ACCORD SUR LA PROTECTION DES DONNEES

ETANT PREALABLEMENT RAPPELE QUE

NEW OXATIS propose une solution technique permettant au Client de créer et de gérer son site Internet de e-commerce.

Le présent Accord, établi en application de l'article 28 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, a pour objet de définir les conditions dans lesquelles NEW OXATIS s'engage, en sa qualité de sous-traitant, à effectuer pour le compte du Client, Responsable de traitement, les opérations de traitement de données à caractère personnel définies ci-après pour lesquels le Client définit seul les moyens et les finalités et en a seul l'initiative.

Dans le cadre de leurs relations contractuelles, les Parties s'engagent à respecter la réglementation en vigueur applicable au Traitement de Données personnelles et, en particulier, le règlement (UE) 2016/679 précité applicable depuis le 25 mai 2018 (ci-après, « le règlement européen sur la protection des Données »), la loi « Informatique et libertés » n°78-17 du 6 janvier 1978 modifiée et les réglementations en matière de propriété industrielle et intellectuelle.

LES PARTIES ONT CONVENU CE QUI SUIT

1. DEFINITIONS

Pour les besoins des présentes, les termes suivants auront le sens qui est donné ci-dessous :

- « **Contrat** » : désigne le document aux termes duquel le Client missionne NEW OXATIS pour exécuter les Services.
- « **Autorité de régulation** » : Désigne toute autorité compétente en matière de protection des Données Personnelles.
- « **Destinataire autorisé** » : Désigne un administrateur, un employé ou un Sous-traitant Ultérieur qui a un besoin légitime d'accéder aux Données Personnelles dans le cadre de l'exécution du contrat de Services.
- « **Données** » : désigne tous types d'informations et/ou données auxquelles les Parties ont accès dans le cadre des relations contractuelles, quel que soit le format ou le support, que ce soit des Données personnelles (définies ci-après) ou non (ex : données financières, opérateurs, clients, partenaires, stratégiques, techniques, professionnelles, administratives, commerciales, juridiques, comptables ...).
- « **Données Personnelles** » : désigne toute information relative à une personne physique identifiée ou qui peut être identifiée comme telle, soit directement soit indirectement par regroupement d'informations, par référence à un numéro d'identification ou à des éléments qui lui sont propres : nom, adresse, numéro de téléphone, adresse IP, adresse email, numéro d'immatriculation d'un véhicule, matricule professionnel, identifiant/login, mot de passe, données de connexion, etc.
- « **Données sensibles** » : désigne les catégories particulières de Données personnelles dont le Traitement est par principe interdit. Il s'agit des Données personnelles qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le Traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
- « **Finalité autorisée** » : Désigne l'objet du Traitement de Données personnelles mis en œuvre par NEW OXATIS, conformément à l'Appendice 1.
- « **Instructions** » : Désigne l'ensemble des instructions écrites par le Responsable de Traitement à destination de NEW OXATIS. Ces instructions peuvent prendre la forme d'un Accord sur la protection des données ou d'échanges écrits, y compris par voie électronique.
- « **NEW OXATIS** » : désigne la société NEW OXATIS, société par actions simplifiée à associé unique, immatriculée au Registre du commerce et des sociétés

de Marseille sous le numéro 831 239 744, sise au 4 boulevard J. Saade – Quai d'Arenc, 13002 Marseille. En vertu des présentes, NEW OXATIS agit en qualité de Sous-Traitant.

- « **Loi sur la Protection des Données** » : Désigne la réglementation en vigueur applicable au Traitement de Données Personnelles et, en particulier :
  (i) le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable depuis le 25 mai 2018 dit « Règlement Général sur la Protection des Données »;
  (ii) la loi « Informatique et libertés » n°78-17 du 6 janvier 1978 modifiée ;
  (iii) toute législation entrant en vigueur et susceptible d'affecter les Traitements visés par le présent Accord ;
  (iv) tout guide de bonnes pratiques publié par les Autorités de régulation ou le Comité Européen sur la Protection des Données.

- « **Parties** » : au singulier désigne NEW OXATIS ou le Client. Au pluriel désigne chacune des deux Parties.

- « **Pays tiers** » : Tout pays non-membre de l'Espace Economique Européen.

- « **Personne concernée** » : Désigne toute personne physique dont les Données personnelles font l'objet d'un Traitement.

- « **Responsable de Traitement** » ou « **Client** » : désigne la personne qui détermine les moyens et les finalités du Traitement.

- « **Services** » : Désigne les prestations de services assurées par NEW OXATIS dans le cadre du Contrat.

- « **Sous-traitant** » : désigne NEW OXATIS qui traite les Données personnelles pour le compte du Responsable du Traitement et sur instruction de celui-ci.

- « **Sous-traitant Ultérieur** » : désigne le sous-traitant de NEW OXATIS qui effectue des Traitements de Données personnelles en suivant strictement les Instructions délivrées par le Responsable de Traitement.

- « **Traitement** » : Désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

- « **Violation de données à caractère personnel** » : désigne une faille de sécurité qui entraîne accidentellement ou illicitement l'accès à ou la destruction, la perte, l'altération, la divulgation non autorisée de Données Personnelles transmises, stockées ou traitées.

2. DUREE

2.1. Le présent Accord entre en vigueur à compter de sa signature et reste applicable durant toute la durée du Contrat.

2.2. Le présent Accord se substitue à toute clause applicable en matière de protection des Données personnelles pouvant se trouver dans le Contrat. En cas de contradiction, les Parties conviennent expressément que le présent Accord prévaudra sur le Contrat.

3. NOMINATION ET ROLE DE NEW OXATIS

Le Client désigne NEW OXATIS pour traiter les Données personnelles en son nom et pour son compte en vue d'atteindre les Finalités autorisées visées à l'Appendice 1 du présent Accord.

4. OBLIGATIONS GENERALES DES PARTIES

4.1. En sa qualité de Sous-Traitant, NEW OXATIS s'engage à :

- Respecter la Loi sur la Protection des Données ;
- Traiter les Données personnelles conformément aux Finalités Autorisées et aux Instructions. En particulier, NEW OXATIS s'interdit de traiter les Données personnelles pour des finalités autres que

les Finalités Autorisés ou en dehors des Instructions du Responsable de Traitement ;
- Coopérer et se conformer aux instructions ou aux décisions de toute Autorité de régulation dans le cadre du Traitement ;
- Sensibiliser son personnel sur les problématiques relatives à la protection des Données personnelles ;
- Ne pas faire ou omettre de faire ou permettre que quelque chose soit fait qui amènerait le Client à enfreindre la Loi sur la protection des données.

4.2. Le Client, en sa qualité de Responsable du Traitement, s'engage à :
- Respecter la Loi sur la Protection des Données ;
- Documenter par écrit toute Instruction concernant le Traitement décrit en Appendice 1 des présentes ;
- Veiller, au préalable et pendant toute la durée du Traitement, au respect des obligations prévues par la Loi sur la Protection des Données ;
- Respecter l'ensemble des obligations dont il est tenu en sa qualité de Responsable du Traitement en vertu de la Loi sur la Protection des Données relatives notamment à l'information des Personnes Concernées.

5. COOPERATION ET ASSISTANCE

5.1. NEW OXATIS s'engage à :

5.1.1. Désigner un interlocuteur privilégié chargé de le représenter auprès du Responsable de Traitement ;

5.1.2. Adhérer et participer activement à une logique de coopération afin de s'assurer du respect de la Loi sur la protection des Données personnelles et des Instructions. En particulier, NEW OXATIS fournira au Client une pleine coopération, des informations et une assistance en cas de plainte, de demande d'avis, de communication, ou de faille réelle ou présumée de sécurité affectant des Données personnelles. NEW OXATIS s'engage en outre à ne faire aucune déclaration ou annonce publique à un tiers, y compris à une Autorité de régulation, sans avoir, au préalable, consulter le Client concernant le contenu d'une telle déclaration ou annonce publique ;

5.1.3. Modifier, transférer et / ou supprimer les Données personnelles détenues par lui ou en son nom par un Sous-traitant Ultérieur, conformément à toute Instruction écrite du Client;

5.1.4. Informer le Client dans les meilleurs délais :

(i) Si NEW OXATIS considère qu'une instruction constitue une violation de la Loi sur la Protection des Données ;

(ii) En cas de survenance d'une Violation de Données personnelle, ou en cas de survenance d'une faille de sécurité affectant le système informatique de NEW OXATIS ou de l'un de ses Sous-traitants Ultérieurs, et ce dans les conditions prévues à l'article 6.2 du présent Accord ;

(iii) Si NEW OXATIS ou un Sous-traitant Ultérieur reçoit une plainte, un avis ou une communication d'une Autorité de régulation qui concerne directement ou indirectement le Traitement ou la conformité de l'une ou l'autre Partie à la Loi sur la protection des données et,

(iv) Si NEW OXATIS ou un Sous-traitant Ultérieur reçoit une plainte, un avis ou une communication d'une Personne concernée dans le cadre de l'exercice de ses droits, ou d'une Autorité de régulation qui concerne directement ou indirectement le Traitement ou la conformité de l'une des Parties sur les opérations de Traitement.

5.1.5. NEW OXATIS s'engage à aider le Client à respecter les obligations énoncées aux articles 32 à 36 du Règlement Général sur la Protection des Données en tenant compte de la nature du Traitement et des informations mises à la disposition de NEW OXATIS. Cette assistance peut inclure la fourniture d'informations et la réalisation d'analyses d'impact en relation avec les opérations de Traitement mis en œuvre par NEW OXATIS. Il est ici précisé que dans le cadre de cet accompagnement, certaines mesures demandées par le Client pourront faire l'objet d'une facturation complémentaire proportionnelle au temps passé par les équipes de NEW OXATIS dans la prise en charge de la demande du Client.

6. SECURITE

6.1. NEW OXATIS s'engage auprès du Client à mettre œuvre des mesures techniques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte, la modification, la divulgation non autorisée ou l'accès aux Données Personnelles détenues ou traitées par lui, y compris toutes les mesures nécessaires pour assurer la conformité avec les exigences de sécurité des données dans la Loi sur la protection des données. En particulier, NEW OXATIS s'engage à se conformer à toute demande raisonnable du Client en ce qui

concerne la sécurité du Traitement de données à caractère personnel.

6.2. En cas de survenance d'une Violation de Données personnelles, réelle ou potentielle, affectant les Services de NEW OXATIS ou d'un Sous-traitant Ultérieur, NEW OXATIS s'engage à :

6.2.1. Notifier au Client toute Violation de Données dans les meilleurs délais après en avoir pris connaissance par message électronique ou par courrier avec accusé de réception ;

6.2.2. Dans la mesure du possible et au regard des informations portées à sa connaissance, accompagner la notification de toute documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente ou à la Personne concernée ;

A ce titre, NEW OXATIS indiquera les points suivants :

(i) La description de la nature de la Violation de Données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de Personnes Concernées par la Violation et les catégories et le nombre approximatif d'enregistrements de Données Personnelles concernés ;

(ii) Le cas échéant, le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

(iii) Dans la mesure du possible, la description des conséquences probables de la Violation de Données à caractère personnel ; et

(iv) La description des mesures prises ou que NEW OXATIS propose de prendre pour remédier à la Violation de Données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

6.2.3. Dans le cas où il n'est pas possible de fournir toutes les informations précisées à l'article 6.2.2 en même temps, les communiquer de manière échelonnée et dans les meilleurs délais.

6.3. Le présent article s'entend sans préjudice des obligations propres du Responsable du Traitement en matière de sécurisation des Données Personnelles.

7. ACCOUNTABILITY

NEW OXATIS s'engage à :

- Tenir régulièrement à jour le registre des activités de traitements tel que prévu à l'article 30 du Règlement Général sur la Protection des Données, et conserver une trace écrite de tout Traitement et Instruction relative aux Traitements effectués pour le compte du Client ;
- Tenir régulièrement à jour le registre des failles de sécurité qui devra être complété dès la survenance d'une Violation de Données personnelles, que cette violation ait, ou non, fait l'objet d'une notification auprès des services de l'Autorité de régulation ;
- Conserver la documentation relative à la formation ou à la sensibilisation de leurs salariés à la protection des Données personnelles ; et
- Documenter, dans la mesure du possible, l'ensemble des procédés mis en place en matière de protection des Données personnelles au travers de leur Politique de sécurité.

8. DESTINATAIRES AUTORISES

8.1 Dans le cadre du Traitement figurant en Appendice 1, NEW OXATIS est expressément autorisée à désigner un ou plusieurs Sous-Traitants Ultérieurs pour les Données Personnelles :

- Après avoir préalablement informé le Client de l'identité du Sous-traitant ultérieur d'une part et des activités de Traitement qui seront entreprises par lui d'autre part. En cas d'ajout ou de remplacement d'un Sous-traitant ultérieur, NEW OXATIS en informera le Client qui dispose d'un délai de dix (10) jours à compter de la date de réception de cette information pour présenter ses objections. A défaut d'objection du Client dans ce délai, la sous-traitance sera considérée comme validée par le Client ;
- A condition qu'un contrat de sous-traitance ultérieure soit conclu avec le Sous-traitant avant qu'il ne transfère ou n'accède à des Données personnelles et que ledit contrat contienne des obligations contraignantes en matière de respect de la Loi sur la Protection des Données ; et
- A condition que NEW OXATIS veille à ce que le Sous-traitant respecte les obligations en matière de confidentialité, énoncées dans le contrat de sous-traitance ultérieure.

8.2 Toute sous-traitance ultérieure des Traitements réalisés par NEW OXATIS en sa qualité de Sous-traitant ne libère pas NEW OXATIS de ses responsabilités et obligations envers le Client en vertu du présent Accord.

9. PERSONNES CONCERNEES

9.1 Dans le cadre de la mise en œuvre des Services, le Client, en qualité de Responsable du Traitement, s'engage à informer préalablement les Personnes Concernées de la mise en place des opérations de Traitement, et le cas échéant obtenir le consentement des personnes concernées pour le déploiement des Services.

9.2 Dans le cas où NEW OXATIS recevrait une demande d'une Personne Concernée souhaitant exercer ses droits en vertu de la Loi sur la protection des données dans le cadre du Traitement figurant en Appendice 1 :

- NEW OXATIS en avisera le Client dans les meilleurs délais et au plus tard dans un délai de trois (3) jours ouvrables.
- NEW OXATIS n'agira que sur instruction écrite du Client ;
- NEW OXATIS ne divulguera pas à la Personne concernée de Données ou de Données Personnelles sans avoir préalablement consulté et obtenu le consentement écrit du Client ;
- Toute opération réalisée par NEW OXATIS dans le cadre d'une demande d'exercice de droit pourra, le cas échéant, donner lieu à une facturation complémentaire compte tenu des investigations techniques réalisées à la demande du Client.

10. TRANSFERTS VERS LES PAYS TIERS

10.1. NEW OXATIS s'engage à :

- N'effectuer aucun transfert de Données Personnelles à des Pays tiers sans le consentement préalable et écrit du Client.
- Se conformer aux Instructions délivrées par le Client concernant les transferts de Données vers des Pays tiers, sauf dans l'hypothèse où NEW OXATIS serait tenue, conformément aux lois applicables, de transférer des Données personnelles vers un Pays tiers. Dans ce cas précis, NEW OXATIS en informera le Client par écrit avant qu'un tel transfert n'ait lieu, à moins que la loi applicable n'interdise une telle notification.

10.2. Le Client consent par les présentes au transfert de Données personnelles aux entités et aux emplacements mentionnées en Appendice 1, aux fins de la stricte exécution des Services par NEW OXATIS en sa qualité de Sous-traitant, et à condition que :

- Le Pays tiers soit un pays qui, selon la Commission européenne, justifie d'un niveau adéquat de protection des Données Personnelles ; ou
- NEW OXATIS satisfait à l'une des conditions suivantes :
    - NEW OXATIS conclut ou obtient de l'entité identifiée en Appendice 1 un accord sur le transfert de données reprenant les modèles de Clauses Contractuelles Types élaborés par la Commission européenne ;
    - Les transferts effectués avec l'entité visée en Appendice 1 s'inscrivent dans le régime d'exception visé à l'article 49 du Règlement Général sur la Protection des Données.

10.2. En sa qualité de Sous-traitant, NEW OXATIS veille à ce qu'aucun transfert ultérieur de Données personnelles vers un autre Pays tiers n'ait lieu à moins que le Client n'accorde son consentement préalablement à ce transfert, ou que ce transfert ultérieur réponde aux exigences posées par l'article 10.1 des présentes.

11. EXIGENCES SUPPLEMENTAIRES

Durant la relation contractuelle, le Client peut identifier des exigences supplémentaires, autres que celles identifiées dans le présent Accord, afin de se conformer à ses obligations en vertu de la Loi sur la protection des données. Lorsque le Client identifie des exigences supplémentaires, les Parties collaborent de bonne foi pour convenir des modifications à cet Accord afin de permettre la conformité des Traitements avec lesdites exigences supplémentaires.

12. PROPRIETE DES DONNEES

Dans le cadre des activités de Traitement, il est expressément convenu que l'ensemble des Données personnelles mis à dispositions par le Client dans le cadre du Traitement demeure la seule propriété pleine et entière du Client.

13. RESPONSABILITE

13.1. Chaque Partie est responsable de tous les dommages directs subis par l'autre et découlant de la violation par elle, ses employés, ses représentants, ses agents et, le cas échéant, ses Sous-traitants ultérieurs (y compris les Destinataires autorisés) de ses obligations en vertu du présent Accord.

13.2 Chaque Partie s'engage à mettre en œuvre tous les moyens nécessaires et raisonnables pour assurer la sécurité des Traitements, et sera dès lors responsable des dommages liés à une défaillance de sécurité qui lui serait imputable entrainant une indisponibilité, une perte de traçabilité, un doute sur l'intégrité ou un défaut de confidentialité des Données personnelles. Il est néanmoins expressément convenu entre les Parties que le risque zéro en matière de sécurité informatique n'existe pas.

13.3. La responsabilité des Parties à l'égard des coûts, des dépenses, des pertes, des dommages ou d'autres responsabilités découlant de ou en relation avec la violation du présent Accord (que ce soit par la Partie ou ses employés, représentants, agents ou Sous-traitants, les Destinataires autorisés) ne pourra être engagée que dans un délai d'un (1) an à compter de la connaissance du dommage.

14. RESILIATION

A l'expiration du Contrat pour quelque motif que ce soit, NEW OXATIS s'engage, selon le choix du Client, à détruire les Données personnelles utilisées dans le cadre des opérations de Traitement pour lesquelles elle agit en sa qualité de Sous-traitant ou à les restituer au Client et à ne conserver les copies existantes qu'en bases archivées à des fins probatoires pour les délais de prescription légale applicables, à moins que le droit de l'Union Européenne ou le droit français n'exige la conservation de certaines Données personnelles.

15. INFORMATION ET AUDIT

15.1. NEW OXATIS s'engage, à ses frais, à fournir sur demande et sans délai, les informations que le Client peut raisonnablement demander pour confirmer que NEW OXATIS agit conformément à la Loi sur la protection des données ;

15.2. Le Client peut commander la réalisation d'audits sur pièce afin de s'assurer du bon niveau de conformité des Traitements réalisés par NEW OXATIS en sa qualité de Sous-Traitant. Ne sont pas concernées par l'audit sur pièces les éléments confidentiels confiés à NEW OXATIS par d'autres clients.

15.3. Le Client peut commander la réalisation d'audits objectifs de conformité à la Loi sur la protection des données sur les opérations de Traitement réalisées par NEW OXATIS en sa qualité de Sous-traitant aux fins de l'exécution des Services dans les conditions définies ci-après :

- L'audit est diligenté par un auditeur extérieur sélectionné ensemble par les Parties pour son expertise, son indépendance et son impartialité et qui n'est, en tout état de cause, pas un concurrent de NEW OXATIS ;
- L'auditeur sélectionné est lié au Parties par un accord de confidentialité et/ou par le secret professionnel ;
- Le Client avise, par écrit et moyennant le respect d'un préavis minimum de trente (30) jours ouvrés, NW OXATIS de son intention de faire procéder à un audit de conformité ;
- En aucune manière, l'audit réalisé ne saurait détériorer ou ralentir les Services proposés par NEW OXATIS ou porter atteinte à la gestion organisationnelle de NEW OXATIS ;
- Un exemplaire du rapport d'audit identique est remis au Client ainsi qu'à NEW OXATIS des suites de la réalisation de la mission d'audit et pour lequel des observations pourront être apportées par les Parties. Ce rapport pourra, le cas échéant, faire l'objet d'un examen approfondi dans le cadre d'un comité de pilotage ;
- Les frais de l'audit de conformité seront portés à la charge exclusive du Client ;
- Le Client ne saurait commander des audits de conformité que dans la limite de un (1) audit par an ; et
- NEW OXATIS disposera d'un délai de trois (3) mois à compter de la communication du rapport d'audit pour corriger à ses frais les manquements et/ou non-conformités constatés. Le cas échéant, NEW OXATIS pourra de façon exceptionnelle allonger ce délai de trois (3) mois après avoir expressément informé le client et justifié objectivement un tel allongement.

15.4. NEW OXATIS s'engage à permettre l'accès des auditeurs sélectionnés à ces sites, installations, documents et informations

nécessaires en vue d'évaluer son bon niveau de conformité, et coopère pleinement avec eux en vue de la bonne réalisation de leur mission.

15.5. Dans l'hypothèse d'un contrôle réalisé par une Autorité de régulation compétente pouvant intéresser les Traitements du Client, NEW OXATIS s'engage à coopérer pleinement avec l'Autorité de régulation.

15.6. Dans l'hypothèse d'un contrôle réalisé par une Autorité de régulation compétente à l'égard du Client, NEW OXATIS s'engage à assister pleinement celui-ci concernant les Traitements réalisés.

15.7. L'ensemble des Données collectées au titre des Audits et Contrôles sont considérées comme des Données confidentielles protégées par le secret des affaires.

16. MODIFICATION DE L'ACCORD

16.1. Cet Accord ne peut être modifié, sauf par écrit signé par les représentants dûment autorisés de chacune des Parties.

16.2. En cas de modification de la Loi sur la protection des données, il est convenu que les Parties pourront réviser les dispositions du présent Accord et négocier de bonne foi pour se conformer à la Loi sur la protection des données mise à jour.

17. DROIT APPLICABLE ET JURIDICTION

17.1. LE PRESENT ACCORD SERA REGI ET INTERPRETE CONFORMEMENT A LA LOI FRANÇAISE ET TOUT LITIGE DECOULANT DE OU EN RELATION AVEC LE PRESENT ACCORD SERA SOUMIS A LA JURIDICTION EXCLUSIVE DES TRIBUNAUX FRANÇAIS, AUXQUELLES CHACUNE DES PARTIES SE SOUMET IRREVOCABLEMENT.

17.2. AVANT TOUTE ACTION CONTENTIEUSE, LES PARTIES CHERCHERONT, DE BONNE FOI, A REGLER A L'AMIABLE LEURS DIFFERENDS RELATIFS A LA VALIDITE, L'INTERPRETATION, L'EXECUTION OU L'INEXECUTION, L'INTERRUPTION, LA RESILIATION OU LA DENONCIATION DU PRESENT CONTRAT AINSI QU'A LA CESSATION PARTIELLE OU TOTALE DES RELATIONS COMMERCIALES ENTRE LES PARTIES ET CE, POUR QUELQUES CAUSES ET SUR QUELQUES FONDEMENTS QUE CE SOIENT. LES PARTIES DEVRONT SE REUNIR AFIN DE CONFRONTER LEURS POINTS DE VUE ET EFFECTUER TOUTES CONSTATATIONS UTILES POUR LEUR PERMETTRE DE TROUVER UNE SOLUTION AU CONFLIT QUI LES OPPOSE.

17.3. LES PARTIES S'EFFORCERONT DE TROUVER UN ACCORD AMIABLE DANS UN DELAI DE 30 JOURS A COMPTER DE LA NOTIFICATION PAR L'UNE D'ELLE DE LA NECESSITE D'UN ACCORD AMIABLE, PAR LETTRE RECOMMANDEE AVEC AVIS DE RECEPTION.

17.4. CEPENDANT IL EST PRECISE QUE LES STIPULATIONS DES PARAGRAPHES CI-DESSUS NE S'APPLIQUERONT PAS EN CAS DE PROBLEME DE QUALITE, DE SECURITE OU DE CONFORMITE, OU D'ATTEINTE AUX DROITS DE TIERS, NOTAMMENT DE PROPRIETE INTELLECTUELLE (NOTAMMENT ACTION EN CONTREFAÇON, CONCURRENCE DELOYALE ET/OU AGISSEMENTS PARASITAIRES) EN RELATION AVEC LES ELEMENTS OBJETS DE LA PRESENTE CONVENTION.

APPENDICE 1 :
INSTRUCTIONS RELATIVES AU TRAITEMENT

NEW OXATIS, en sa qualité de Sous-Traitant, est autorisée à traiter pour le compte du Client les Données à Caractère Personnel nécessaires pour fournir les Services souscrits par le Client.

Pour l'exécution du ou des services objet du présent contrat, le Client met à la disposition de NEW OXATIS, en sa qualité de sous-traitant, les informations nécessaires suivantes :

A. Coordonnées du Délégué à la Protection des Données

Délégué à la protection des données de NEW OXATIS	DPO NEW OXATIS 4 boulevard J. Saade - Quai d'Arenc,13002 Marseille – France dataprotection@oxatis.com

B. Détail du Traitement

Catégories de Personnes concernées	• Les clients du Client (ci-après les « Acheteurs ») ; • Les collaborateurs du Client disposant d'un accès à la Solution (ci-après les « Utilisateurs »).
Catégories de données	• Données relatives à l'identité des Acheteurs et/ou des Utilisateurs (nom, prénom, adresse email, numéro de téléphone, adresse postale) ; • Données relatives à la facturation (produit acheté, date de l'achat, montant HT de la facture, montant TTC de la facture, adresse de facturation) ; • Données relatives à la satisfaction des Acheteurs (note attribuée au Client et/ou à ses produits ou services, commentaire rédigé par l'Acheteur) ; • Toute autre donnée à caractère personnel collectée par le Client et hébergée sur la Solution
Finalités Autorisées	Les Finalités Autorisées dépendent des fonctionnalités activées par le Client. Ainsi, selon les fonctionnalités sélectionnées le Client, NEW OXATIS est autorisée à traiter les données pour la : • Gestion et paramétrage des comptes d'Utilisateur ; • Gestion des comptes Acheteurs ; • Gestion des commandes ; • Gestion de la livraison ; • Gestion de la facturation ; • Gestion des opérations marketing (communication, promotions…) ; • Gestion des avis client ; • Gestion du service après-vente ; • Élaboration de statistiques.
Durée de conservation	Les Données Personnelles sont conservées par NEW OXATIS pendant toute la durée du Contrat. En tout état de cause, elles seront supprimées ou restituées au Client dans les conditions prévues par l'Accord.
Transferts Hors-UE	Les Données Personnelles sont stockées en France.
Mesures organisationnelles de sécurité	Les Données Personnelles traitées par NEW OXATIS sont protégées par des mesures de sécurité adaptées auxdites Données.

	1. Référentiel sécurité NEW OXATIS a mis en place un référentiel sécurité composé de : • Un plan d'assurance sécurité ; • Un plan de continuité d'activité ; • Un règlement intérieur ; • Une charte d'utilisation des systèmes d'information ; • Une charte télétravail ; • Une politique de gestion des incidents. **2. Administrateurs systèmes et équipe dédiée** NEW OXATIS a désigné quatre administrateurs système qui supervisent l'infrastructure de manière quotidienne. Une équipe d'astreinte prend en charge la supervision et la gestion des alertes en dehors des heures ouvrées et pendant les jours fériés. **3. Gestion des habilitations** NEW OXATIS a mis en place des mesures de gestion des habilitations. **4. Obligation de confidentialité** Les collaborateurs de NEW OXATIS sont soumis à une obligation contractuelle de confidentialité. **5. Sensibilisation** NEW OXATIS sensibilise ses collaborateurs aux enjeux spécifiques à la protection et à la sécurité des Données Personnelles. **6. Assurance** L'infrastructure de NEW OXATIS (hors stockage) est couverte par une assurance critique J+1. Les équipements de stockage sont couverts par une assurance critique 4 heures. **7. Procédures de test** NEW OXATIS réalise des tests d'intrusion et de recherche des vulnérabilités par l'intermédiaire d'une société qualifiée PASSI (Prestataires d'Audit de la Sécurité des Systèmes d'Information) par l'ANSSI. Ces tests sont conduits avant et après chaque évolution significative de l'infrastructure. New Oxatis met également en place des procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement.
Mesures de sécurité techniques	**1. Mesures d'authentification** La plateforme applique une politique de complexité stricte pour la création des mots de passe : • Longueur comprise entre 8 et 20 caractères alphanumériques (sans accents). • Au moins 1 lettre MAJUSCULE. • Au moins 1 lettre minuscule. • Au moins 1 chiffre. • Au moins 1 caractère spécial de la liste suivante : *$@&()[]{}=#.-!?+/£€% Le protocole de renouvellement de ces derniers est sécurisé par email, avec l'envoi d'un mail de confirmation contenant un lien de réinitialisation ayant une durée de validité d'une heure. Les mots de passes sont hashés via algorithme

Argon et stockés au format texte. Les webservices ne permettent pas d'accéder ni d'écrire les mots de passe.

En interne, l'accès aux données est protégé par des mots de passe forts comprenant entre 16 et 24 caractères dont, à minima, une majuscule, une minuscule, des chiffres et des caractères spéciaux.

Les administrateurs système utilisent un gestionnaire de mot de passe professionnel (LASTPASS Enterprise) afin de générer systématiquement des mots de passe forts et uniques.

Les administrateurs système sont tenus de modifier leur mot de passe toutes les 6 semaines, étant précisé que tout nouveau mot de passe doit être différent de l'intégralité des mots de passe précédemment utilisés.

2. Enregistrement des accès et gestion des incidents

NEW OXATIS soumet l'accès à distance à ses infrastructures à une connexion VPN.

Les accès à son infrastructure font l'objet d'une journalisation et d'une surveillance. Les logs sont conservés 24h sur le serveur Web original. Ils sont centralisés chaque heure depuis tous les serveurs Web sur un serveur de log et conservés pour une durée de 7 jours. Ils sont aussi intégrés à une solution d'analyse de log pour une durée de 15 jours.

3. Protection contre les attaques malveillantes

NEW OXATIS utilise CloudFare. La solution de protection anti-DDoS de Cloudflare sécurise les sites web, les applications et les réseaux entiers, tout en s'assurant que le trafic légitime n'est pas compromis. Doté d'une capacité de 51 Tbps, le réseau de Cloudflare bloque en moyenne 72 milliards de menaces par jour. Cloudflare est conforme aux normes ISO 27001:2013, PCI DSS 3.2.1, SOC 2 Type II.

NEW OXATIS utilise également une protection anti DDoS dédiée et délivrée par des équipements Arbor Networks (http://www.arbornetworks.com/). Arbor Networks est le leader des solutions anti DDoS et fournit des solutions de sécurité depuis plus de 10 ans à plus de 90% des Fournisseurs d'accès de niveau 1 (Tier 1 Service Providers).

NEW OXATIS utilise des équipements WAF (Web Application Firewall) Fortigate qui scannent le trafic entrant pour s'assurer de sa conformité au niveau du protocole et des entêtes http, des cookies, des champs de formulaire, etc. Ces équipements filtrent les menaces OWASP (Open Web Application Security Project).

4. Sécurité des données et des flux

Les Données Personnelles sont chiffrées :

- Au repos. A cet effet, NEW OXATIS utilise principalement AWS KMS pour chiffrer les bases de données en AES-256.
- Pendant le transport, par l'intermédiaire du protocole TLS.

5. Hébergement des données

L'infrastructure de NEW OXATIS est organisée de sorte qu'il n'existe pas de point de défaillance unique.

L'infrastructure est hébergée sur un Data Center de classe 4 (Jaguar Network du groupe Iliad). Le Data Center a obtenu la conformité PCI DSS le 16 avril 2014.

6. Sauvegarde et intégrité des données :

Les serveurs et équipements composant l'infrastructure sont entièrement redondés et ce à tous les niveaux (alimentation électrique, carte réseaux, carte contrôleur etc…). Les équipements réseaux sont également redondés.

NEW OXATIS a mis en cluster tous les équipements critiques : firewalls, load balancers, relais de messagerie, hyperviseurs, baies de stockage et bases de données.

Les données critiques sont sauvegardées selon le principe du 3-2-1 : il existe a minima trois copies, sur deux supports différents, dont une hors-site.

Les données des clients sont sauvegardées via des snapshots toutes les heures.

Les bases de données SQL sont intégralement sauvegardées toutes les nuits et de manière incrémentale toutes les 15 minutes. La durée de rétention sur site au niveau des baies est de 10 jours au niveau des bases de données et des fichiers.

Une sauvegarde automatique des machines virtuelles est réalisée tous les jours ce qui permet, à tout moment, de revenir aux versions antérieures.

Afin d'améliorer les temps de restauration en cas de reprise d'activité, une baie de stockage secondaire (disposée dans une autre salle que la baie de production) est dédiée à la réplication des données de la baie principale via un réseau privé de 10GB. NEW OXATIS dispose également de serveurs de secours permettant de relancer l'activité.

7. Supervision

NEW OXATIS met en place trois types de supervision :

- **Supervision Internet (World Wide Web).** Une mesure de qualité et une surveillance de la disponibilité de nos services sont effectuées par des sondes au niveau d'Internet pour s'assurer que tous nos services répondent à chaque instant.
- **Supervision Interne de l'infrastructure.** Une solution de supervision est en place au sein de l'infrastructure pour auditer en temps réel tous les équipements, serveurs, stockages et réseaux.
- **Outil propriétaire de supervision**. New Oxatis a développé un ensemble très conséquent de scripts et d'outils de supervision pour contrôler la bonne exécution des processus métiers.

8. Maintenance

Une veille quotidienne est effectuée pour suivre les alertes de sécurité remontées par les fabricants et les autorités spécialisés.

9. Sécurité réseau et serveur

Le Data Center est situé à 5 kilomètres du siège social de NEW OXATIS, ce qui a permis la mise en place d'un réseau privé et d'une fibre dédiée. Grâce à ce réseau privé, il est possible d'accéder à l'infrastructure sans passer par le world wide web, ce qui augmente considérablement le niveau de sécurité. Aucun accès direct (RDP) n'est effectué via le réseau WAN.

Dans le cadre d'une attaque par déni de service massif, NEW OXATIS conserve ainsi un accès dédié et privé pour accéder à ses infrastructures.

10. Sécurité physique des locaux et lieux de stockage des données

La qualité du bâtiment, des infrastructures et des équipements de sécurité est conforme à l'état de l'art.

La sécurisation physique de l'environnement est garantie par 6 points de contrôle d'accès, dont un biométrique. Ainsi, sont notamment prévues les mesures suivantes : accès biométriques, supervision et personnel sur site 24h/24h et 7j/7, couloirs thermiques (Cold Corridor), systèmes de détection de fumée par aspiration avec avertissement précoce (VESDA), systèmes d'extinction à gaz inerte.

La liste des accès et droits d'accès est maintenue à jour par le directeur technique de NEW OXATIS.

C. Sous-traitants ultérieurs autorisés

Identité du Sous-Traitant	Catégories de traitement réalisés	Emplacement des opérations de traitement	Transferts hors UE	Commentaires
AWS	Hébergement des Données Personnelles	France	Non	
CLOUDFLARE	Hébergement des Données Personnelles			
JAGUAR	Hébergement des Données Personnelles Stockage Cloud Gestion du réseau	France	Non	
MAILJET	Hébergement des Données Personnelles	Allemagne, Belgique	USA, Inde	Transfert encadré par des clauses contractuelles types
MNC France	Hébergement des Données Personnelles	France	Suisse	Pays offrant une protection adéquate
SENDINBLUE	Emailing / Newsletter	France, Irlande, Allemagne	Canada, USA	Clauses contractuelles types et minimisation des données
ALTRAN	Prestataire Program Manager / Testeur	France	Non	
OVEA	Hébergement onPremise plateforme PWB	France	Non	
WOLEET	Fournisseur de block-chain pour preuve de facturation/pour cryptage des factures	France	Non	
BIG COMMERCE	CMS e-commerce	France / USA	Oui	Transfert encadré par des clauses contractuelles types
GOOGLE CLOUD PLATFORM	Hébergement des Données Personnelles pour BigCommerce Stockage Cloud	Allemagne	Non	