Accord sur le traitement des données conformément au RGPD et Clauses Contractuelles Types

Le présent Accord sur le traitement des données conformément au RGPD (l'« **ATD** ») est conclu entre l'entité désignée comme Responsable du traitement (le « **Responsable du traitement** ») et Proofpoint, Inc., 925 W. Maude Avenue, Sunnyvale, Californie 94085, États-Unis (le « **Sous-traitant** » ou « **Proofpoint** ») et est annexé aux documents suivants : (1) les Conditions générales de Proofpoint, Contrat Cadre de Souscription et Annexe(s) de produit concernées, (2) le contrat de licence pour utilisateur final (un CLUF-EULA, ou contrat en ligne dit « clickwrap » ou clickthrough ») accepté par le Responsable du traitement lors de l'enregistrement et accès initial du Responsable du traitement au produit ou service de Proofpoint, ou (3) tout autre accord de licence rédigé et signé entre les parties au titre duquel le Sous-traitant fournit les produits ou services au Responsable du traitement (le « **Contrat de Services** »). Le présent ATD prend effet à la date de signature du Responsable du traitement, mais uniquement si Proofpoint reçoit l'ATD signé selon les instructions ci-dessous.

Le présent ATD stipule les modalités selon lesquelles le Sous-traitant pourra recevoir et traiter les Données à caractère personnel transmises par le Responsable du traitement. Le présent ATD tient compte de la nature du traitement en vertu du Contrat de Services et décrit les mesures techniques et organisationnelles appropriées prises par le Sous-traitant en vue du traitement des Données à caractère personnel.

En outre, le présent ATD incorpore les Clauses Contractuelles Types annexées à la décision de la Commission européenne (EU) 2021/914 (les « **CCT** »). Outre les obligations lui incombant en vertu du présent ATD, Proofpoint respectera les obligations mises à la charge d'un Importateur de données en vertu des desdites CCT. Toute référence à l'**Importateur de données** sera réputée désigner **Proofpoint, Inc. ou le Sous-traitant** et toute référence à l'**Exportateur de données** ou au Responsable du traitement de données sera réputée désigner le **Responsable du traitement** et ses filiales basées dans l'Union européenne. Par les présentes, le Responsable du traitement déclare et garantit détenir le droit et l'autorité pour conclure le présent ATD pour son propre compte et celui de ses filiales.

Les Parties au présent ATD acceptent par les présentes d'être légalement liées par les modalités des Annexes 1 (Conditions de traitement des données) et 2 (Clauses contractuelles types) jointes et leurs appendices et annexes respectifs. Le présent ATD a été présigné par le Sous-traitant, Proofpoint, Inc. Pour que le présent ATD entre en vigueur, le Responsable du traitement doit au préalable :

1. Compléter et signer la rubrique d'informations ci-dessous avec le nom, l'adresse et la signature de l'entité juridique du Responsable du traitement ; et
2. Envoyer l'ATD complété et signé à Proofpoint par courrier électronique à l'adresse privacy@proofpoint.com.

Si le Responsable du traitement apporte des modifications ou suppressions au présent ATD, celles-ci sont rejetées et considérées invalides, sauf décision contraire de Proofpoint. Le signataire du Responsable de traitement déclare et garantit détenir l'autorité légale pour obliger le Responsable du traitement au titre du présent ATD. Le présent ATD prendra automatiquement fin lors de l'expiration du Contrat de Services, ou avant, en cas de résiliation anticipée en vertu des modalités du présent ATD.

Accepté et convenu par le Responsable du traitement :	Accepté et convenu par **Proofpoint, Inc.** : (**Sous-traitant**)
Signature : _____	Signature : DocuSigned by: Paul Auvil 2955B8CEBD2B45C...
Nom : _____	Nom : Paul Auvil, Directeur financier
Date : _____	
Société : _____	
Adresse : _____	
_____	

ANNEXE 1

CONDITIONS DE TRAITEMENT DES DONNÉES

1. Définitions.

a. Tous les termes non définis dans le présent ATD auront le sens qui leur est attribué : premièrement, dans le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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 (**RGPD**) ; et deuxièmement, dans le Contrat de Services.

b. **Données du Responsable du traitement** désignent les Données à caractère personnel du Responsable du traitement, celles-ci ayant la même définition que dans le RGPD.

c. **Législations sur la protection des données** désignent toutes les lois et réglementations applicables concernant le traitement des données à caractère personnel dans la mesure où elles sont liées à la fourniture des Produits et Services de Proofpoint en vertu du Contrat de Services.

d. **Personne concernée** désigne la personne identifiée ou identifiable à qui les Données à caractère personnel font référence.

e. **Traitement** (et ses dérivés) a le sens qui lui est donné à l'article 4.2 du RGPD.

f. **Sous-traitant ultérieur** désigne tout sous-traitant engagé par le Sous-traitant pour traiter des Données à caractère personnel.

g. **Autorité de contrôle** désigne une autorité publique, instituée par un État membre de l'UE conformément au RGPD.

2. Traitement des Données à caractère personnel.

a. Eu égard aux activités décrites en Appendice 1, les parties prévoient que le Responsable du traitement et ses filiales basées en Union européenne (ou leurs filiales ou clients) seront le responsable du traitement / l'exportateur de données et que le Sous-traitant sera le sous-traitant des données / l'importateur des données dans la mesure où il traite des Données à caractère personnel. Le Responsable du traitement accepte et garantit que ses instructions fournies au Sous-traitant concernant le traitement des Données à caractère personnel sont et seront conformes aux dispositions pertinentes des Lois sur la protection des données en vigueur.

b. L'objet et la durée du Traitement des Données à caractère personnel sont définis dans le Contrat de Services, qui décrit les Services fournis au Responsable du traitement. La nature et la finalité du Traitement, les types de Données à caractère personnel et les catégories de Personnes concernées sont énoncés à l'Appendice 1 du présent ATD.

c. Le Responsable du traitement est responsable de l'exactitude, de la qualité et de la légalité des Données à caractère personnel, ainsi que des moyens par lesquels le Responsable du traitement a acquis les Données à caractère personnel.

d. Contrat de Services et le présent ATD constituent par les présentes les instructions du Responsable du traitement fournies au Sous-traitant concernant : (1) le traitement des Données à caractère personnel et (2) le transfert desdites Données à caractère personnel vers tout pays ou territoire, lorsque cela est raisonnablement nécessaire à la prestation des Services.

3. Analyse d'impact relative à la protection des données (« AIPD »).

En tenant compte de la nature du Traitement, le Sous-traitant peut apporter au Responsable du traitement son concours raisonnable nécessaire à l'exécution de l'obligation du Responsable du traitement, en vertu du RGPD, de procéder à une analyse d'impact relative à la protection des données liée à l'utilisation du Service par le Responsable du traitement, dans la mesure où le Responsable du traitement n'a pas par ailleurs accès aux informations concernées, et dans la mesure où lesdites informations sont à la disposition du Sous-traitant. Le Sous-traitant assistera de manière raisonnable le Responsable du traitement dans le cadre de la coopération ou de la consultation préalable de l'Autorité de contrôle dans l'exécution de ses tâches relatives à l'obligation AIPD du Responsable du traitement, dans la mesure requise par le RGPD.

4. **Droits des personnes concernées.** Le Sous-traitant, dans la mesure autorisée par la loi, informera immédiatement le Responsable du traitement s'il reçoit une demande émanant d'une Personne concernée visant à exercer le droit d'accès, le droit de rectification, la restriction de traitement, le droit à l'oubli, la portabilité des données, l'opposition au traitement par la Personne concernée, ou son droit de ne pas faire l'objet d'une prise de décision individuelle automatisée. En tenant compte de la nature du traitement, le Sous-traitant apportera son concours au Responsable du traitement par des mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour l'exécution de l'obligation du Responsable du traitement de répondre à la demande de la Personne concernée.

5. **Utilisation limitée des Données à caractère personnel et du personnel**. Sauf disposition contraire stipulée dans le présent Accord de prestation de service, le Sous-traitant (i) n'acquerra aucun droit dans ou sur les Données à caractère personnel ; et (ii) le Sous-traitant et ses filiales prendront des mesures raisonnables pour garantir la fiabilité de tout employé, agent ou prestataire d'un Sous-traitant ultérieur engagé et ayant accès aux Données à caractère personnel, garantissant dans tous les cas que l'accès soit strictement limité aux personnes présentant un besoin de connaître/accéder aux Données à caractère personnel concernées, comme strictement nécessaire aux fins du Contrat de Services, et pour se conformer aux lois sur la protection des données et la confidentialité en vigueur, garantissant que l'ensemble de ces personnes soient soumises à des accords de confidentialité ou à des obligations professionnelles ou légales de confidentialité.

6. **Sous-traitants ultérieurs**.

a. **Désignation des Sous-traitants ultérieurs**. Le Responsable du traitement donne son consentement général au Sous-traitant pour le recours de Sous-traitants ultérieurs. Le Responsable du traitement reconnaît et accepte que (a) les filiales du Sous-traitant puissent jouer le rôle de Sous-traitants ultérieurs ; et (b) le Sous-traitant et ses filiales respectivement puissent engager des Sous-traitants ultérieurs externes dans le cadre de la prestation des Services. Le Sous-traitant ou ses filiales ont conclu un accord écrit avec chaque Sous-traitant ultérieur contenant des obligations de protection des données au moins aussi strictes que celles du présent ATD en matière de protection des Données du Responsable du traitement dans la mesure applicable à la nature des Services fournis par ledit Sous-traitant ultérieur. Le Sous-traitant sera pleinement responsable vis-à-vis du Responsable du traitement de l'exécution des obligations des Sous-traitants ultérieurs conformément au contrat conclu avec le Sous-traitant.

b. **Liste**. La liste actuelle des sous-traitants ultérieurs du Service est disponible sur le site de Proofpoint Trust à l'adresse : https://www.proofpoint.com/us/legal/trust. Si le Sous-traitant apporte des modifications ou des ajouts à cette liste, dans la mesure où le Responsable du traitement s'est inscrit pour recevoir des notifications sur le site du Trust, le Sous-traitant l'informera de ces modifications par courrier électronique. Les parties conviennent que cette notification satisfait aux exigences de notification stipulées à l'Article 28.2 du RGPD et de la Clause 9 des Clauses contractuelles types.

c. **Objection**. Le Responsable du traitement peut s'opposer au recours par le Sous-traitant à un nouveau Sous-traitant ultérieur en le notifiant par écrit sans délai au Sous-traitant à l'adresse privacy@proofpoint.com. Dans le cas où le Responsable du traitement s'oppose à un nouveau Sous-traitant ultérieur, le Sous-traitant (après réception de l'objection écrite du Responsable du traitement comme indiqué précédemment) déterminera raisonnablement si une solution peut être trouvée avec le Responsable du traitement pour éviter le traitement des Données à caractère personnel par le nouveau Sous-traitant ultérieur auquel il s'est opposé, sans affecter indûment le Responsable du traitement. Si le Sous-traitant n'est pas en mesure de proposer une telle solution dans un délai raisonnable, qui ne doit pas dépasser trente (30) jours, le Responsable du traitement peut annuler la commande en question concernant uniquement le Service qui ne peut pas être fourni par le Sous-traitant sans recourir au nouveau Sous-traitant ultérieur auquel il s'oppose, en le notifiant par écrit au Responsable du traitement dans les trente (30) jours suivant la désignation du Sous-traitant.

7. **Catégories particulières de Données à caractère personnel**. Le Responsable du traitement (et ses filiales basées au sein de l'Union européenne) sera seul responsable du respect des lois sur la protection des données et la confidentialité, applicables au Responsable du traitement (et à ses filiales basées au sein de l'Union européenne), incluant toute Donnée à caractère personnel qui requiert une gestion particulière ou des catégories particulières de Données à caractère personnel telles que, entre autres, les données relatives à la race ou l'origine ethnique d'une personne, aux opinions politiques,

aux croyances religieuses ou philosophiques, à l'adhésion à un syndicat, à la santé, à l'orientation sexuelle ou aux finances personnelles.

8. Sécurité des Données à caractère personnel.

a. Le Sous-traitant doit au minimum mettre en œuvre les mesures techniques et organisationnelles spécifiées à l'Appendice 2 pour assurer la sécurité des Données à caractère personnel. Ces mesures incluent toute mesure de protection des Données à caractère personnel contre une violation de la sécurité entraînant une destruction, une perte, une altération, une divulgation ou un accès non autorisé aux Données à caractère personnel, de manière accidentelle ou illégale. Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques encourus par les Personnes concernées.

b. Le Sous-traitant du traitement n'accorde l'accès aux Données à caractère personnel en cours de traitement aux membres de son personnel que dans la mesure nécessaire à la mise en œuvre, la gestion et le suivi du Contrat de prestation de services. Le Sous-traitant s'assure que les personnes autorisées à traiter les Données à caractère personnel reçues se sont engagées à respecter la confidentialité ou sont soumises à une obligation légale de confidentialité appropriée.

9. Coopération avec les Autorités de contrôle. Le Sous-traitant assistera de manière raisonnable le Responsable du traitement dans le cadre de la coopération ou de la consultation préalable de l'Autorité de contrôle dans l'exécution de ses tâches relevant de l'Article 8 du présent ATD, dans la mesure requise par le RGPD. En outre, dans le cadre de la demande de l'Autorité de contrôle, aux frais du Responsable du traitement, le Sous-traitant fera raisonnablement tout son possible pour obtenir le concours raisonnable des Sous-traitants ultérieurs en fournissant un accès aux informations pertinentes nécessaires pour exécuter les obligations du Responsable du traitement en vertu du RGPD.

10. Violation des Données à caractère personnel.

a. En cas d'utilisation, de divulgation ou d'acquisition non autorisée connue par un tiers de Données à caractère personnel compromettant la sécurité, la confidentialité ou l'intégrité des Données à caractère personnel conservées par le Sous-traitant (« Infraction à la sécurité »), le Sous-traitant informera le Responsable du traitement par écrit de la violation dans un délai de 48 heures et fournira des informations périodiques par la suite.

b. Cette notification doit contenir, au minimum
   (i) une description de la nature de l'Infraction à la sécurité (y compris, si possible, les catégories et le nombre approximatif de Personnes concernées et d'enregistrements de données concernés) ;
   (ii) les coordonnées d'un point de contact où il est possible d'obtenir de plus amples informations concernant la violation des Données à caractère personnel ; et
   (iii) ses conséquences probables et les mesures prises ou proposées pour remédier à l'Infraction à la sécurité, y compris pour en atténuer les effets négatifs éventuels.

c. Si, et dans la mesure où, il n'est pas possible de fournir toutes ces informations en même temps, la notification initiale contiendra les informations disponibles à ce moment-là et les autres informations seront fournies par la suite, dans les meilleurs délais, à mesure qu'elles deviennent disponibles.

11. Transfert international des Données.

a. **Généralités**. Le Sous-traitant se conformera aux exigences des Lois applicables en matière de protection des données concernant le transfert international de Données à caractère personnel à partir de l'Espace économique européen. Uniquement pour la fourniture des Services au Responsable du traitement en vertu du Contrat de Services, les Données à caractère personnel peuvent être transférées et stockées et/ou traitées dans tout pays dans lequel le Sous-traitant ou ses Sous-traitants ultérieurs opèrent, ce qui peut inclure des pays tiers. Tous les transferts de Données à caractère personnel hors de l'Espace économique européen sont régis par les Clauses contractuelles types que les parties concluent par les présentes et intègrent au présent ATD en tant qu'Annexe 2.

b. **Évaluation du transfert de données.** Plusieurs services de sécurité du Sous-traitant exigent qu'un certain nombre de Données à caractère personnel soit transféré aux États-Unis, et donc,

conformément à la Clause 14(b) des Clauses Contractuelles Types, le Sous-traitant a réalisé une Évaluation du transfert de données (également appelée Évaluation de l'impact du transfert), qui peut être consultée à l'adresse https://www.proofpoint.com/sites/default/files/misc/pfpt-us-data-transfer-assessment-20201028.pdf.

12. Requêtes gouvernementales.

a. Conformément à la Clause 15 des Clauses Contractuelles Types, le Sous-traitant ne divulguera à aucun organisme gouvernemental ou une autorité publique tiers, les Données du Responsable du traitement, sauf si cela s'avère nécessaire pour respecter la loi ou un ordre valide et contraignant d'un organisme gouvernemental (tel qu'une assignation ou une ordonnance du tribunal). Si un organisme gouvernemental envoie au Sous-traitant une demande de Données sensibles du Responsable du traitement, le Sous-traitant tentera de rediriger l'organisme gouvernemental vers le Responsable du traitement pour lui demander directement ces données. À cette fin, le Sous-traitant peut fournir les informations minimales relatives au Responsable du traitement à l'organisme gouvernemental. Si le Sous-traitant se trouve dans l'obligation de divulguer des Données du Responsable du traitement à un organisme gouvernemental, il le notifiera au Responsable du traitement dans un délai raisonnable afin de lui permettre de demander une ordonnance de protection ou tout autre recours approprié, si la loi n'empêche pas le Sous-traitant de le faire. En vertu de la Loi américaine sur la surveillance du renseignement étranger (Foreign Intelligence Surveillance Act, FISA), le Sous-traitant est un « service informatique à distance » et non un fournisseur de télécommunications. Il est donc peu probable (selon le Sous-traitant) que la société fasse l'objet d'une demande gouvernementale en vertu de ces lois.

b. Afin de s'assurer que le Responsable du traitement devient et reste conscient des risques liés au transfert de données vers un pays tiers, le Sous-traitant peut, de temps à autre, sur demande raisonnable du Responsable du traitement, sans dépasser une fois par année civile, fournir une ou plusieurs réponses à un questionnaire structuré du Responsable du traitement concernant les lois et règlements du pays de destination applicables au Sous-traitant ou à ses Sous-traitants ultérieurs qui permettraient aux autorités publiques d'accéder aux Données du Responsable du traitement faisant l'objet du transfert, en particulier dans les domaines du renseignement, de l'application de la loi et de la surveillance administrative et réglementaire applicables aux données transférées. Le Sous-traitant doit être en mesure de fournir au Responsable du traitement ce type d'informations au mieux de ses connaissances et après avoir déployé tous les efforts possibles pour les obtenir.

13. Vérification et audit.

a) Conformément à l'Article 28.3 (h) du RGPD, le Sous-traitant met à la disposition du Responsable du traitement, sur demande écrite raisonnable et sous réserve de la signature d'un accord de confidentialité spécifique, les informations relatives au Traitement des Données à caractère personnel du Responsable du traitement nécessaires pour démontrer le respect par le Sous-traitant des obligations lui incombant en vertu du présent ATD. Le Sous-traitant autorise les demandes d'inspection sur site par le Responsable du traitement ou un auditeur indépendant en ce qui concerne le Traitement des Données à caractère personnel afin de vérifier le respect du présent ATD, si (a) le Sous-traitant n'a pas fourni de preuves écrites suffisantes du respect des mesures techniques et organisationnelles ; (b) une Infraction à la sécurité s'est produite ; (c) une inspection est officiellement demandée par l'Autorité de contrôle du Sous-traitant ; ou (d) la Loi sur la protection des données confère au Responsable du traitement un droit d'inspection sur site obligatoire ; et à condition que le Responsable du traitement n'exerce pas ce droit plus d'une fois par an, à moins que la Loi sur la protection des données impose des inspections plus fréquentes. Toute information fournie par le Responsable du traitement et/ou les audits réalisés conformément au présent article est soumise à la signature d'un accord de confidentialité spécifique. Ces inspections d'installations sont menées de façon à ne jamais impacter la sûreté, la sécurité, la confidentialité, l'intégrité, la disponibilité, la continuité et la résilience des installations inspectées, ni à exposer ou compromettre de toute autre manière les données confidentielles qui y sont traitées.

b) Chaque partie prend en charge les frais qu'elle a engagés dans le cadre d'un audit ou d'une inspection. Cette disposition s'applique également à toute communication d'information ou à tout audit réalisé conformément à l'Article 8.9 (c-e) des Clauses Contractuelles Types.

14. Résiliation.

Le Responsable du traitement reconnaît et convient qu'en cas de suspension ou de résiliation de tout Traitement de données en vertu du présent ATD ou de la Clause 18 des Clauses Contractuelles Types, le délai dans lequel le Sous-traitant doit cesser tout Traitement et supprimer les données à caractère personnel sera régi par le Contrat de prestation de services.

APPENDICE 1 À L'ATD – DÉTAILS DU TRAITEMENT

Le présent Appendice 1 comprend certains détails du Traitement des Données à caractère personnel du Client, conformément à l'Article 28(3) du RGPD (ou, le cas échéant, aux dispositions équivalentes de toute autre Loi sur la protection des données).

Produit	Personnes concernées	Catégories de données à caractère personnel traitées	Opérations de traitement	Période de conservation
Archive	Employés, prestataires et clients	Toute Donnée à caractère personnel incluse dans le contenu capturé (y compris les e-mails, les messages instantanés, le contenu des réseaux sociaux, la télémétrie des messages associés et les pièces jointes)	• Archive est une solution d'archivage basée sur le Cloud conçue pour l'investigation légale, la conformité réglementaire et l'accès aux données pour les utilisateurs finaux du Client. Elle fournit en outre un référentiel central et consultable qui prend en charge un large éventail de types de contenu.	Déterminée par le Responsable du traitement
CAD/CASB	Employés, prestataires	Métadonnées des titulaires de comptes Cloud (adresses e-mail, noms, position), métadonnées de fichier et journaux des accès aux comptes Cloud	Cloud Account Defense aide le Client à détecter les activités suspectes autour de ses comptes Cloud et à identifier ceux qui sont compromis. Cloud App Security Broker utilise des politiques pour empêcher la perte des données sensibles ou confidentielles du Client contenues dans ses comptes Cloud. CASB IaaS Protection aide le Client à identifier ses ressources IaaS, à protéger les données sensibles dans le stockage IaaS, et à surveiller et arrêter les connexions non autorisées à ses comptes Cloud.	Jusqu'à 180 jours à compter de la fin de la souscription du Responsable du traitement
Cloudmark Active Filter, Authority, Content Categories, Insight Server et Sender Intelligence ; Cloudmark Spam Reporting Service	Employés, prestataires, clients	Données de télémétrie associées aux e-mails, SMS, MMS et RCS, notamment les adresses e-mail, adresses IP et numéros de téléphone	Les produits Cloudmark s'appuient sur une analyse intelligente des menaces pour assurer la sécurité des e-mails et de la messagerie mobile contre les spams et les logiciels malveillants.	30 jours pour les messages signalés par le destinataire comme étant potentiellement nuisibles. 30 jours pour les messages signalés par le destinataire comme non nuisibles.
Cloudmark Safe Messaging Cloud, Cloudmark	Employés, prestataires, clients	Données de télémétrie associées aux e-mails, SMS, MMS et RCS, notamment	Les produits Cloudmark s'appuient sur une analyse intelligente des menaces pour assurer la sécurité des e-mails et de la messagerie mobile contre les spams et les logiciels malveillants.	30 jours pour les messages signalés par le destinataire comme étant potentiellement nuisibles.

Safe Messaging Cloud Hybrid		les adresses e-mail, adresses IP et numéros de téléphone.		30 jours pour les messages signalés par le destinataire comme non nuisibles. Sinon, selon ce qui a été négocié par le Responsable du traitement.
Compliance Gateway	Employés, prestataires et clients	Toute Donnée à caractère personnel incluse dans le contenu capturé (y compris les e-mails, les messages instantanés, le contenu des réseaux sociaux, la télémétrie des messages associés et les pièces jointes)	Compliance Gateway agit comme un hub central pour filtrer et acheminer le contenu des messages vers les systèmes d'archivage, de supervision et d'analyse du Client.	Jusqu'à 14 jours à compter de la fin de la souscription du Responsable du traitement
Content Capture	Employés, prestataires et clients	Toute Donnée à caractère personnel incluse dans le contenu capturé (y compris les e-mails, les messages instantanés, le contenu des réseaux sociaux, la télémétrie des messages associés et les pièces jointes)	Content Capture capture le contenu à partir des plateformes de messagerie et de stockage Cloud prises en charge et fournit des services de conformité tels que l'investigation électronique, l'archivage et la supervision.	Jusqu'à 90 jours à compter de la fin de la souscription du Responsable du traitement
Content Patrol	Employés, prestataires et clients	Toute Donnée à caractère personnel incluse dans le contenu capturé (y compris les e-mails, les messages instantanés, le contenu des réseaux sociaux, la télémétrie des messages associés et les pièces jointes)	Content Patrol permet au Client de capturer, surveiller, corriger et générer des rapports de conformité sur les activités de leurs utilisateurs finaux sur les comptes de réseaux sociaux contrôlés par le Client.	Jusqu'à 90 jours à compter de la fin de la souscription du Responsable du traitement
Continuity	Employés, prestataires et toute autre personne envoyant ou recevant des e-mails via le système de messagerie électronique d'entreprise du Responsable du traitement	Toute Donnée à caractère personnel incluse dans un e-mail	Continuity assure le stockage temporaire des e-mails entrants et sortants du Client dans le cadre de la messagerie Web à la demande. Continuity sert uniquement d'option secondaire de basculement d'urgence en cas de défaillance du service de messagerie du Client, et non de solution principale d'archivage des e-mails ou de solution principale de basculement.	Les messages expirent au bout de 30 jours.
Digital Discover, Digital Protection et	Employés, prestataires, clients ou toute autre personne publiant des	ID des comptes utilisateurs des réseaux sociaux de l'entreprise, contenu des	Analyse des plateformes de réseaux sociaux pour trouver les comptes affiliés à un client afin de détecter les comptes faux, frauduleux et diffamatoires liés au client. Analyse du contenu statique et interactif.	Jusqu'à 90 jours à compter de la fin de la souscription du Responsable du traitement

Digital Compliance	messages sur les comptes de réseaux sociaux du Client	réseaux sociaux et informations biographiques optionnelles si elles sont incluses dans le profil de compte des utilisateurs de l'entreprise	Connecteurs au service d'archivage des réseaux sociaux, conformément à la réglementation.	
Email Data Loss Prevention (DLP)	Employés, prestataires et toute autre personne envoyant ou recevant des e-mails via le système de messagerie électronique d'entreprise du Client	Toute Donnée à caractère personnel incluse dans un e-mail	Email DLP utilise des politiques visant à prévenir la perte de données sensibles ou confidentielles du Client par le biais de la messagerie électronique.	Jusqu'à 366 jours après la collecte, sauf pour les analyses des menaces, qui sont conservées jusqu'à 18 mois après la collecte.
Email Fraud Defense	Employés, prestataires, clients et toute autre personne envoyant ou recevant des e-mails via le système de messagerie électronique d'entreprise du Client	Informations figurant dans l'en-tête de l'e-mail, y compris les adresses e-mail, les adresses IP, les noms de l'expéditeur et du destinataire.	EFD traite les rapports globaux DMARC (Domain-based Message Authentication, Reporting & Conformance) et les données contenues dans les rapports DMARC forensic pour les domaines des clients, et évalue l'authenticité des expéditeurs sur la base des informations d'authentification de l'expéditeur, pour mettre en évidence le trafic envoyé par des sources non authentifiées et non autorisées.	Les données contenues dans les rapports Cloudmark forensic sont conservées pendant 30 jours après leur collecte. Les données contenues dans les rapports DMARC forensic sont conservés pendant 90 jours après leur collecte.
Email Encryption	Employés, prestataires, clients et toute autre personne envoyant ou recevant des e-mails via le système de messagerie électronique d'entreprise du Client	Toute Donnée à caractère personnel incluse dans un e-mail	Email Encryption fournit une solution entièrement intégrée de cryptage et de décryptage des messages.	Le contenu des messages cryptés est conservé selon les modalités fixées par le Responsable du traitement (jusqu'à 366 jours).
Email Protection	Employés, prestataires et toute autre personne envoyant ou recevant des e-mails via le système de messagerie électronique d'entreprise du Responsable du traitement	Toute Donnée à caractère personnel incluse dans un e-mail	Email Protection comprend des fonctions telles que la détection des spams pour identifier et classer les messages indésirables, la protection anti-virus pour détecter et filtrer les messages contenant des virus connus, des fonctions anti-virus « zero-hour » pour détecter et filtrer les messages contenant des contenus suspects et un dossier de quarantaine pour analyser et éliminer les contenus suspects.	Jusqu'à 18 mois après la collecte
Endpoint Data Loss Protection	Employés, prestataires	Métadonnées enregistrées pour les utilisateurs du Responsable du traitement	Endpoint Data Loss Prevention déploie un logiciel (un Agent) sur les ordinateurs de bureau et les serveurs appartenant au Client ou contrôlés par lui, sur des plateformes prises en charge. Ces Agents capturent les métadonnées enregistrées à partir des activités des utilisateurs sous licence et stockent ces données dans l'archive Endpoint Data Loss Prevention de Proofpoint.	Jusqu'à 90 jours à compter de la fin de la souscription du Responsable du traitement

Essentials	Employés, prestataires, clients	Toute Donnée à caractère personnel incluse dans un e-mail	• Analyse, filtrage et routage des e-mails en transit envoyés à des parties externes au client et reçus de celles-ci, via le système de messagerie électronique d'entreprise du Client. • Si la fonctionnalité d'archivage est utilisée, voir « Archive » ci-dessus • Si le sandboxing TAP est utilisé, voir « TAP » ci-dessous	Jusqu'à 18 mois après la collecte.
Insider Threat Management (ITM) en mode SaaS	Employés, prestataires : a) Administrateurs ou analystes ITM en mode SaaS, utilisant le portail Internet. b) Utilisateurs de poste de travail, en utilisant les postes de travail de l'exportateur de données sur lesquels l'agent ITM en mode SaaS a été installé.	Adresse e-mail, identifiant du périphérique tel que l'adresse IP, informations sur l'utilisateur telles que le nom et l'ID utilisateur, informations sur le site Internet telles que l'URL et le nom de la page, informations sur l'application telles que le nom de l'application, le nom de l'exécutable et le titre de la fenêtre. En outre, ITM a la capacité de capturer le contenu de l'écran, qui est configuré et contrôlé par le client. La capture d'écran peut englober toute donnée à caractère personnel supplémentaire affichée sur l'écran de l'utilisateur.	ITM déploie un agent de poste de travail sur les ordinateurs portables, les ordinateurs de bureau et les serveurs désignés que possède ou contrôle le responsable du traitement des données. Les agents recueillent des données télémétriques sur les activités des utilisateurs du périphérique, c'est-à-dire les personnes concernées. Si le responsable du traitement des données l'autorise, les agents peuvent également faire des captures d'écran des activités des périphériques des utilisateurs. Le client détermine seul s'il souhaite activer les fonctionnalités de capture d'écran, ainsi que la période de conservation des données de ce contenu. Les données de télémétrie et de capture d'écran sont stockées sur la solution de stockage SaaS ITM multi-tenant de Proofpoint.	Conformément à la période de conservation définie par le Responsable du traitement, jusqu'à une période maximale de 366 jours.
Intelligent Classification and Protection	Employés, prestataires, clients et toute personne qui consulte le document	Toute Donnée à caractère personnel incluse dans un document.	Localise et identifie automatiquement les données sensibles et critiques pour l'entreprise afin d'améliorer les solutions de protection des données existantes telles que l'étiquetage, le cryptage, le contrôle d'accès, la prévention des pertes de données et le CASB, et propose des règles et/ou des politiques de protection au Client.	Jusqu'à 90 jours à compter de la fin de la souscription du Responsable du traitement
Internal Mail Defense (IMD)	Employés, prestataires	Toute Donnée à caractère personnel incluse dans un e-mail	IMD utilise les fonctions Email Protection et TAP pour protéger les communications électroniques internes du Client contre les spams et les contenus malveillants.	Jusqu'à 18 mois après la collecte.
Browser Isolation et E-mail Isolation	Employés et prestataires	Adresses e-mail, cookies du site de l'utilisateur et historique du navigateur, ainsi que l'emplacement du centre de données du conteneur d'isolation.	Les produits Browser Isolation et Email Isolation mettent en place un navigateur Web ou un environnement de messagerie Web isolé à distance pour protéger le Client contre les menaces potentielles lorsque les utilisateurs se connectent à Internet ou à des comptes de messagerie Web sur des périphériques appartenant au Client ou contrôlés par lui. Le Client n'autorisera pas les utilisateurs à transmettre par l'intermédiaire d'Isolation (ou à y afficher) des documents contrefaits, diffamatoires, menaçants ou offensants.	Jusqu'à 90 jours à compter de la fin de la souscription du Responsable du traitement

NexusAI for Compliance	Employés, prestataires et clients	Toute Donnée à caractère personnel incluse dans le contenu capturé (y compris les e-mails, les messages instantanés, le contenu des réseaux sociaux, la télémétrie des messages associés et les pièces jointes)	NexusAI for Compliance utilise l'apprentissage automatique pour évaluer les messages archivés pris en charge (tels que les e-mails, les réseaux sociaux, les plateformes de collaboration et les messages mobiles) signalés pour examen par le Client via le produit Intelligent Supervision de Proofpoint.	Jusqu'à 24 heures à compter de la fin de la souscription du Responsable du traitement
Nexus People Risk Explorer	Employés, prestataires	Noms, adresses e-mail, toute Donnée à caractère personnel contenus dans les analyses des menaces	Proofpoint Nexus People Risk Explorer exploite les données de sécurité centrées sur les personnes provenant de Targeted Attack Protection, Security Awareness Training, Cloud Account Defense et Cloud Account Security Broker de Proofpoint pour fournir des informations sur les types, la gravité et la fréquence des menaces visant le Client et ses employés.	Jusqu'à 90 jours à compter de la fin de la souscription du Responsable du traitement
Anti-Phishing Suite : comprend PhishAlarm et PhishAlarmAnalyzer	Employés, prestataires	Nom Adresse e-mail Toute Donnée à caractère personnel incluse dans un e-mail	Acheminement et analyse des e-mails suspects signalés par les utilisateurs finaux à l'aide du bouton PhishAlarm. PhishAlarm Analyzer permet une identification très réactive des attaques de phishing en temps réel. Les e-mails signalés via PhishAlarm et PhishAlarm Analyzer sont consultés et classés par catégorie, et immédiatement disponibles pour les équipes d'intervention du Client.	Jusqu'à 30 jours à compter de la fin de la souscription du Responsable du traitement, à l'exception des analyses des menaces, qui sont conservées jusqu'à 18 mois après leur collecte
Proofpoint Security Awareness Training (PSAT)	Employés, prestataires	Nom, adresse e-mail et autres champs de données choisis par le client pour le téléchargement vers PSAT à partir de l'Active Directory du Client.	Les données à caractère personnel sont utilisées aux fins de lancement de la formation de sensibilisation à la cybersécurité des employés, ainsi que pour l'évaluation et l'établissement des rapports de sécurité des employés.	Jusqu'à 90 jours à compter de la fin de la souscription du Responsable du traitement ; toutefois, pendant la souscription du Responsable du traitement, les administrateurs Responsable du traitement peuvent apporter des modifications aux utilisateurs et les supprimer.
Secure E-Mail Relay (SER)	Employés Prestataires Tous les destinataires d'e-mails envoyés en masse via le système de messagerie électronique d'entreprise du Client	Nom Adresse e-mail Toute Donnée à caractère personnel incluse dans un e-mail	Secure Email Relay (SER) est une solution hébergée et multi-tenant qui permet au Client de contrôler les applications qui envoient des e-mails en utilisant les domaines qu'il possède ou contrôle. Elle ajoute une couche de sécurité à chaque application et distribue les e-mails sur Internet de manière conforme au protocole DMARC après que les contrôles AS/AV de Proofpoint ont été effectués. SER ne peut être utilisé que pour la remise d'e-mails conformes aux lois applicables aux messages envoyés en masse ou non sollicités.	Jusqu'à 30 jours à compter de la fin de la souscription du Responsable du traitement
SecureShare	Employés, prestataires, toute autre personne invitée à consulter un fichier partagé	Nom, adresses e-mail	SecureShare est une méthode sécurisée pour le partage de fichiers et le stockage temporaire de ces fichiers.	Jusqu'à 180 jours après la collecte.

Targeted Attack Protection (TAP)	Employés, prestataires, clients Tout autre individu envoyant ou recevant des e-mails via le système de messagerie électronique d'entreprise du Client	Nom Adresse e-mail Toute Donnée à caractère personnel incluse dans un e-mail	TAP identifie et offre une protection contre les URL et les pièces jointes malveillantes dans les e-mails à l'aide d'un moteur d'analyse dynamique des logiciels malveillants.	Jusqu'à 18 mois après la collecte.
Threat Response Auto-pull (TRAP)	Employés, prestataires, clients Tout autre individu envoyant ou recevant des e-mails via le système de messagerie électronique d'entreprise du Client	Nom Adresse e-mail Toute Donnée à caractère personnel incluse dans un e-mail	TRAP est une plateforme de gestion des incidents qui comprend l'automatisation de l'analyse et de la suppression des e-mails indésirables.	La conservation des incidents clos est définie par le Responsable du traitement. Les données MIME des messages complets sont purgées tous les 30 jours pour les incidents clos.
ThreatSimulator	Employés, prestataires	Nom Adresse e-mail	Les données à caractère personnel sont utilisées pour des campagnes de phishing simulées. Le Client ne peut envoyer des e-mails de phishing simulés qu'à des domaines qu'il possède ou contrôle.	Sur demande du client et dans les 90 jours suivant cette demande.
Zero Trust Network Access (anciennement Meta)	Employés, prestataires	Adresse et nom de l'utilisateur ainsi que son numéro de téléphone (facultatif) et les événements du trafic intranet tels que les événements d'acceptation/départ et les requêtes DNS (le client a la possibilité d'activer ou de désactiver l'enregistrement des événements du trafic Internet).	Meta superpose un réseau de confiance zéro au réseau d'entreprise du client. Les utilisateurs accèdent au réseau d'entreprise en se connectant à la couche réseau de Meta via un VPN avec leurs identifiants de connexion. Une fois connecté au réseau Meta, chaque utilisateur se voit attribuer une identité unique qui se connecte au réseau d'entreprise sous-jacent de l'exportateur de données. L'accès aux actifs au sein du réseau d'entreprise de l'exportateur de données se fait grâce à l'identité unique de l'utilisateur.	Jusqu'à 90 jours à compter de la fin de la souscription du Responsable du traitement

1. Sous-traitants ultérieurs.

La liste actuelle des Sous-traitants ultérieurs est disponible ici : https://www.proofpoint.com/us/legal/trust

APPENDICE 2 À L'ATD – SÉCURITÉ DU TRAITEMENT

Compte tenu de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque de niveaux variables de probabilité et de gravité concernant les droits et libertés des personnes physiques, le Sous-traitant met en œuvre les mesures décrites ci-dessous afin de garantir un niveau de sécurité approprié pour la fourniture des Services :

A. *Authentification de l'utilisateur*

La direction a établi et approuvé un programme de sécurité de l'information.
Un cadre de politiques et de normes de sécurité de l'information a été élaboré, à l'appui des objectifs du programme de sécurité de l'information.
Des procédures ont été mises en place pour authentifier et autoriser les utilisateurs à accéder aux systèmes, et pour garantir le respect de ces procédures.
Des procédures ont été mises en place pour assurer le respect des politiques de demande, d'établissement, de délivrance, de suspension, de suppression et de fermeture des comptes utilisateurs et des privilèges d'accès associés, par exemple l'accès au système est accordé en fonction du rôle sur la base du concept du moindre privilège.
Un processus vise à surveiller les tentatives de connexion échouées. Les infractions à la sécurité identifiées sont résolues.
L'accès à l'environnement de production du Sous-traitant par les employés du Sous-traitant est accordé en fonction des besoins de l'entreprise. Un VPN authentifié à deux facteurs est utilisé.
Des contrôles permettent de limiter la mise en œuvre de changements dans la production aux seules personnes autorisées.

Type d'accès

Les différents types d'accès des utilisateurs finaux du client sont documentés dans le Guide de l'administrateur propre au service et contrôlés par les administrateurs du client via le tableau de bord du service, l'interface utilisateur ou l'intégration SAML.

B. *Exécution de copies de sauvegarde*

Les données de configuration et de rapport des clients sont sauvegardées régulièrement et stockées sur disque rotatif.

Les procédures de sauvegarde et de conservation des données et des programmes ont été documentées et mises en œuvre.

C. *Ordinateurs et terminaux d'accès*

Les ordinateurs utilisés par les employés du Sous-traitant pour accéder à l'infrastructure de ce dernier doivent utiliser un tunnel VPN sécurisé pour ce faire. Tous les postes de travail des employés doivent être équipés d'un logiciel anti-virus à jour et des politiques permettent de limiter les logiciels susceptibles d'être installés sur ces machines. Tous les employés du Sous-traitant doivent s'authentifier auprès d'un système d'authentification centralisé pour accéder aux réseaux d'entreprise et de production du Sous-traitant.

Contrôles du Sous-traitant de données

Les nouveaux employés doivent signer un accord de confidentialité concernant les logiciels propriétaires et les informations relatives aux clients.
Les nouveaux employés reçoivent également une copie du Code de conduite de sécurité du Sous-traitant, un résumé du programme de sécurité de l'information du Sous-traitant, dont ils doivent accuser réception.
L'accès à l'environnement de production du Sous-traitant par les employés du Sous-traitant est accordé en fonction des besoins de l'entreprise. Un VPN authentifié à deux facteurs est utilisé.

Des outils de gestion centralisée de la configuration sont utilisés pour s'assurer que les postes de travail des employés sont correctement configurés.

D. ***Journaux d'accès***

En ce qui concerne les Services, les journaux d'accès revêtent au moins deux formes différentes :

Toutes les tentatives d'accès aux systèmes informatiques du Sous-traitant de données sont consignées de manière centralisée et toute activité inhabituelle est automatiquement signalée à l'équipe de sécurité informatique mondiale du Sous-traitant. En outre, le Sous-traitant applique des politiques de verrouillage des comptes et des exigences en matière de mot de passe. Les journaux d'accès du client aux Services sont générés et conservés, selon le cas, pour chaque Service.

Des procédures ont été mises en place pour authentifier et autoriser les utilisateurs à accéder aux systèmes, et pour garantir le respect de ces procédures.
Un processus de contrôle est en place et suivi pour vérifier périodiquement et confirmer que les privilèges d'accès restent autorisés et appropriés.
Un processus vise à surveiller les tentatives de connexion échouées. Les infractions à la sécurité identifiées sont examinées et résolues.
Les données relatives aux événements liés aux applications sont conservées afin de fournir des informations chronologiques et des journaux permettant de réviser, d'examiner et de reconstituer les événements liés aux systèmes, au traitement des données et aux applications.

E. ***Systèmes de télécommunication***

Toutes les installations de production du Sous-traitant disposent de flux Internet redondants provenant de divers fournisseurs de bande passante.

F. ***Instruction du personnel***

L'ensemble du personnel du Sous-traitant est tenu de suivre un programme annuel de formation en ligne sur la sécurité et la sensibilisation. En outre, les membres du personnel peuvent recevoir une formation continue spécifique à leur rôle. Cette formation peut être dispensée par Proofpoint ou par un tiers.

Le Sous-traitant dispose d'un plan d'organisation, qui sépare les rôles et les tâches incompatibles du personnel concerné.
Des rôles et responsabilités de gestion distincts ont été définis pour séparer les rôles des opérations informatiques, du développement et de la maintenance des systèmes et des fonctions générales du Sous-traitant.
Les rôles et les responsabilités du personnel sont clairement définis.

G. ***Utilisation d'ordinateurs***

L'accès à distance aux réseaux de production du Sous-traitant est limité aux systèmes exécutant un logiciel de sécurité approuvé et géré par le Sous-traitant. Tous les systèmes du Sous-traitant fournis au personnel sont gérés par un système de configuration centralisé. Tous les employés du Sous-traitant sont informés des politiques d'utilisation acceptable du Sous-traitant pour les ordinateurs, l'accès à Internet et les communications par e-mail. Les employés du Sous-traitant doivent prendre connaissance de ces politiques et accepter de les respecter.

Les nouveaux employés doivent signer un accord de confidentialité concernant les logiciels propriétaires et les informations relatives aux clients.

Les nouveaux employés prennent connaissance et acceptent le Code de conduite de sécurité du Sous-traitant.

H. ***Impression de données***

Les données du client sont traitées en mémoire et ne peuvent pas être imprimées. En outre, aucune imprimante n'est disponible dans l'environnement de production du Sous-traitant et tous les services d'impression sont désactivés par défaut sur tous les serveurs de production.

K. ***Contrôle d'accès physique***

Contrôles du Sous-traitant de données

Pour les produits hébergés chez les fournisseurs de colocation du Sous-traitant, ce dernier contrôle l'accès physique à son infrastructure. Pour les produits hébergés chez les fournisseurs d'hébergement AWS, Azure ou Google Cloud, l'accès physique est contrôlé par le fournisseur d'hébergement.

L. **Mesures de sécurité physique des centres de données**

Les contrôles de sécurité physique des installations de colocation sont conformes aux normes des centres de données de niveau III, y compris la sécurité sur site 24 heures sur 24 et 7 jours sur 7, les points d'accès surveillés, les mécanismes de protection contre le piratage, l'authentification à deux facteurs et la vidéosurveillance. Les installations utilisées par AWS, Azure ou Google Cloud sont conformes aux normes des centres de données de niveau III.

M. ***Contrôle d'accès aux systèmes informatiques***

Contrôles du Sous-traitant de données

Le Sous-traitant de données contrôle l'accès aux systèmes fournissant des Services comme suit :

1. Tous les employés et prestataires du Sous-traitant de données reçoivent des identifiants d'utilisateur uniques. Le partage de compte n'est pas autorisé.
2. Les exigences en matière de mot de passe sont définies et appliquées par un outil de synchronisation des mots de passe. Les exigences sont les suivantes :
    a. Minimum de 12 caractères
    b. Ne doit pas figurer sur les listes publiques de mots de passe violés
    c. Historique de 23
    d. Obligation de changer tous les 180 jours
    e. Verrouillage du compte après cinq (5) tentatives de connexion infructueuses.
3. Accès logique accordé en fonction du rôle.
4. La journalisation de l'audit est en place sur le VPN de l'environnement de production du Sous-traitant de données.
5. Les journaux d'audit sont surveillés en temps quasi réel par un outil d'agrégation de journaux et d'alerte. Les alertes sont configurées pour être envoyées à l'équipe de sécurité de l'information mondiale du Sous-traitant de données.

N. ***Contrôle d'accès aux données***

Les données du client ne peuvent pas être conservées dans l'environnement d'entreprise du Sous-traitant. L'accès aux systèmes hébergeant les Services est contrôlé de la manière suivante :

1. L'accès est accordé en fonction du rôle chez le Sous-traitant.
2. Seul le personnel autorisé du Sous-traitant est autorisé à avoir un accès privilégié à un environnement de production du Sous-traitant.

O. La ***journalisation des audits*** est en place sur le VPN et sur les systèmes de l'environnement de production du Sous-traitant.

P. ***Mettre en œuvre un contrôle d'accès respectant le principe du moindre privilège***

L'accès à l'environnement de production du Sous-traitant est accordé en fonction du rôle.

Q. ***Sécurité lors du transfert et du traitement***

Le Sous-traitant ne permet pas la conservation des données du Client dans l'environnement d'entreprise du Sous-traitant, où résident les employés et les prestataires du Sous-traitant. L'environnement de production du Sous-traitant est séparé logiquement et physiquement de l'environnement d'entreprise du Sous-traitant :

1. L'accès à l'environnement de production du Sous-traitant se fait via un VPN authentifié à deux facteurs utilisant des périphériques approuvés par le Sous-traitant et n'est fourni qu'aux employés et prestataires du Sous-traitant dont le rôle nécessite un accès.
2. Des pare-feu conformes aux normes du secteur sont mis en place et configurés pour autoriser uniquement le trafic sur les ports nécessaires au fonctionnement des Services, tous les autres étant refusés par défaut.
3. Tous les accès Administrateurs aux interfaces Internet hébergées par les Services sont cryptés via HTTPS/TLS.

Contrôles d'accès au système

1. LDAP est utilisé pour l'authentification du personnel du Sous-traitant auprès des environnements de production.
2. Un accès privilégié n'est accordé qu'au personnel autorisé du Sous-traitant.

Sécurité des postes de travail

1. Les postes de travail utilisés pour accéder à l'environnement de production du Sous-traitant de données sont gérés de manière centralisée, disposent des correctifs de sécurité applicables, exécutent des logiciels de sécurité standardisés et sont régulièrement analysés pour détecter les vulnérabilités.

Sécurité du serveur

1. Les correctifs de sécurité applicables sont appliqués en fonction de leur criticité.
2. Les services inutiles sont désactivés.
3. Les mots de passe par défaut sont changés.

R. ***Sécurité lors de la transmission de données sur des réseaux publics***

1. Tous les accès administratifs du Sous-traitant aux Services sont cryptés via HTTPS/TLS.

S. ***Contrôles de la phase de mise en œuvre et d'exploitation***

La fonctionnalité fournie par les Services est exécutée automatiquement et ne nécessite pas d'intervention humaine, sauf à des fins d'analyse et pour résoudre les problèmes liés aux Services. Les Services sont conçus pour fonctionner comme décrit dans le Contrat de prestations de services.

T. ***Traçabilité de tout accès, modification et suppression***

L'accès aux systèmes utilisés par les Services est contrôlé de la manière suivante :

1. L'accès est accordé en fonction du rôle chez le Sous-traitant.
2. Seul le personnel autorisé est autorisé à avoir un accès privilégié à un environnement de production du Sous-traitant.
3. La journalisation des audits est en place sur le VPN et sur les systèmes de l'environnement de production du Sous-traitant.
4. Les journaux d'audit générés par les services enregistrent l'accès aux Services par le personnel du Responsable du traitement de données.

U. *Garantie d'un traitement des données conforme*

Sauf à des fins d'analyse et pour résoudre les problèmes liés aux Services, le personnel du Sous-traitant ne traite pas manuellement les données des clients. Toutes les données des clients sont traitées automatiquement par les Services, comme décrit dans la documentation des Services.

V. *Garantie de la disponibilité*

Cela est réalisé de la manière suivante :

1. Les infrastructures de chaque installation de production sont configurées en mode haute disponibilité, avec une double alimentation électrique et deux connexions réseau différentes au minimum.
2. Les installations de colocation sont conformes aux normes des centres de données de niveau III, y compris l'alimentation redondante et les contrôles environnementaux redondants.
3. Les installations de colocation sont équipées de générateurs sur site avec un approvisionnement en carburant d'au moins deux (2) jours.
4. Un plan de continuité des activités pour la protection du personnel du Sous-traitant de données et la reprise des processus opérationnels du Sous-traitant de données est documenté et testé chaque année.
5. Une infrastructure de surveillance distribuée contrôle la disponibilité et les performances.
6. .

W. *Séparation des données*

Les Services garantissent la séparation des données des clients. Cela est réalisé de la manière suivante :

1. La séparation logique est assurée par le service en utilisant tout ou partie des éléments suivants :
   a. Des ID client uniques pour chaque client qui sont utilisés pour marquer les données du client au sein du service ;
   b. Des IP uniques ;
   c. Des clés de cryptage uniques.

ANNEXE 2

Clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil.

CLAUSES CONTRACTUELLES TYPES

Responsable du traitement et sous-traitant

SECTION I

Clause 1

Finalités et champ d'application

(a) Les présentes clauses contractuelles types visent à garantir le respect des exigences du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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) en cas de transfert de données à caractère personnel vers un pays tiers.

(b) Les parties :

(i) la ou les personnes physiques ou morales, la ou les autorités publiques, la ou les agences ou autre(s) organisme(s) (ci-après la ou les « entités ») qui transfèrent les données à caractère personnel, mentionnés à l'annexe I.A (ci-après l'« exportateur de données »), et

(ii) la ou les entités d'un pays tiers qui reçoivent les données à caractère personnel de l'exportateur de données, directement ou indirectement par l'intermédiaire d'une autre entité également partie aux présentes clauses, mentionnées à l'annexe I.A. (ci-après l'« importateur de données »), sont convenues des présentes clauses contractuelles types (ci-après les « Clauses »).

(c) Les présentes Clauses s'appliquent au transfert de données à caractère personnel précisé à l'Annexe I.B.

(d) L'appendice aux présentes clauses, qui contient les annexes qui y sont mentionnées, fait partie intégrante des présentes clauses.

Clause 2

Effet et invariabilité des clauses

(a) Les présentes clauses établissent des garanties appropriées, notamment des droits opposables pour la personne concernée et des voies de droit effectives, en vertu de l'article 46, paragraphe 1, et de l'article 46, paragraphe 2, point c), du règlement (UE) 2016/679 et, en ce qui concerne les transferts de données de responsables du traitement à sous-traitants et/ou de sous-traitants à sous-traitants, des clauses contractuelles types en vertu de l'article 28, paragraphe 7, du règlement (UE) 2016/679, à condition qu'elles ne soient pas modifiées, sauf pour sélectionner le ou les modules appropriés ou pour ajouter ou mettre à jour des informations dans l'appendice. Cela n'empêche pas les parties d'inclure les clauses contractuelles types prévues dans les présentes clauses dans un contrat plus large et/ou d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les présentes clauses et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

(b) Les présentes clauses sont sans préjudice des obligations auxquelles l'exportateur de données est soumis en vertu du règlement (UE) 2016/679.

Clause 3

Tiers bénéficiaires

(a) Les personnes concernées peuvent invoquer et faire appliquer les présentes clauses, en tant que tiers bénéficiaires, contre l'exportateur et/ou l'importateur de données, avec les exceptions suivantes :

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7 ;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) et (e) ;

(iii) Clause 9 – Clause 9(a), (c), (d) et (e) ;

(iv) Clause 12 – Clause 12(a), (d) et (f) ;

(v) Clause 13 ;

(vi) Clause 15.1(c), (d) et (e) ;

(vii) Clause 16(e) ;
(viii) Clause 18 – Clause 18(a) et (b)
(b) Le paragraphe a) est sans préjudice des droits des personnes concernées au titre du règlement (UE) 2016/679.

Clause 4

Interprétation
(a) Lorsque les présentes clauses utilisent des termes définis dans le règlement (UE) 2016/679, ceux-ci ont la même signification que dans ledit règlement.

(b) Les présentes clauses sont lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679.

(c) Les présentes clauses ne sont pas interprétées dans un sens contraire aux droits et obligations prévus dans le règlement (UE) 2016/679.

Clause 5

Hiérarchie
En cas de contradiction entre les présentes clauses et les dispositions des accords connexes entre les parties existant au moment où les présentes clauses sont convenues, ou souscrites par la suite, les présentes clauses prévalent.

Clause 6

Description du ou des transferts
Les détails du ou des transferts, en particulier les catégories de données à caractère personnel qui sont transférées et la ou les finalités pour lesquelles elles le sont, sont précisés à l'Annexe I.B.

Clause 7 – Facultative

Clause d'adhésion – Non applicable

SECTION II – OBLIGATIONS DES PARTIES

Clause 8

Garanties en matière de protection des données
L'exportateur de données garantit qu'il a entrepris des démarches raisonnables pour s'assurer que l'importateur de données est à même, par la mise en œuvre de mesures techniques et organisationnelles appropriées, de satisfaire aux obligations qui lui incombent en vertu des présentes clauses.

Transfert de responsable du traitement à sous-traitant

8.1 **Instructions**
(a) L'importateur de données ne traite les données à caractère personnel que sur instructions documentées de l'exportateur de données. L'exportateur de données peut donner ces instructions pendant toute la durée du contrat.
(b) S'il n'est pas en mesure de suivre ces instructions, l'importateur de données en informe immédiatement l'exportateur de données.

8.2 **Limitation des finalités**
L'importateur de données traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du transfert, telles que précisées à l'Annexe I.B, sauf en cas d'instructions supplémentaires de l'exportateur de données.

8.3 **Transparence**

Sur demande, l'exportateur de données met gratuitement à la disposition de la personne concernée une copie des présentes clauses, notamment de l'appendice tel que rempli par les parties. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les mesures décrites à l'Annexe II et les données à caractère personnel, l'exportateur de données peut occulter une partie du texte de l'appendice aux présentes clauses avant d'en communiquer une copie, mais fournit un résumé valable s'il serait autrement impossible, pour la personne concernée, d'en comprendre le contenu ou d'exercer ses droits. Les parties fournissent à la personne concernée, à la demande de celle-ci, les motifs des occultations, dans la mesure du possible sans révéler les informations occultées. Cette clause est sans préjudice des obligations qui incombent à l'exportateur de données en vertu des articles 13 et 14 du règlement (UE) 2016/679.

8.4 **Exactitude**

Si l'importateur de données se rend compte que les données à caractère personnel qu'il a reçues sont inexactes, ou sont obsolètes, il en informe l'exportateur de données dans les meilleurs délais. Dans ce cas, l'importateur de données coopère avec l'exportateur de données pour effacer ou rectifier les données.

8.5 **Durée du traitement et effacement ou restitution des données**

Le traitement par l'importateur de données n'a lieu que pendant la durée précisée à l'Annexe I.B. Au terme de la prestation des services de traitement, l'importateur de données, à la convenance de l'exportateur de données, efface toutes les données à caractère personnel traitées pour le compte de ce dernier et lui en apporte la preuve, ou lui restitue toutes les données à caractère personnel traitées pour son compte et efface les copies existantes. Jusqu'à ce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement des données à caractère personnel, ce dernier garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données à caractère personnel que dans la mesure où et aussi longtemps que cette législation locale l'exige. Ceci est sans préjudice de la clause 14, en particulier de l'obligation imposée à l'importateur de données par la clause 14, paragraphe e), d'informer l'exportateur de données, pendant toute la durée du contrat, s'il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences de la clause 14, paragraphe a).

8.6 **Sécurité du traitement**

(a) L'importateur de données et, durant la transmission, l'exportateur de données mettent en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données, notamment pour les protéger d'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à ces données (ci-après la « violation de données à caractère personnel »). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et de la ou des finalités du traitement ainsi que des risques inhérents au traitement pour les personnes concernées. Les parties envisagent en particulier de recourir au chiffrement ou à la pseudonymisation, notamment pendant la transmission, lorsque la finalité du traitement peut être atteinte de cette manière. En cas de pseudonymisation, les informations supplémentaires permettant d'attribuer les données à caractère personnel à une personne concernée précise restent, dans la mesure du possible, sous le contrôle exclusif de l'exportateur de données. Pour s'acquitter des obligations qui lui incombent en vertu du présent paragraphe, l'importateur de données met au moins en œuvre les mesures techniques et organisationnelles précisées à l'Annexe II. Il procède à des contrôles réguliers pour s'assurer que ces mesures continuent d'offrir le niveau de sécurité approprié.

(b) L'importateur de données ne donne l'accès aux données à caractère personnel aux membres de son personnel que dans la mesure strictement nécessaire à la mise en œuvre, à la gestion et au suivi du contrat. Il veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

(c) En cas de violation de données à caractère personnel concernant des données à caractère personnel traitées par l'importateur de données au titre des présentes clauses, ce dernier prend des mesures appropriées pour remédier à la violation, y compris des mesures visant à en atténuer les effets négatifs.

L'importateur de données informe également l'exportateur de données de cette violation dans les meilleurs délais après en avoir eu connaissance. Cette notification contient les coordonnées d'un point de contact auprès duquel il est possible d'obtenir plus d'informations, ainsi qu'une description de la nature de la violation (y compris, si possible, les catégories et le nombre approximatif de personnes concernées et d'enregistrements de données à caractère personnel concernés), de ses conséquences probables et des mesures prises ou proposées pour y remédier, y compris, le cas échéant, des mesures visant à en atténuer les effets négatifs potentiels. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et les autres informations sont fournies par la suite, dans les meilleurs délais, à mesure qu'elles deviennent disponibles.

(d) L'importateur de données coopère avec l'exportateur de données et l'aide afin de lui permettre de respecter les obligations qui lui incombent en vertu du règlement (UE) 2016/679, notamment celle d'informer l'autorité de contrôle compétente et les personnes concernées, compte tenu de la nature du traitement et des informations à la disposition de l'importateur de données.

8.7 **Données sensibles**

Lorsque le transfert concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne, ou des données relatives à des condamnations pénales et à des infractions (ci-après les « données sensibles »), l'importateur de données applique les restrictions particulières et/ou les garanties supplémentaires décrites à l'Annexe I.B.

8.8 **Transferts ultérieurs**

L'importateur de données ne divulgue les données à caractère personnel à un tiers que sur instructions documentées de l'exportateur de données. En outre, les données ne peuvent être divulguées à un tiers situé en dehors de l'Union européenne (4) (dans le même pays que l'importateur de données ou dans un autre pays tiers, ci-après « transfert ultérieur »), que si le tiers est lié par les présentes clauses ou accepte de l'être, en vertu du module approprié, ou si :

(i) le transfert ultérieur est effectué vers un pays bénéficiant d'une décision d'adéquation en vertu de l'article 45 du règlement (UE) 2016/679 qui couvre le transfert ultérieur ;

(ii) le tiers offre d'une autre manière des garanties appropriées conformément aux articles 46 ou 47 du règlement (UE) 2016/679 en ce qui concerne le traitement en question ;

(iii) le transfert ultérieur est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice dans le contexte de procédures administratives, réglementaires ou judiciaires spécifiques ; ou

(iv) le transfert ultérieur est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Tout transfert ultérieur est soumis au respect, par l'importateur de données, de toutes les autres garanties au titre des présentes clauses, en particulier de la limitation des finalités.

8.9 **Documentation et conformité**

(a) L'importateur de données traite rapidement et de manière appropriée les demandes de renseignements de l'exportateur de données concernant le traitement au titre des présentes clauses.

(b) Les parties sont en mesure de démontrer le respect des présentes clauses. En particulier, l'importateur de données conserve une trace documentaire appropriée des activités de traitement menées pour le compte de l'exportateur de données.

(c) L'importateur de données met à la disposition de l'exportateur de données toutes les informations nécessaires pour démontrer le respect des obligations prévues par les présentes clauses et, à la

demande de l'exportateur de données, pour permettre la réalisation d'audits des activités de traitement couvertes par les présentes clauses, et contribuer à ces audits, à intervalles raisonnables ou s'il existe des indications de non-respect. Lorsqu'il décide d'un examen ou d'un audit, l'exportateur de données peut tenir compte des certifications pertinentes détenues par l'importateur de données.

(d) L'exportateur de données peut choisir de procéder à l'audit lui-même ou de mandater un auditeur indépendant. Les audits peuvent comprendre des inspections dans les locaux ou les installations physiques de l'importateur de données et sont, le cas échéant, effectués avec un préavis raisonnable.

(e) Les parties mettent à la disposition de l'autorité de contrôle compétente, à la demande de celle-ci, les informations mentionnées aux paragraphes b) et c), y compris les résultats de tout audit.

_____

(4) L'accord sur l'Espace économique européen (accord EEE) prévoit l'extension du marché intérieur de l'Union européenne aux trois pays de l'EEE que sont l'Islande, le Liechtenstein et la Norvège. La législation de l'Union en matière de protection des données, notamment le règlement (UE) 2016/679, est couverte par l'accord EEE et a été intégrée dans l'Annexe XI de celui-ci. Dès lors, une divulgation par l'importateur de données à un tiers situé dans l'EEE ne peut être qualifiée de transfert ultérieur aux fins des présentes clauses.

Clause 9

Recours à des sous-traitants ultérieurs

(a) AUTORISATION ÉCRITE GÉNÉRALE – L'importateur de données a l'autorisation générale de l'exportateur de données de recruter un ou plusieurs sous-traitants ultérieurs à partir d'une liste arrêtée d'un commun accord. L'importateur de données informe expressément par écrit l'exportateur de données de tout changement concernant l'ajout ou le remplacement de sous-traitants ultérieurs qu'il est prévu d'apporter à cette liste au moins 30 jours à l'avance, donnant ainsi à l'exportateur de données suffisamment de temps pour émettre des objections à l'encontre de ces changements avant le recrutement du ou des sous-traitants ultérieurs. L'importateur de données fournit à l'exportateur de données les informations nécessaires pour permettre à ce dernier d'exercer son droit d'émettre des objections.

(b) Lorsque l'importateur de données recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte de l'exportateur de données), il le fait au moyen d'un contrat écrit qui prévoit, en substance, les mêmes obligations en matière de protection des données que celles qui lient l'importateur de données au titre des présentes clauses, notamment en ce qui concerne les droits du tiers bénéficiaire pour les personnes concernées. (8) Les parties conviennent qu'en respectant la présente clause, l'importateur de données satisfait aux obligations qui lui incombent en vertu de la clause 8.8. L'importateur de données veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses.

(c) L'importateur de données fournit à l'exportateur de données, à la demande de celui-ci, une copie du contrat avec le sous-traitant ultérieur et de ses éventuelles modifications ultérieures. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les données à caractère personnel, l'importateur de données peut occulter une partie du texte du contrat avant d'en communiquer une copie.

(d) L'importateur de données reste pleinement responsable à l'égard de l'exportateur de données de l'exécution des obligations qui incombent au sous-traitant ultérieur en vertu du contrat qu'il a conclu avec lui. L'importateur de données notifie à l'exportateur de données tout manquement du sous-traitant ultérieur aux obligations qui lui incombent en vertu dudit contrat.

(e) L'importateur de données convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire en vertu de laquelle, dans les cas où l'importateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'exportateur de données a le droit de résilier le contrat du sous-traitant ultérieur et de donner instruction à ce dernier d'effacer ou de restituer les données à caractère personnel.

(8) Cette exigence peut être satisfaite par l'adhésion du sous-traitant ultérieur aux présentes clauses en vertu du module approprié, conformément à la clause 7.

Clause 10

Droits des personnes concernées

(a) L'importateur de données informe rapidement l'exportateur de données de toute demande reçue d'une personne concernée. Il ne répond pas lui-même à cette demande, à moins d'y avoir été autorisé par l'exportateur de données.

(b) L'importateur de données aide l'exportateur de données à s'acquitter de son obligation de répondre aux demandes de personnes concernées désireuses d'exercer leurs droits en vertu du règlement (UE) 2016/679. À cet égard, les parties indiquent à l'Annexe II les mesures techniques et organisationnelles appropriées, compte tenu de la nature du traitement, au moyen desquelles l'aide sera fournie, ainsi que la portée et l'étendue de l'aide requise.

(c) Lorsqu'il s'acquitte des obligations qui lui incombent en vertu des paragraphes a) et b), l'importateur de données se conforme aux instructions de l'exportateur de données.

Clause 11

Voies de recours

(a) L'importateur de données informe les personnes concernées, sous une forme transparente et aisément accessible, au moyen d'une notification individuelle ou sur son site Web, d'un point de contact autorisé à traiter les réclamations. Il traite sans délai toute réclamation reçue d'une personne concernée.

(b) En cas de litige entre une personne concernée et l'une des parties portant sur le respect des présentes clauses, cette partie met tout en œuvre pour parvenir à un règlement à l'amiable dans les meilleurs délais. Les parties se tiennent mutuellement informées de ces litiges et, s'il y a lieu, coopèrent pour les résoudre.

(c) Lorsque la personne concernée invoque un droit du tiers bénéficiaire en vertu de la clause 3, l'importateur de données accepte la décision de la personne concernée :

(i) d'introduire une réclamation auprès de l'autorité de contrôle de l'État membre dans lequel se trouve sa résidence habituelle ou son lieu de travail, ou auprès de l'autorité de contrôle compétente au sens de la clause 13 ;
(ii) de renvoyer le litige devant les juridictions compétentes au sens de la clause 18.
(d) Les parties acceptent que la personne concernée puisse être représentée par un organisme, une organisation ou une association à but non lucratif dans les conditions énoncées à l'article 80, paragraphe 1, du règlement (UE) 2016/679.

(e) L'importateur de données se conforme à une décision qui est contraignante en vertu du droit applicable de l'Union ou d'un État membre.

(f) L'importateur de données convient que le choix effectué par la personne concernée ne remettra pas en cause le droit procédural et matériel de cette dernière d'obtenir réparation conformément à la législation applicable.

Clause 12

Responsabilité

(a) Chaque partie est responsable envers la ou les autres parties des dommages qu'elle cause à l'autre ou aux autres parties du fait d'un manquement aux présentes clauses.

(b) L'importateur de données est responsable à l'égard de la personne concernée, et la personne concernée a le droit d'obtenir réparation de tout dommage matériel ou moral qui lui est causé par l'importateur de données ou son sous-traitant ultérieur du fait d'une violation des droits du tiers bénéficiaire prévus par les présentes clauses.

(c) Nonobstant le paragraphe b), l'exportateur de données est responsable à l'égard de la personne concernée et celle-ci a le droit d'obtenir réparation de tout dommage matériel ou moral qui lui est causé par l'exportateur de données ou l'importateur de données (ou son sous-traitant ultérieur) du fait d'une

violation des droits du tiers bénéficiaire prévus par les présentes clauses. Ceci est sans préjudice de la responsabilité de l'exportateur de données et, si l'exportateur de données est un sous-traitant agissant pour le compte d'un responsable du traitement, de la responsabilité de ce dernier au titre du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725, selon le cas.

(d) Les parties conviennent que, si l'exportateur de données est reconnu responsable, en vertu du paragraphe c), du dommage causé par l'importateur de données (ou son sous-traitant ultérieur), il a le droit de réclamer auprès de l'importateur de données la part de la réparation correspondant à la responsabilité de celui-ci dans le dommage.

(e) Lorsque plusieurs parties sont responsables d'un dommage causé à la personne concernée du fait d'une violation des présentes clauses, toutes les parties responsables le sont conjointement et solidairement et la personne concernée a le droit d'intenter une action en justice contre n'importe laquelle de ces parties.

(f) Les parties conviennent que, si la responsabilité d'une d'entre elles est reconnue en vertu du paragraphe e), celle-ci a le droit de réclamer auprès de l'autre ou des autres parties la part de la réparation correspondant à sa/leur responsabilité dans le dommage.

(g) L'importateur de données ne peut invoquer le comportement d'un sous-traitant ultérieur pour échapper à sa propre responsabilité.

Clause 13

Contrôle

(a) [Si l'exportateur de données est établi dans un État membre de l'UE :] L'autorité de contrôle chargée de garantir le respect par l'exportateur de données du Règlement (UE) 2016/679 en ce qui concerne le transfert de données, comme indiqué à l'Annexe I.C, agit en tant qu'autorité de contrôle compétente. [Si l'exportateur de données n'est pas établi dans un État membre de l'UE, mais relève du champ d'application territorial du Règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2, et qu'il a désigné un représentant au sens de l'article 27, paragraphe 1, du Règlement (UE) 2016/679 :] L'autorité de contrôle de l'État membre dans lequel le représentant au sens de l'article 27, paragraphe 1, du Règlement (UE) 2016/679 est établi, comme indiqué à l'Annexe I.C, agit en tant qu'autorité de contrôle compétente. [Lorsque l'exportateur de données n'est pas établi dans un État membre de l'UE, mais relève du champ d'application territorial du Règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2, sans toutefois avoir à désigner un représentant au sens de l'article 27, paragraphe 2, du Règlement (UE) 2016/679 :] L'autorité de contrôle d'un des États membres dans lesquels se trouvent les personnes concernées dont les données à caractère personnel sont transférées au titre des présentes clauses en lien avec l'offre de biens ou de services ou dont le comportement fait l'objet d'un suivi, telle qu'indiquée à l'Annexe I.C, agit en qualité d'autorité compétente.

(b) L'importateur de données accepte de se soumettre à la juridiction de l'autorité de contrôle compétente et de coopérer avec elle dans le cadre de toute procédure visant à garantir le respect des présentes clauses. En particulier, l'importateur de données accepte de répondre aux demandes de renseignements, de se soumettre à des audits et de se conformer aux mesures adoptées par l'autorité de contrôle, notamment aux mesures correctrices et compensatoires. Il confirme par écrit à l'autorité de contrôle que les mesures nécessaires ont été prises.

SECTION III – LÉGISLATIONS LOCALES ET OBLIGATIONS EN CAS D'ACCÈS DES AUTORITÉS PUBLIQUES

Clause 14

Législations et pratiques locales ayant une incidence sur le respect des clauses

(a) Les parties garantissent qu'elles n'ont aucune raison de croire que la législation et les pratiques du pays tiers de destination applicables au traitement des données à caractère personnel par l'importateur de données, notamment les exigences en matière de divulgation de données à caractère personnel ou les mesures autorisant l'accès des autorités publiques à ces données, empêchent l'importateur de données de s'acquitter des obligations qui lui incombent en vertu des présentes clauses. Cette disposition repose sur l'idée que les législations et les pratiques qui respectent l'essence des libertés et droits fondamentaux et qui n'excèdent pas ce qui est nécessaire et proportionné dans une société

démocratique pour préserver un des objectifs énumérés à l'article 23, paragraphe 1, du règlement (UE) 2016/679 ne sont pas en contradiction avec les présentes clauses.

(b) Les parties déclarent qu'en fournissant la garantie mentionnée au paragraphe a), elles ont dûment tenu compte, en particulier, des éléments suivants :

(i) des circonstances particulières du transfert, parmi lesquelles la longueur de la chaîne de traitement, le nombre d'acteurs concernés et les canaux de transmission utilisés ; les transferts ultérieurs prévus ; le type de destinataire ; la finalité du traitement ; les catégories et le format des données à caractère personnel transférées ; le secteur économique dans lequel le transfert a lieu et le lieu de stockage des données transférées ;

(ii) des législations et des pratiques du pays tiers de destination – notamment celles qui exigent la divulgation de données aux autorités publiques ou qui autorisent l'accès de ces dernières aux données – pertinentes au regard des circonstances particulières du transfert, ainsi que des limitations et des garanties applicables (12) ;

(iii) de toute garantie contractuelle, technique ou organisationnelle pertinente mise en place pour compléter les garanties prévues par les présentes clauses, y compris les mesures appliquées pendant la transmission et au traitement des données à caractère personnel dans le pays de destination.

(c) L'importateur de données garantit que, lors de l'évaluation au titre du paragraphe b), il a déployé tous les efforts possibles pour fournir des informations pertinentes à l'exportateur de données et convient qu'il continuera à coopérer avec ce dernier pour garantir le respect des présentes clauses.

(d) Les parties conviennent de conserver une trace documentaire de l'évaluation au titre du paragraphe b) et de mettre cette évaluation à la disposition de l'autorité de contrôle compétente si celle-ci en fait la demande.

(e) L'importateur de données accepte d'informer sans délai l'exportateur de données si, après avoir souscrit aux présentes clauses et pendant la durée du contrat, il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences du paragraphe a), notamment à la suite d'une modification de la législation du pays tiers ou d'une mesure (telle qu'une demande de divulgation) indiquant une application pratique de cette législation qui n'est pas conforme aux exigences du paragraphe a).

(f) À la suite d'une notification au titre du paragraphe e), ou si l'exportateur de données a d'autres raisons de croire que l'importateur de données ne peut plus s'acquitter des obligations qui lui incombent en vertu des présentes clauses, l'exportateur de données définit sans délai les mesures appropriées (par exemple des mesures techniques ou organisationnelles visant à garantir la sécurité et la confidentialité) qu'il doit adopter et/ou qui doivent être adoptées par l'importateur de données pour remédier à la situation. L'exportateur de données suspend le transfert de données s'il estime qu'aucune garantie appropriée ne peut être fournie pour ce transfert ou si l'autorité de contrôle compétente lui en donne l'instruction. Dans ce cas, l'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement de données à caractère personnel au titre des présentes clauses. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient convenues autrement. Lorsque le contrat est résilié en vertu de la présente clause, la clause 16, paragraphes d) et e), s'applique.

---

(12) En ce qui concerne l'incidence de ces législations et pratiques sur le respect des présentes clauses, différents éléments peuvent être considérés comme faisant partie d'une évaluation globale. Ces éléments peuvent inclure une expérience concrète, documentée et pertinente de cas antérieurs de demandes de divulgation émanant d'autorités publiques, ou l'absence de telles demandes, couvrant un laps de temps suffisamment représentatif. Il peut s'agir de registres internes ou d'autres documents établis de manière continue conformément au principe de diligence raisonnable et certifiés à un niveau hiérarchique élevé, pour autant que ces informations puissent être partagées légalement avec des tiers. Lorsque cette expérience pratique est invoquée pour conclure que l'importateur de données ne sera pas empêché de respecter les présentes clauses, il y a lieu de l'étayer par d'autres éléments pertinents et objectifs, et il appartient aux parties d'examiner avec soin si ces éléments, pris dans leur ensemble, ont un poids suffisant, du point de vue de leur fiabilité et de leur représentativité, pour soutenir cette conclusion. En particulier, les parties doivent s'assurer que leur expérience pratique est corroborée et non contredite par des informations fiables accessibles au public ou disponibles d'une autre manière sur l'existence ou l'absence de demandes dans le même secteur et/ou sur l'application pratique du droit, comme la jurisprudence et les rapports d'organes de contrôle indépendants.

Clause 15

Obligations de l'importateur de données en cas d'accès des autorités publiques

15.1 **Notification**

(a) L'importateur de données convient d'informer sans délai l'exportateur de données et, si possible, la personne concernée (si nécessaire avec l'aide de l'exportateur de données) :

(i) s'il reçoit une demande juridiquement contraignante d'une autorité publique, y compris judiciaire, en vertu de la législation du pays de destination en vue de la divulgation de données à caractère personnel transférées au titre des présentes clauses ; cette notification comprend des informations sur les données à caractère personnel demandées, l'autorité requérante, la base juridique de la demande et la réponse fournie ; ou

(ii) s'il a connaissance d'un quelconque accès direct des autorités publiques aux données à caractère personnel transférées au titre des présentes clauses en vertu de la législation du pays de destination ; cette notification comprend toutes les informations dont l'importateur de données dispose.

(b) Si la législation du pays de destination interdit à l'importateur de données d'informer l'exportateur de données et/ou la personne concernée, l'importateur de données convient de tout mettre en œuvre pour obtenir une levée de cette interdiction, en vue de communiquer autant d'informations que possible, dans les meilleurs délais. L'importateur de données accepte de garder une trace documentaire des efforts qu'il a déployés afin de pouvoir en apporter la preuve à l'exportateur de données, si celui-ci lui en fait la demande.

(c) Lorsque la législation du pays de destination le permet, l'importateur de données accepte de fournir à l'exportateur de données, à intervalles réguliers pendant la durée du contrat, autant d'informations utiles que possible sur les demandes reçues (notamment le nombre de demandes, le type de données demandées, la ou les autorités requérantes, la contestation ou non des demandes et l'issue de ces contestations, etc.).

(d) L'importateur de données accepte de conserver les informations mentionnées aux paragraphes a) à c) pendant la durée du contrat et de les mettre à la disposition de l'autorité de contrôle compétente si celle-ci lui en fait la demande.

(e) Les paragraphes a) à c) sont sans préjudice de l'obligation incombant à l'importateur de données, en vertu de la clause 14, paragraphe e), et de la clause 16, d'informer sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentes clauses.

15.2 **Contrôle de la légalité et minimisation des données**

(a) L'importateur de données accepte de contrôler la légalité de la demande de divulgation, en particulier de vérifier si elle s'inscrit dans les limites des pouvoirs conférés à l'autorité publique requérante, et de la contester si, après une évaluation minutieuse, il conclut qu'il existe des motifs raisonnables de considérer qu'elle est illégale en vertu de la législation du pays de destination, des obligations applicables en vertu du droit international et des principes de courtoisie internationale. L'importateur de données exerce les possibilités d'appel ultérieures dans les mêmes conditions. Lorsqu'il conteste une demande, l'importateur de données demande des mesures provisoires visant à suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente se prononce sur son bien-fondé. Il ne divulgue pas les données à caractère personnel demandées tant qu'il n'est pas obligé de le faire en vertu des règles de procédure applicables. Ces exigences sont sans préjudice des obligations incombant à l'importateur de données en vertu de la clause 14, paragraphe e).

(b) L'importateur de données accepte de garder une trace documentaire de son évaluation juridique ainsi que de toute contestation de la demande de divulgation et, dans la mesure où la législation du pays de destination le permet, de mettre les documents concernés à la disposition de l'exportateur de données. Il les met également à la disposition de l'autorité de contrôle compétente si celle-ci lui en fait la demande.

(c) L'importateur de données accepte de fournir le minimum d'informations autorisé lorsqu'il répond à une demande de divulgation, sur la base d'une interprétation raisonnable de la demande.

SECTION IV – DISPOSITIONS FINALES

Clause 16

Non-respect des clauses et résiliation

(a) L'importateur de données informe sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentes clauses, quelle qu'en soit la raison.

(b) Dans le cas où l'importateur de données enfreint les présentes clauses ou n'est pas en mesure de les respecter, l'exportateur de données suspend le transfert de données à caractère personnel à l'importateur de données jusqu'à ce que le respect des présentes clauses soit à nouveau garanti ou que le contrat soit résilié. Ceci est sans préjudice de la clause 14, paragraphe f).

(c) L'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement de données à caractère personnel au titre des présentes clauses, lorsque :

(i) l'exportateur de données a suspendu le transfert de données à caractère personnel à l'importateur de données en vertu du paragraphe b) et que le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;

(ii) l'importateur de données enfreint gravement ou de manière persistante les présentes clauses ;

(iii) l'importateur de données ne se conforme pas à une décision contraignante d'une juridiction ou d'une autorité de contrôle compétente concernant les obligations qui lui incombent au titre des présentes clauses.

Dans ces cas, il informe l'autorité de contrôle compétente de ce non-respect. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient convenues autrement.

(d) Les données à caractère personnel qui ont été transférées avant la résiliation du contrat au titre du paragraphe c) sont immédiatement restituées à l'exportateur de données ou effacées dans leur intégralité, à la convenance de celui-ci. Il en va de même pour toute copie des données. L'importateur de données apporte la preuve de l'effacement des données à l'exportateur de données. Jusqu'à ce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement des données à caractère personnel transférées, ce dernier garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données que dans la mesure où et aussi longtemps que cette législation locale l'exige.

(e) Chaque partie peut révoquer son consentement à être liée par les présentes clauses i) si la Commission européenne adopte une décision en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 qui couvre le transfert de données à caractère personnel auquel les présentes clauses s'appliquent ; ou ii) si le règlement (UE) 2016/679 est intégré dans le cadre juridique du pays vers lequel les données à caractère personnel sont transférées. Ceci est sans préjudice des autres obligations qui s'appliquent au traitement en question en vertu du règlement (UE) 2016/679.

Clause 17

Droit applicable

Les présentes Clauses sont régies par le droit d'un des États membres de l'Union européenne, pour autant que ce droit reconnaisse des droits au tiers bénéficiaire. Les parties conviennent qu'il s'agira : (a) du droit du pays spécifié dans le Contrat de prestation de services si ledit Contrat est régi par le droit d'un État membre de l'UE, ou (b) du droit néerlandais si le Contrat de prestation de services est régi par le droit d'un pays tiers.

Clause 18
Élection de for et juridiction

Tout litige survenant du fait des présentes clauses est tranché par les juridictions d'un État membre de l'Union européenne.

(a) Les Parties conviennent qu'il s'agit des tribunaux (i) spécifiés dans le Contrat de prestation de services si celui-ci a désigné un tribunal d'un État membre de l'UE, ou (ii) des tribunaux d'Amsterdam si le Contrat de prestation de services a désigné un tribunal d'un pays tiers.

(b) La personne concernée peut également poursuivre l'exportateur et/ou l'importateur de données devant les juridictions de l'État membre dans lequel elle a sa résidence habituelle.

(c) Les parties acceptent de se soumettre à la compétence de ces juridictions.

NOTE EXPLICATIVE :

APPENDICE

Il doit être possible de distinguer clairement les informations applicables à chaque transfert ou catégorie de transferts et, à cet égard, de déterminer le ou les rôles respectifs des parties en tant qu'exportateur(s) et/ou importateur(s) de données. Il n'est pas forcément nécessaire de remplir et de signer des appendices distincts pour chaque transfert/catégorie de transferts et/ou relation contractuelle, si cette transparence peut être garantie au moyen d'un seul appendice. Toutefois, si cela est nécessaire pour garantir une clarté suffisante, il convient d'utiliser des appendices distincts.

ANNEXE I

A. **LISTE DES PARTIES**

Exportateur(s) de données : L'exportateur de données est désigné comme le Responsable du traitement à la page 1 du présent ATD.

Importateur(s) de données : L'importateur de données est Proofpoint, Inc., un fournisseur de services de sécurité de messagerie et de réseaux sociaux, d'analyse des menaces et de formation à la sécurité.

B. **DESCRIPTION DU TRANSFERT**

Les **Personnes concernées** sont les employés et prestataires du Responsable du traitement, ainsi que les employés et prestataires des clients et des fournisseurs du Responsable du traitement.

Catégories de données : les catégories de données sont stipulées dans l'Appendice 1 du présent ATD. Le Responsable du traitement ne transférera pas de données sensibles à Proofpoint.

Opérations de traitement : la fréquence de transfert, la nature et la finalité du traitement, ainsi que la période de conservation, sont stipulées à l'Appendice 1 du présent ATD.

C. **AUTORITÉS DE CONTRÔLE COMPÉTENTES** ***Indiquez la ou les autorités de contrôle compétentes conformément à la Clause 13***

[Si l'exportateur de données est établi dans un État membre de l'UE :] L'autorité de contrôle de l'État membre du siège social de l'exportateur de données.

[Si l'exportateur de données n'est pas établi dans un État membre de l'UE, mais relève du champ d'application territorial du Règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2, et qu'il a désigné un représentant au sens de l'article 27, paragraphe 1, du Règlement (UE) 2016/679 :] L'autorité de contrôle de l'État membre du siège social de l'exportateur de données.

[Si l'exportateur de données n'est pas établi dans un État membre de l'Union, mais relève du champ d'application territorial du règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2 sans toutefois avoir à désigner un représentant en vertu de l'article 27, paragraphe 2, du Règlement (UE) 2016/679 :] L'autorité de contrôle aux Pays-Bas.

ANNEXE II

MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS LES MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À GARANTIR LA SÉCURITÉ DES DONNÉES

Les mesures de sécurité, techniques et organisationnelles sont décrites à l'Appendice 2 du présent ATD.

ANNEXE III

LISTE DES SOUS-TRAITANTS ULTÉRIEURS

La liste actuelle des sous-traitants ultérieurs du Service est disponible sur le site de Proofpoint Trust à l'adresse : https://www.proofpoint.com/us/legal/trust