciser) :

Les sujets de données comprennent les personnes sur lesquelles les données sont fournies au fournisseur via les produits par (ou sur la direction de) le client ou les utilisateurs finaux du client.

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

Les données relatives aux personnes fournies au fournisseur via les produits, par (ou sur la direction du) client ou par les utilisateurs finaux du client, telles que les coordonnées

(E) catégories spéciales de données (le cas échéant)
Les données 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.

A) Contrôle d'accès physique.

- Sophos dispose d'une stratégie de contrôle d'accès physique ;
- Tous les employés portent des badges d'identification/d'accès ;
- Les entrées des installations sont protégées par des badges d'accès ou des clés;
- Les installations sont divisées en (i) zones d'accès public (telles que les zones d'accueil), (ii) zones d'accès général au personnel et (iii) zones d'accès restreint auxquelles seuls les employés ayant un besoin commercial exprès peuvent accéder;
- 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;
- Les niveaux d'accès des personnes sont approuvés par les membres supérieurs du personnel et vérifiés sur une base trimestrielle;
- Le personnel de la réception et/ou de la sécurité est présent aux entrées des grands sites;
- Les installations sont protégées par des alarmes ;
- Les visiteurs sont préenregistrés et les journaux des visiteurs sont conservés.

B) Contrôle d'accès au système.

- Sophos dispose d'une stratégie de contrôle d'accès logique ;
- Le réseau est protégé par des pare-feu à chaque connexion Internet ;
- Le réseau interne est segmenté par des pare-feu en fonction de la sensibilité des applications ;
- LES ID et autres contrôles de détection et de blocage des menaces s'exécutent sur tous les pare-feu ;
- Le filtrage du trafic réseau repose sur des règles qui appliquent le principe du « moindre accès »;
- 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 ;
- L'accès à tous les systèmes et applications est contrôlé par une procédure de connexion sécurisée ;
- Les personnes ont des ID utilisateur et des mots de passe uniques pour leur propre usage;
- Les mots de passe sont soumis à des tests de résistance et les modifications sont appliquées aux mots de passe faibles ;
- Les écrans et les sessions se verrouillent automatiquement après une période d'inactivité ;
- Les produits de protection contre les programmes malveillants Sophos sont installés en standard ;
- Des analyses régulières des vulnérabilités sont effectuées sur les adresses IP et les systèmes ;
- Les systèmes sont corrigés sur un cycle régulier avec un système de hiérarchisation pour un suivi rapide des correctifs urgents.

C) Contrôle d'accès aux données.

- Sophos dispose d'une stratégie de contrôle d'accès logique ;

- 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 ;
- L'accès à tous les systèmes et applications est contrôlé par une procédure de connexion sécurisée ;
- Les personnes ont des ID utilisateur et des mots de passe uniques pour leur propre usage;
- Les mots de passe sont soumis à des tests de résistance et les modifications sont appliquées aux mots de passe faibles ;
- Les écrans et les sessions se verrouillent automatiquement après une période d'inactivité ;
- Les ordinateurs portables sont cryptés à l'aide des produits Sophos chiffrement ;
- Les expéditeurs sont dirigés de considérer le fichier chiffrement avant d'envoyer un e-mail externe.

D) Contrôle d'entrée.

- L'accès à tous les systèmes et applications est contrôlé par une procédure de connexion sécurisée ;
- Les personnes ont des ID utilisateur et des mots de passe uniques pour leur propre usage;
- Les produits Sophos Central utilisent la couche de transfert chiffrement pour protéger les données en transit ;
- La communication entre le logiciel client et le système Sophos dorsal est effectuée via HTTPS pour sécuriser les données en transit, établissant une communication sécurisée via des certificats et la validation du serveur.

E) Contrôle du sous-traitant.

- Les sous-traitants ayant accès aux données entreprennent une procédure DE vérification DE la sécurité INFORMATIQUE avant l'intégration et selon les besoins suivants ;
- Les contrats comportent des obligations appropriées en matière de confidentialité et de protection des données, fondées sur les obligations du sous-traitant.

F) Contrôle de disponibilité.

- Sophos protège ses locaux contre les risques d'incendie, d'inondation et autres risques environnementaux;
- Des générateurs de secours sont disponibles pour maintenir les alimentations en cas de coupure de courant ;
- Les centres de données et les salles de serveurs utilisent les contrôles et la surveillance de la température;
- 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.

G) Contrôle de la ségrégation.

- Sophos maintient et applique un processus de contrôle qualité pour le déploiement de nouveaux produits clients ;
- Les environnements de test et de production sont séparés ;
- Les nouveaux logiciels, systèmes et développements sont testés avant leur mise en production.

H) Contrôle organisationnel.

- Sophos dispose d'une équipe dédiée à la sécurité INFORMATIQUE ;
- L'équipe de gestion des risques et de la conformité gère les rapports et les contrôles internes sur les risques, notamment les rapports sur les principaux risques pour la direction.
- Un processus d'intervention en cas d'incident identifie et corrige les risques et les vulnérabilités en temps opportun;
- Chaque nouvel employé entreprend une formation à la protection des données et à la sécurité INFORMATIQUE ;
- Le département SÉCURITÉ INFORMATIQUE mène des campagnes trimestrielles de sensibilisation à la sécurité.

Pièce 3
Produits hébergés

- Sophos Central
- Sophos Cloud Optix
- Central Device Encryption
- Central Endpoint Protection
- Central Endpoint Intercept X
- Central Endpoint Intercept X Advanced
- Central Mobile Advanced
- Central Mobile Standard
- Central Phish Threat
- Central Intercept X Advanced for Server
- Central Server Protection
- Central Mobile Security
- Central Web Gateway Advanced
- Central Web Gateway Standard
- Central Email Standard
- Central Email Advanced
- Central Wireless Standard
- Tout autre produit Sophos administré et exploité via Sophos Central

Pièce 4

Données de référence pour LES CLAUSES CONTRACTUELLES TYPES de l'UE

ANNEXE 1 DES CLAUSES CONTRACTUELLES TYPES DE L'UE

A : LISTE DES PARTIES

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

Nom du client: fourni au fournisseur en vertu du Contrat principal

Adresse: fournie au fournisseur dans le cadre de l'e-mail de contact Contrat principal :

Nom/poste de la personne à contacter : tel que fourni au fournisseur en vertu du Contrat principal

Activités relatives aux données transférées en vertu des présentes clauses : Comme décrit à la clause 3 ci-dessus

Rôle (contrôleur/processeur) : Contrôleur

Importateur(s) de données : [*identité et coordonnées de l'importateur(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 : Sophos Limited (pour et pour le compte de ses filiales européennes et suisses)

Adresse : The Pentagon, Abingdon Science Park Abingdon, OX14 3YP, Royaume-Uni

Numéro d'immatriculation : 2096520

Nom, poste et coordonnées de la personne-ressource : dataprotection@sophos.com

Activités relatives aux données transférées en vertu des présentes clauses : Comme décrit à la clause 3 ci-dessus.

Rôle (contrôleur/processeur) : Processeur

B. DESCRIPTION DU TRANSFERT

Catégories de sujets de données dont les données personnelles sont transférées :

Tel que décrit à la section C, pièce 1 ci-dessus

Catégories de données personnelles transférées :

Tel que décrit à la section D, pièce 1 ci-dessus.

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 :

Tel que décrit à la section E, pièce 1 ci-dessus.

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

Continu

Nature du traitement

Tel que décrit à la section A, pièce 1 ci-dessus.

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

Tel que décrit à la section A, pièce 1 ci-dessus.

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

Pour la durée de la période contractuelle.

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

Comme décrit à la clause 3 ci-dessus.

AUTORITÉ DE SURVEILLANCE COMPÉTENTE

VOIR L'ARTICLE 9.8 CI-DESSUS

ANNEXE II – MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À ASSURER LA SÉCURITÉ DES DONNÉES[1]

Les mesures sont énoncées à la pièce 2 ci-dessus.

ANNEXE III – LISTE DES SOUS-PROCESSEURS[2]

Non requis en vertu de l'alinéa 9(a), l'option 1 **n'a pas** été sélectionnée.

[1] L'annexe II doit être remplie pour tous les modules sauf LE MODULE QUATRE.
[2] L'annexe III ne s'applique qu'au MODULE DEUX (transfert du contrôleur au processeur) et AU MODULE TROIS (transfert du processeur au processeur) lorsque l'option 1 de la clause 9(a) a été sélectionnée.