LAUNCHMETRICS

Accord sur le Traitement des Données

Le présent Accord sur le Traitement des Données (« **DPA** ») énonce les conditions générales relatives à la confidentialité et la sécurité des Données Personnelles (telles que définies ci-dessous) associées aux services que le Prestataire de Service (« **nous** », ou « **notre** ») fournit au Client selon le Contrat de Prestation de Service d'Augure (« **Contrat Principal** »).

Si vous avez des questions concernant ce DPA, vous pouvez les envoyer par courrier électronique à legal@launchmetrics.com.

Afin d'éviter toute ambiguïté, les termes en majuscules non définis dans le présent DPA ont le sens qui leur est donné dans d'autres parties du Contrat Principal.

En contrepartie des engagements et accords mutuels du présent DPA et du Contrat Principal, ainsi que de toute autre contrepartie valable, dont la suffisance est par la présente reconnue, le Client et le Prestataire de Service conviennent de ce qui suit :

I. GÉNÉRAL

1.1. **Durée et entrée en vigueur.** Afin de lever toute ambiguïté, ce DPA restera pleinement en vigueur jusqu'à la date de résiliation du Contrat Principal et est applicable à compter de sa signature, mais les engagements énumérés ci-dessous n'entrent en vigueur qu'à partir du 25 mai 2018.

II. DÉFINITIONS

2.1. « **Lois Applicables en matière de Protection des Données** » désigne la législation qui protège les droits et libertés fondamentaux des personnes physiques et, en particulier, leur droit à la vie privée en ce qui concerne le Traitement des Données Personnelles et qui s'applique au Prestataire aux États-Unis et dans l'Union européenne, en ce compris les lois de tout membre de l'Union européenne et le Règlement général sur la protection des données (UE) 2016/679 (le « **RGPD** ») ainsi que tout(e) autre loi, règlement et législation dérivée d'application nationale, avec toutes les modifications et mises à jour successives apportées au sein de la législation française et de toute loi remplaçant le RGPD ou la Loi n°78-17 du 6 janvier 1978 relative au Traitement des données, au stockage des données et aux libertés individuelles (la « **Loi sur la Protection des Données Personnelles** »).

2.2. « **Responsable du Traitement** » a la signification qui lui est donnée dans le RGPD.

2.3. « **Sous-traitant** » a la signification qui lui est donnée dans le RGPD.

2.4. « **EEE** » désigne l'Espace Économique Européen.

2.5. «**Données Personnelles** » désigne toutes les informations se rapportant à une personne physique identifiée ou identifiable, comme un prénom, un nom, une adresse e-mail, une adresse postale, un numéro de téléphone, une date de naissance, un numéro de sécurité sociale (ou son équivalent), un numéro de permis de conduire, un numéro de compte, un numéro de carte bancaire (crédit ou débit), des données de localisation, un numéro d'identification, des renseignements sur l'état de santé ou à caractère médical, tout autre identifiant unique ou un ou plusieurs éléments propres à son identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale ou entendus comme « Renseignements Personnels », « Données à Caractère Personnel », « Données Sensibles », « Données Personnelles », « Catégories Particulières » ou dont le sens est couvert par toute autre appellation similaire dans les Lois Applicables en matière de Protection des Données, sous quelque forme que ce soit, que le Prestataire reçoit, consulte, recueille, Traite, produit, compile ou créé dans le cadre du présent Accord.

2.6. « **Traiter** », « **Traitées** » ou « **Traitement** » désigne toute opération ou ensemble d'opérations portant sur des Données Personnelles, effectuées ou non à l'aide de procédés automatisés, telles que la création, la collecte, la procuration, l'obtention, l'acquisition, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, la diffusion ou toute autre forme de mise à disposition, l'utilisation, la divulgation par transmission, la limitation, l'effacement ou la destruction.

2.7. « **Mesures de Sécurité Techniques et Organisationnelles** » désigne l'ensemble des mesures visant à protéger les Données Personnelles contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la divulgation ou l'accès non autorisés, ainsi que contre toute autre forme de Traitement illicite.

III. PROTECTION DES DONNÉES

3.1. **Conformité avec les lois.** Les parties s'engagent à respecter toutes les exigences des Lois Applicables en matière de Protection des Données.

3.2. **Rôle des Parties.** Ce DPA s'applique lorsque des Données Personnelles sont Traitées par le Prestataire. Le Client est considéré comme étant Responsable du Traitement de ses Données et le Prestataire agit en tant que Sous-Traitant.

3.3. **Instructions de Traitement.** Le Prestataire s'engage à Traiter les Données Personnelles dans le cadre de ses obligations en vertu du présent Contrat uniquement selon les instructions écrites du Client, et le Prestataire consent à agir en accord avec les instructions du Client. Le Prestataire est tenu d'informer le Client par écrit dès que possible s'il n'est pas en mesure de respecter les instructions du Client. Si le Prestataire n'est pas en mesure de respecter les instructions du Client, le Client s'engage à suspendre le transfert ou la divulgation ou l'accès par le Prestataire aux Données Personnelles, et à mettre fin à toute autre activité de Traitement des Données Personnelles par le Prestataire, si cela est nécessaire pour être en conformité avec les Lois Applicables en matière de Protection des Données.

3.4. **Description des Données Personnelles Traitées par le Prestataire.** Une liste concernant la portée et la durée du Traitement, les catégories de personnes concernées et les types de données personnelles Traitées est présentée dans l'annexe 1 de ce DPA.

3.5. **Demandes concernant le Traitement.** Le Prestataire doit Traiter, dans un délai rapide et de la manière appropriée, les demandes du Client portant sur le Traitement des Données Personnelles conformément au présent DPA ou au Contrat Principal.

3.6. **Personnel d'Augure.**

3.6.1 **Obligations de Confidentialité.** Le Prestataire reconnaît que, sauf dans les cas permis par la section applicable du Contrat Principal, le Prestataire et ses employés, agents, consultants et entrepreneurs doivent Traiter de manière strictement confidentielle (i) l'existence et les conditions de ce DPA, de l'Accord et de tout contrat connexe ; (ii) toutes les Données Personnelles (qu'elles soient agrégées ou non et quel que soit le support utilisé) susceptibles d'être divulguées à tout moment au Prestataire ou ses employés, agents, consultants ou entrepreneurs par le Client, les Sociétés affiliées du Client, ou leurs employés, agents, consultants ou entrepreneurs respectifs dans la perspective, dans le cadre ou découlant de l'exécution des services pour et au nom du Client ou des Sociétés affiliées du Client ; (iii) toutes les Données Personnelles (qu'elles soient agrégées ou non et quel que soit le support utilisé) susceptibles d'être Traitées à tout moment par le Prestataire ou ses employés, agents, consultants ou entrepreneurs dans le cadre ou découlant de l'exécution des services pour et au nom du Client ou des Sociétés affiliées du Client ; et (iv) toute information issue des informations décrites aux points (ii) et (iii) ci-dessus; ((ii), (iii) et (iv) désignant collectivement les Données Personnelles) ;

sous réserve, toutefois, que les Parties conviennent que tous les documents ou informations utilisés dans le cadre ou découlant des activités que le Prestataire est autorisé à exercer conformément à la section applicable du Contrat Principal sont réputés ne pas constituer des « Données Personnelles », même si lesdits documents ou informations utilisés dans le cadre desdites activités pourraient constituer ou inclure des « Données Personnelles » dans d'autres contextes).

3.6.2 **Limitation d'accès.** Le Prestataire doit veiller à ce que l'accès aux Données Personnelles du Client soit limité aux membres du personnel qui ont besoin d'un tel accès pour permettre l'exécution du Contrat Principal et que ceux-ci soient soumis à l'obligation de préserver la confidentialité des Données Personnelles.

3.6.3 **Supervision et Sensibilisation.** Le Prestataire s'engage à exercer un contrôle suffisant et approprié sur ses employés, entrepreneurs, consultants, agents, fournisseurs et partenaires pertinents afin de garantir un niveau de confidentialité et de sécurité approprié pour les Données Personnelles. Le Prestataire proposera une formation, le cas échéant, portant sur les exigences de confidentialité et de sécurité de l'information énoncées dans ce DPA, pour les employées, entrepreneurs, consultants, agents, fournisseurs et partenaires ayant accès aux Données Personnelles.

3.6.4 **Délégué à la Protection des Données.** Le Prestataire désignera un Délégué à la Protection des Données lorsque cette nomination est requise par les Lois Applicables en matière de Protection des Données. Le délégué peut être contacté à: dpo@launchmetrics.com.

3.7. **Restitution et Suppression des Données Clients.** Rapidement après l'expiration ou la résiliation anticipée du Contrat, ou à tout moment antérieur spécifié par le Client, le Prestataire doit, dans le respect de la volonté du Client, restituer de manière sécurisée au Client ou à toute personne qu'il aura désignée, ou détruire de manière sécurisée ou rendre illisible ou indéchiffrable si la restitution au Client n'est pas raisonnablement possible ou souhaitable (une telle décision ne peut être fondée que sur une déclaration écrite du Client), tous les originaux et copies, sur tous supports, de toutes les Données Personnelles dont le Prestataire a la possession, la garde ou le contrôle, sauf si les Lois Applicables en matière de Protection des Données exigent le stockage des Données Personnelles.

3.8. **Mécanismes de transfert.** Le Prestataire s'interdit de transférer des Données Personnelles en dehors de l'EEE, **sauf** autorisation écrite préalable du Client et sous réserve des conditions suivantes :

- Le Client ou le Prestataire a apporté les garanties appropriées concernant le transfert des Données Personnelles conformément à l'Article 46 du RGPD ;
- Le Sujet des Données dispose de droits opposables et de voies de droit effectives ;
- Le Prestataire respecte ses obligations en vertu des Lois Applicables en matière de Protection des Données en assurant un niveau de protection adéquat pour toutes les Données Personnelles faisant l'objet d'un transfert ; et
- Le Prestataire respecte les instructions raisonnables qui lui ont été préalablement communiquées par le Client en ce qui concerne le Traitement des Données Personnelles.

IV. SOUS-TRAITANTS

4.1. **Sélection des Sous-traitants.** Le Client accepte que le Prestataire sous-traite ses obligations en vertu du présent Contrat à des entreprises affiliées ou des sous-traitants tiers afin d'exécuter et remplir les engagements et les obligations du Prestataire en vertu du Contrat Principal. Le Prestataire confirme avoir conclu ou (le cas échéant) qu'il conclura avec (chaque) sous-traitant tiers un contrat écrit intégrant des conditions substantiellement semblables à celles énoncées dans ce DPA, à l'image de celles qui ont été conclues entre le Client et le Prestataire, et que (chaque) sous-traitant tiers a donné des garanties suffisantes qu'il mettra en oeuvre des mesures pour s'assurer que le Traitement des Données Personnelles est conforme aux exigences du RGPD et protégera les droits des personnes concernées.

4.2. **Liste des Sous-traitants.** Le cas échéant, le Prestataire doit tenir une liste à jour des sous-traitants, en précisant (i) leur nom et leurs coordonnées, ainsi que (ii) la nature des tâches qui leur sont confiées, et (iii) l'emplacement du Traitement.

4.3. **Nouveaux Sous-traitants.** Le Prestataire avise le Client par écrit avant la désignation de tout nouveau Sous-traitant, y compris tous les détails du Traitement à effectuer par le Sous-traitant.

4.4. **Droit d'opposition.** Pour éviter tout doute, il sera raisonnable pour le Client de refuser ou de différer un tel consentement si le Client a des doutes raisonnables qu'un Sous-traitant est en mesure d'exécuter et de remplir les engagements et obligations du Prestataire au titre de ce DPA.
L'opposition doit être fondée sur des motifs raisonnables (par exemple, si le Client prouve qu'il existe des risques importants pour la protection de ses Données Personnelles chez le Sous-traitant).

4.5. **Sous-Traitants dans un pays tiers.** Le Client autorise le Prestataire à accepter au nom et pour le compte du Client un Sous-traitant qui Traite ou utilise les Données Personnelles du Client en dehors de l'EEE, à conclure des Clauses contractuelles types de l'UE pour le transfert de Données Personnelles vers des sous-traitants établis dans des pays tiers, datant du 5 février 2010 (« Clause Contractuelle type ») lorsqu'il n'existe pas de décision de niveau de protection adéquate concernant le pays dans lequel un Sous-traitant Traite ou utilise des Données Personnelles. Ceci s'applique dès la date de la présente autorisation en ce qui concerne la Clause contractuelle type déjà conclue par le Prestataire avec ses Sous-traitants.

4.6. **Responsabilité.** Le Prestataire reste pleinement responsable de tous les actes ou omissions de tout Sous-traitant tiers qu'il aura nommé conformément à cette section IV.

V. DROIT DES SUJETS DE DONNÉES

5.1. **Demande des sujets de données.** Dans les limites autorisées par la loi, le Prestataire informera le Client, dès que possible, par écrit, de toute demande concernant les Données Personnelles reçues de la part des contacts du Client, des consommateurs, des employés ou autres (« Sujet de Données »). Le Prestataire aidera le Client, au frais du Client, à répondre à toute demande d'un Sujet de Données et à respecter ses obligations en vertu des Lois Applicables en matière de Protection des Données, en matière de sécurité, de notification de violation, d'analyse d'impact et de consultation des autorités de surveillance ou des autorités de régulation. Le Prestataire coopérera avec le Client si un Sujet des Données cherche à exercer les droits suivants : accès, rectification, limitation du Traitement, effacement (« droit à l'oubli »), portabilité des données, opposition au Traitement ou ne pas faire l'objet d'une prise de décision individuelle automatisée.

VI. SÉCURITÉ

6.1. **Propriété des données.** Toutes les Données Personnelles doivent demeurer en tout temps la propriété exclusive du Client, et le Prestataire s'interdit d'avoir ou d'obtenir un quelconque droit à leur égard.

6.2. **Mesures de sécurité techniques et organisationnelles.** Le Prestataire s'engage à prendre toutes les Mesures de Sécurité Techniques et Organisationnelles nécessaires en vue de protéger les Données Personnelles fournies par le Client contre tout Traitement non autorisé ou illicite et contre toute perte, destruction ou endommagement accidentels, lesdites mesures devant être proportionnelles au préjudice pouvant résulter du Traitement non autorisé ou illicite ou de ladite perte, ladite destruction ou ledit endommagement accidentels et de la nature des données à protéger, tout en tenant compte du développement technologique et du coût de mise en œuvre de ces mesures le cas échéant, notamment des mesures de pseudonymisation et de chiffrage des Données Personnelles.

6.3. **Protection des Données.** Le Prestataire s'engage à élaborer, assurer et mettre en œuvre un programme de sécurité complet par écrit, intégrant toutes les garanties administratives, techniques, physiques, organisationnelles et opérationnelles appropriées et autres mesures de sécurité visant à (i) assurer la sécurité et la confidentialité des Données Personnelles, (ii) assurer une protection contre tout(e)s les menaces ou risques prévisibles touchant la sécurité et l'intégrité des Données Personnelles, et (iii) assurer une protection contre tout Incident de Sécurité. Le Prestataire surveille régulièrement le respect de ces mesures.

6.4. **Incident de sécurité et Gestion de la violation des Données Personnelles et notifications.** Le Prestataire s'engage à informer le Client par écrit, dans les meilleurs délais, de la violation de toute stipulation du présent DPA ou de tout vol effectif ou présumé, ou de tout(e) Traitement non autorisé, perte, utilisation, divulgation ou acquisition ou accès aux Données Personnelles (ci-après, les « Incidents de Sécurité Client ») dont le Prestataire prend connaissance et pouvant exiger qu'une notification soit faite à une autorité de surveillance ou à un Sujet des Données en vertu des Lois Applicables en matière de Protection des Données ou que le Prestataire soit tenu de notifier au Client en vertu des Lois Applicables en matière de Protection des Données. Le Prestataire doit fournir une coopération et une assistance raisonnables et dès que possible pour identifier la cause de cet Incident de Sécurité Client et prendre des mesures commercialement raisonnables pour remédier à la cause de l'Incident dans la mesure où la correction est sous le contrôle du Prestataire. Les obligations ci-incluses ne s'appliquent pas aux incidents causés par le Client, les utilisateurs autorisés, les produits non liés à Augure ou les cas de force majeure.

6.5. **Audits.** Le Prestataire doit tenir des dossiers et renseignements complets et exacts pour démontrer sa conformité avec ses obligations en vertu du présent Contrat et également à des fins d'audit réalisés par ou au nom du Client. Avant le début de tout audit, le champ d'application de l'audit, la durée et l'emploi du temps est précisé et convenu entre les deux parties par écrit et évalue le risque de non-conformité avec certains principes de protection des données. Le Client limitera son activité d'audit aux services et lieux convenus par écrit. Un calendrier de réunions et d'activités d'audit doit être établi par écrit et indiquer l'interlocuteur désigné pour l'audit ainsi que les zones d'activité à auditer. Le Client doit fournir au Prestataire un préavis de quinze (15) jours. Le Client peut réaliser un nouvel audit au cours des trois ans suivant le dernier audit. Le Client assume le coût et les dépenses de l'audit. Le Client s'engage à signer un accord de confidentialité avant chaque audit. L'équipe d'audit du Client est juridiquement liée par l'accord de confidentialité du Prestataire, qui interdit au Client de divulguer sciemment et sans observer aucune forme de prudence les informations confidentielles au sujet de l'audit. Le Client doit aviser promptement le Prestataire de toute information concernant toute non-conformité découverte au cours d'un audit, et le Prestataire doit déployer des efforts commercialement raisonnables pour remédier à toute non-conformité confirmée.

6.6. **Accès judiciaire.** Sous réserve du droit applicable, le Prestataire est tenu d'informer le Client par écrit dès que possible de toute citation à comparaître ou de toute autre ordonnance judiciaire ou administrative émanant d'une autorité gouvernementale ou dans le cadre d'une procédure visant à obtenir l'accès ou la divulgation de Données Personnelles. Le Client a le droit de se défendre à la place et au nom du Prestataire. Le Client peut, s'il le désire, demander une ordonnance de protection. Le Prestataire s'engage, dans la mesure du raisonnable, à collaborer avec le Client dans le cadre de ladite défense.

VII. MODIFICATION(S) DU DPA

Le présent Accord sur le Traitement des Données pourra être modifié en fonction des évolutions légales et réglementaires, notamment celles de la Loi sur la Protection des Données Personnelles, et du RGDP tels qu'ils existent à ce jour et tels qu'ils pourraient être modifiés et, à toute autre règle, loi, recommandation, règlement de l'autorité française de protection des données ou de toute autorité de contrôle européenne compétente.

ANNEXE 1

Détail du Traitement

Le Traitement des données par le Prestataire en vertu du présent Contrat est réalisé comme suit :

Portée des opérations de Traitement :

Le Prestataire s'engage à assurer le Traitement des Données Personnelles dans toute la mesure nécessaire à la réalisation des Services conformément au Contrat. Pour plus d'informations concernant le Traitement de ces données dans le cadre d'un Service particulier, veuillez-vous reporter à la Politique de Confidentialité en ligne, propre au Service en question. La base légale du traitement correspond à l'exécution du contrat du Prestataire.

Dans le cadre de l'utilisation des Services, le Prestataire peut être amené à utiliser des Données concernant les Utilisateurs de ses Services.

Nature et Objet du Traitement :

Le Prestataire s'engage à Traiter les Données Personnelles uniquement dans le but de réaliser les Services conformément au Contrat, et conformément aux instructions du Client dans le cadre de son utilisation des Services.

Durée du Traitement :

Le Prestataire s'engage à Traiter les Données Personnelles pendant toute la durée du Contrat, sauf s'il en a été convenu autrement par écrit ou légalement requis.

Types de Données Personnelles Traitées :

Le Client peut transmettre des Données Personnelles aux Services, dans la mesure qui aura été déterminée et contrôlée par le Client à son entière discrétion, lesquelles peuvent inclure, sans toutefois s'y limiter, des Données Personnelles concernant les catégories de personnes suivantes :

Nom, prénom et civilité de l'utilisateur	Nom, prénom et civilité influenceurs/journalistes
Fonction de l'utilisateur	Données relatives à la vie professionnelle influenceurs/jo
Email et téléphone de l'utilisateur	Données contact professionnel influenceurs/journalistes
Données de connexion utilisateur	Données relatives à la vie privée (DDN)
Historique d'utilisation	Données de réseaux sociaux influenceurs/journalistes

Catégories des Personnes concernées :

Le Client peut transmettre des Données Personnelles aux Services, dans la mesure qui aura été déterminée et contrôlée par le Client à son entière discrétion, qui peuvent inclure, sans toutefois s'y limiter, des Données Personnelles concernant les catégories de personnes suivantes :

Client lui même

Employeur ou relations commerciales du Client

Individus ou organisations en relation avec le Client

Droits des Personnes concernées :

Une personne concernée a le droit de:

- accéder aux Données;
- s'opposer au traitement;
- demander la rectification, effacement, restriction du traitement des Données;
- demander le transfert de ses Données (portabilité des données);
- ainsi que retirer son consentement ou envoyer une plainte à l'autorité de surveillance

Comment exercer ses droits :

Le Client et les personnes concernées peuvent exercer leurs droits à tous moments en envoyant un email à l'une des adresses suivantes: support@launchmetrics.com ou dpo@launchmetrics.com.

ANNEXE 2

Mesures de sécurité techniques et organisationnelles

1. Niveau d'application.

1.1. Audits de sécurité régulièrement programmés, en interne comme en externe.
1.2. Audits de sécurité externes et analyses de vulnérabilité réalisées par TrustWave. Les résultats de ces audits sont disponibles à la demande du Client.
1.3. Utilisation d'un Protocole SSL /TLS.
1.4. Normes cryptographiques rigoureuses, incluant des techniques avancées de hachage de mots de passe.
1.5. Politiques rigoureuses en matière de gestion des incidents, contrôle des changements et gestion des actifs.
1.6. L'accès aux applications est limité aux seules adresses IP sur liste blanche (à la demande du Client) : les clients peuvent choisir d'accéder à leurs données et à l'application uniquement à partir d'adresses IP qu'ils auront précisées au moment de l'installation.
1.7. Authentification par mot de passe pour tous les utilisateurs : seuls les Utilisateurs Autorisés ont accès à l'application. En outre, il existe différents niveaux d'autorisation. Par exemple, les utilisateurs non autorisés pour l'accès administrateur ne peuvent ajouter ou supprimer des utilisateurs.
1.8. Support pour différentes fonctions et autorisations pour chaque fonction. Les autorisations peuvent être configurées selon la fonction ou l'utilisateur. Seuls les fonctions ou les utilisateurs bénéficiant d'une autorisation d'accès à une ressource protégée peuvent le faire.
1.9. Toutes les activités de l'utilisateur sont enregistrées : en cas d'activité non autorisée, nous pouvons examiner le journal d'activité pour enquêter sur les faits et transmettre ledit journal au Client à sa demande.
1.10. Utilisation d'une authentification par mot de passe à usage unique pour les systèmes critiques. Les applications AWS, Gmail, Github, Lastpass sont toutes soumises à la deuxième couche de sécurité du système OTP où l'utilisateur doit saisir son identifiant et son mot de passe ainsi que le code apparaissant sur l'application d'authentification.

2. Plan de rétablissement.

2.1. Sauvegarde complète des données toutes les 24 heures.
2.2. Tous les serveurs sont sécurisés et utilisent des équilibreurs de charge. Le Prestataire est en mesure de détecter le trafic et réaliser la maintenance au sein des serveurs sans affecter le service du Client.
2.3. Les sauvegardes sont conservées localement et à distance sur S3.
2.4. Rétention des données à trente (30) jours.
2.5. En cas de perte totale du centre de données ou des données, le Client peut être redirigé vers un centre de données secondaire avec la sauvegarde de données la plus récente en moins de 4 heures.

3. Hébergement.

3.1. Les serveurs sont hébergés dans plusieurs centres de données de pointe certifiés SSAE et ISO 27001.
3.2. Les équipements bénéficient de plusieurs niveaux de sécurité physique et sont supportés par une alimentation redondante et un accès Internet HSRP/VRRP. Le Datacenter Prosodie est situé dans des bâtiments placés sous haute surveillance, où le personnel de sécurité assure un contrôle 24 h/24 h, 7 j/7. D'autres mesures de sécurité sont en place telles que des serrures biométriques munies de lecteurs d'empreintes digitales, des caméras de surveillance et des détecteurs de mouvements placés à des endroits stratégiques, ainsi que des systèmes d'alarme sur les portes.
3.3. L'accès à distance au réseau de Launchmetrics au sein d'AWS et du Datacenter Prosodie est autorisé uniquement aux employés autorisés par une connexion VPN sécurisée.

4. Réseau de bureau.

4.1. Le réseau de bureau est protégé par un pare-feu Cisco. Seul un accès autorisé est permis.
4.2. Les documents sont partagés uniquement entre les employés autorisés. Les documents se trouvant sur le réseau de bureau ne sont pas publics et peuvent être consultés uniquement par les employés ou consultants autorisés.
4.3. L'accès au bâtiment n'est pas donné tant que le visiteur n'a pas reçu une pré-autorisation ou qu'un employé en service lui en autorise l'accès.

5. Mises à jour. Le Prestataire s'efforce constamment d'améliorer ses Services et ses plateformes. Les dernières mises à jour touchant les Mesures de Sécurité Techniques et Organisationnelles du Prestataire sont disponibles à la demande. Le Client peut contacter le Prestataire via cette adresse e-mail support@launchmetrics.com et lui demander le document suivant : Launchmetrics - Security Policy and Practices.docx.

ANNEXE 3

Liste des prestataires ou partenaires tiers (Sous-traitants)

Prestataire Infrastructure – Stockage des données de Services :

Nom de l'entité	Type d'entité	Pays
Amazon Web Services, Inc.	Fournisseur de service cloud et d'hébergement	États-Unis
Amazon Data Services Ireland Ltd	Fournisseur de service cloud et d'hébergement	Irlande

(sur demande seulement, à noter que le Service: Discover est intégralement hébergé sur AWS Irelande)

Sous-traitants du Groupe Launchmetrics :

Nom de l'entité	Pays
Fashion GPS, Inc. dba Launchmetrics	États-Unis
Fashion GPS Europe Ltd	Royaume-Uni
Fashion GPS France	France
Fashion GPS HK	Hong Kong
Augure SA	France
Augure UK Ltd.	Royaume-Uni
Augure US Inc.	États-Unis
Augure Spain	Espagne Italie
Visual Box SRL	Roumanie
Launchmetrics Technologies SRL	États-Unis
Style Coalition	Allemagne
Launchmetrics Germany GmbH	

Prestataires spécifiques aux Services :

A compléter si applicable