Protection des données à caractère personnel CALLIMEDIA SAS pour sa plateforme LMS « Upility® »
Données personnelles collectées par le Client

Préambule : La BOÎte à Outils **ou « Upility® » est une plateforme LMS (Learning Management System) de formation et/ou d'enseignement à distance propriété de CALLIMEDIA SAS.**
Le Client a souscrit un contrat auprès de CALLIMEDIA SAS pour que CALLIMEDIA élabore des modules de formation à distance (*digital learning*) qui seront diffusés par la Plateforme « Upility® » sur un thème choisi par le Client afin de former les Utilisateurs choisis par le Client.
Dans le cadre de ce contrat, le Client est amené à communiquer les données personnelles des Utilisateurs à la SAS CALLIMEDIA (ci-après le « Prestataire »).

Le Client et le Prestataire s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel, incluant le Règlement général européen de protection des données personnelles n°2016-679 dit « RGPD » et la loi n°78-17 du 06 janvier 1978 dite « informatique, fichiers et libertés » (ci-après la « Réglementation »)

Au sens de l'article 4, points 7 et 8 du RGPD, le **Client est responsable du traitement** et le **Prestataire intervient en qualité de sous-traitant** des données à caractère personnel.

Article 1 – Définitions

« Client », désigne ___ au capital social de ____ euros, dont le siège social est situé ____, immatriculée au Registre du Commerce et des Sociétés de ____ sous le numéro ____, a conclu un contrat de prestation de service avec CALLIMEDIA SAS portant sur l'utilisation de la Plateforme et dont la présente annexe fait partie intégrale.

« **Utilisateur** », désigne l'internaute se connectant sur la Plateforme **pour suivre une formation à distance, c'est aussi la « personne concernée »,** au moyen de codes sécurisés émis par le Prestataire et communiqués par Le Client] pour suivre une formation à distance**.**

« **Données personnelles** » désignent conformément à la réglementation applicable en matière de protection des données personnelles, toute information se rapportant à une personne physique identifiée ou identifiable (la « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

« **Personne concernée** » désigne la personne physique dont les Données personnelles sont traitées ;

« **Responsable du traitement** » désigne conformément à la réglementation applicable en matière de protection des données personnelles, la personne qui détermine les finalités et les moyens du traitement des Données personnelles (art.4 § 7 RGPD).

« **Sous-traitant** » désigne conformément à la réglementation applicable en matière de protection des données personnelles, la personne qui traite des Données personnelles, sous l'autorité, sur instructions et pour le compte du Responsable du traitement (art.4§ 8 RGPD).

« **Traitement de données personnelles** » désigne conformément à la réglementation applicable en matière de protection des données personnelles, 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" (art 4 § 2 RGPD).
Les données ainsi traitées doivent être mises dans un fichier qui est défini comme tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés.

« Finalité d'un traitement » désigne conformément à la réglementation applicable en matière de protection des données personnelles, l'objectif principal d'une application informatique de données personnelles. Exemples de

finalité : formation, gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, formation en ligne, etc.

« Destinataire » désigne conformément à la réglementation applicable en matière de protection des données personnelles, toute Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers, à l'exception des autorités publiques qui reçoivent communication dans le cadre d'une mission d'enquête (art.4 §9 RGPD).

« Cookies » = « traceurs », témoins de connexion qui analysent la navigation de l'internaute, ses déplacements, ses habitudes de consultation ou de consommation afin notamment, de lui proposer éventuellement des parcours de formations ciblées ou des services personnalisés.

« DPD » désigne conformément à la réglementation applicable en matière de protection des données personnelles, le Délégué à la Protection des Données (en anglais DPO : Data Protection Officer).

« **Violation de Données personnelles** » désigne conformément à la réglementation applicable en matière de protection des données personnelles, une violation de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la corruption, le détournement de finalité, la compromission de la confidentialité ou la divulgation non autorisée de Données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Article 2 - Objet

La présente Annexe a pour objet de définir les obligations respectives du Client et du Prestataire et de définir les conditions dans lesquelles le Prestataire s'engage à effectuer pour le compte du Client des opérations de Traitement de données à caractère personnel définies ci-après, et assure leur protection conformément à la Réglementation.
En cas de conflit ou d'ambiguïté entre les stipulations de la présente Annexe et celles du Contrat, les stipulations de la présente Annexe prévaudront.

Article 3 – Descriptions des Traitements objets de la sous-traitance

Le Prestataire est autorisé à traiter pour le compte du Client les Données personnelles nécessaires pour une prestation de service de formation e-learning destinée à former un public professionnel et non professionnel sur les thèmes définis par le Client.
Le Prestataire ne peut traiter les Données personnelles pour d'autres finalités que celles nécessaires pour l'exécution du Contrat sans l'autorisation du Client.
La **durée des traitements** mis en œuvre par le Prestataire pour le Client correspond à la durée du Contrat.

Le **Client détermine sous sa responsabilité** les **finalités des traitements** confiés au Prestataire, lesquels sont les suivantes :

- La collecte et la sauvegarde des données personnelles et des données de formation nécessaire à la fourniture du service ;
- La navigation sur le Site et la gestion et la traçabilité de la prestation de service commandés par le client : données de connexion et d'utilisation du Site ;
- La formation à distance « e-learning » : gestion des comptes des Utilisateurs , mise en ligne des contenus de formation, validation d'un quiz d'évaluation, gestion des statistiques, exploitation des résultats de l'Utilisateur ;
- La prévention et la lutte contre la fraude informatique (spamming, hacking…) : adresse IP, le mot de passe (hashé) ;
- L'amélioration de la navigation sur la Plateforme : données de connexion et d'utilisation ;
- Le maintien en condition opérationnel de la Plateforme ;
- La fourniture d'un service de support applicatif ;
- La réalisation d'enquêtes de satisfaction facultatives auprès de l'équipe de direction ou de l'équipe de projet du Client : adresse de courrier électronique (e-mail).

Les **Données personnelles** transmises par le Client à CALLIMEDIA SAS sont :

Nom ; prénom ; adresse de courrier électronique (e-mail), mot de passe de l'Utilisateur.

Les données collectées générées lors de l'utilisation de la Plateforme : date et heure de connexion, temps passé, note d'évaluation si quiz ainsi que les logs applicatifs, les informations liées au navigateur web et l'historique de formation.

CALLIMEDIA SAS et sa Plateforme ne commercialisent pas les Données personnelles collectées et ne les transmettent pas à des tiers.

La **catégorie de Personnes concernées** est constituée par tout Utilisateur de la Plateforme.

Les Données personnelles ne sont recueillies que sur **la base légale** du consentement de l'Utilisateur / Personne concernée et de l'exécution du Contrat conclu entre Le Client et Le Prestataire et/ou leur intérêt légitime notamment quant à l'exploitation de données statistiques.

Les **destinataires des Données personnelles** collectées sont :

- Le service développement et/ou le service Support Client de CALLIMEDIA SAS.
- Les administrateurs de la Plateforme au sein du Client.
- **OVEA, SARL inscrite au RCS de Montpellier sous le N° 441 938 222** dont le siège est 59 rue Nelson Mandela à 34070 MONTPELLIER, en sa qualité d'**hébergeur** de la Plateforme sur le serveur du site https://upility-lms.com/

La durée **de conservation** des Données personnelles est celle de la durée d'exécution du Contrat.

Les **droits de la Personne concernée** sont, conformément à la réglementation applicable, les suivants :

- accéder aux données à caractère personnel la concernant, les compléter, les rectifier, demander leur effacement ou exercer son droit à la limitation du traitement de ses données (article 17 du RGPD), lorsqu'elles sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite,
- droit de retirer à tout moment son consentement (article 13-2 RGPD)
- droit à la limitation du traitement de ses données (article 18 RGPD)
- droit d'opposition au traitement de ses données (article 21 RGPD)
- droit à la portabilité des données qu'elle a fournies, lorsque ces données font l'objet de traitements automatisés fondés sur son consentement ou sur un contrat (article 20 RGPD)
- droit de définir le sort de ses données après sa mort et de choisir que CALLIMEDIA SAS communique (ou non) ses données à un tiers qu'elle aura préalablement désigné. Dès que CALLIMEDIA SAS a connaissance du décès d'une Personne concernée et à défaut d'instructions préalable de sa part, les données de la Personne concernée décédée seront détruites sauf si leur conservation s'avère nécessaire à des fins probatoires ou pour répondre à une obligation contractuelle ou légale.

Article 4- Obligations du Prestataire, Sous-traitant envers le Responsable du traitement

Le Prestataire s'engage à :

- traiter les Données personnelles pour les seules finalités qui font l'objet du Contrat ;
- traiter les Données personnelles conformément aux instructions du Client, à moins que le Prestataire ne soit tenu d'y procéder en vertu de la loi ou du droit applicable au Contrat. Dans ce cas, le Prestataire informera le Client de son obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs d'intérêt public.
  Si le Prestataire considère qu'une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l'Union, du droit français ou du droit des États membres relatives à la protection des données, il en informe immédiatement le Client par écrit ;
- garantir la confidentialité des Données personnelles traitées dans le cadre du Contrat et, en particulier, empêcher leurs destruction, fuite, déformation, détournement, atteinte ou divulgation à des tiers non autorisés ;
- veiller à ce que les personnes autorisées à traiter des Données personnelles dans le cadre du Contrat ;
- s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- reçoivent la formation nécessaire en matière de protection des données à caractère personnel.
- prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection

des Données personnelles dès la conception et de protection des Données personnelles par défaut ;
- proposer des prestations respectueuses des principes de proportionnalité, de minimisation et de limitation des Données personnelles, assurant que seules les données pertinentes telles que visées à l'article 3.3 de la présente Annexe sont traitées.

Le Prestataire est responsable de son personnel et du respect par ce dernier des obligations lui incombant en vertu de la présente Annexe.
À cet égard, le personnel du Prestataire ne pourra accéder aux Données personnelles, les utiliser, les modifier, sauf lorsque cela est strictement nécessaire aux fins de la fourniture des services tels que mentionnés au Contrat, de la prévention ou du traitement des problèmes techniques ou pour en assurer la sécurisation.

Le Prestataire met en place des mesures techniques et organisationnelles appropriées pour s'assurer du respect par son personnel de ses obligations notamment en termes de contrôle des personnes habilitées à accéder aux données, de sécurisation des accès et de traçabilité. Il en tient la description à la disposition de son Client à sa demande.

Le Prestataire s'engage à ce que l**es données soient conservées en France et ne fassent pas l'objet de transfert vers un autre pays et vers un pays hors Union Européenne.**

En tout état de cause, le Prestataire s'engage à ne transférer aucune Donnée personnelle en dehors de la France, sans l'autorisation écrite et préalable du Client.
En cas d'autorisation du Client, le Prestataire s'engage à ce que ce que de tels transferts soient faits en conformément avec la réglementation applicable et si nécessaire en cas de transfert hors Union Européenne, encadrés par l'adhésion à une décision d'adéquation de la Commission européenne ou toutes autres garanties appropriées prévues par l'article 46 du RGPD et à ce qu'aucun transfert de Données personnelles hors du territoire de l'Union européenne ne diminue d'une quelconque manière la protection accordée aux Personnes concernées du Client.

Le Prestataire tient à la disposition du Client à sa demande, la documentation nécessaire pour démontrer le respect de ses obligations dans le cadre de la présente Annexe.

Article 5 – Obligations du Client, Responsable du traitement

5.1 En tant que commanditaire de la prestation, le Client est responsable des traitements mis en œuvre par le Prestataire pour son compte et, par conséquent, il appartient au seul Client de s'assurer de la base légale des traitements dont il décide et qu'il confie au Prestataire dans le cadre du Contrat.
Le Client s'engage à fournir au Prestataire et à documenter par écrit si requis par le Prestataire, toute instruction concernant le Traitement par le Prestataire.

Le Client s'engage à collecter les Données personnelles auprès des Utilisateurs à qui il destine l'accès à la Plateforme **et à ce titre il appartient au seul Client de recueillir tout consentement auprès des Personnes concernées, en corrélation avec les finalités poursuivies.**

Si un audit réalisé par le Client démontre une non-conformité du Prestataire aux obligations de la présente Annexe, le Prestataire dispose d'un délai de soixante (60) jours pour y remédier.

Article 6 – Coopération et assistance

Le Client fournie l'information relative au traitement qu'il fait réaliser par le Prestataire aux Personnes concernées au moment de la collecte des données et en tout état de cause avant de réaliser le traitement des données.

En cas de demande d'une Personne concernée auprès du Client (notamment demande d'accès, de modification, d'effacement, d'opposition, de limitation ou de portabilité) nécessitant l'aide du Prestataire, ce dernier s'engage à apporter dans les plus brefs délais son concours au Client afin que ce dernier soit en mesure de répondre dans les délais légaux impartis à ladite Personne concernée.

Si une Personne concernée envoie directement une demande au Prestataire, celui-ci en informe immédiatement le Client par courrier électronique à l'adresse : maxime.vigne@horus-pharma.com et doit agir selon les instructions du Client.

Le Prestataire s'engage à coopérer loyalement et dans les meilleurs délais avec le Client dans le cadre d'analyses d'impact relatives à la protection des Données personnelles.

Les Parties s'engagent à coopérer entre elles loyalement et sans délai dans le cadre de consultation préalable des autorités de contrôle, notamment de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Article 7 – Sous-traitance ultérieure

Le Prestataire ne peut avoir recours à un Sous-traitant ultérieur pour réaliser des activités de traitements spécifiques aux fins d'exécution de son contrat de prestation de services qu'avec l'autorisation écrite et préalable du Client, étant précisé que ce dernier peut la refuser peut la refuser avec une motivation légitime et argumentée par écrit. Tout changement de Sous-traitant ultérieur devra faire l'objet d'une nouvelle demande dans les conditions du présent article.

Dans ce cadre, le Prestataire s'engage à signer un contrat écrit avec chaque Sous-traitant ultérieur imposant à ce dernier le respect de la Réglementation et de l'ensemble des obligations équivalentes dans la présente Annexe.
À ce titre, le Prestataire s'engage à ne faire appel qu'à des Sous-traitant ultérieur qui présentent des garanties suffisantes, et en tout état de cause au moins équivalentes à celles du Prestataire.
Le Prestataire devra fournir au Client avec la demande d'autorisation de sous-traitance, l'ensemble des justificatifs permettant au Client de s'assurer que ce Sous-traitant présente les garanties effectivement suffisantes.
Passé le délai de trente (30) jours de la demande d'autorisation de la sous-traitance, l'absence de refus écrit par le Client vaut acceptation du Sous-traitant ultérieur par le Client.
Le Prestataire demeure pleinement responsable de ces sous-traitants devant le Client.

Article 8 – Notification des violations de Données personnelles.

Le Prestataire notifie au Client, Responsable du traitement, la survenue de toute violation de Données personnelles ayant ou susceptible d'avoir des conséquences directes ou indirectes sur les Données personnelles, la vie privée, les droits et libertés des Personnes concernées, ou susceptible d'affecter négativement l'image, la réputation ou l'honorabilité du Client.

La notification est adressée par courrier électronique dans un délai maximum de Quarante-huit (48) heures à compter de la survenue de la violation des Données personnelles, à l'adresse suivante : 22 allée Camille Muffat, 06200 NICE.

Cette notification est accompagnée de toute documentation utile afin de permettre au Client si nécessaire de notifier cette violation à l'autorité de contrôle compétente et comporte au moins :

- la description de la nature de la violation de Données personnelles y compris, si possible, les catégories et nombre approximatif de Personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de Données personnelles concernées ;
- 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 ;
- la description des conséquences probables de la violation des Données personnelles ;
- la description des mesure à mettre en œuvre ou déjà mise en œuvre pour remédier à la violation des Données personnelles, y compris le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Le Prestataire s'abstient de divulguer et de communiquer toute information relative à la violation des Données personnelles, sauf obligation légale ou autorisation écrite données par le Client.

Le Prestataire s'engage à collaborer activement afin de mettre en place des actions nécessaires à la correction de tout dysfonctionnement lui incombant qui serait à l'origine ou une conséquence de la violation des Données personnelles et à empêcher que cette violation ne se reproduise plus.

Article 9 – Sécurité des Données personnelles.

À travers sa Plateforme **,** le Prestataire s'engage à prendre toutes précautions utiles afin de préserver la confidentialité, l'intégrité et la sécurité des Données personnelles et notamment d'empêcher qu'elles ne soient

déformées, endommagées, détournées ou communiquées à des tiers non autorisés, et plus généralement à mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour protéger les Données personnelles contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé.

Le Prestataire s'engage à mettre en œuvre les mesures de sécurité suivantes :

- *la pseudonymisation et le chiffrement des données à caractère personnel*
- *les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;*
- *les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;*

une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement décrites ci-après :

Nom	Description	Intervenant
Mise à jour des logiciels serveurs	Des mises à jour des logiciels serveurs (PHP, MySQL, Redis, NGINX) sont décidées par le Technical Lead de Callimedia et réalisées par le prestataire OVEA. Dès que OVEA confirme que la mise à jour a été réalisée, le Technical Lead vérifie le travail et le valide. Toute demande et réponse est réalisée par mail.	OVEA (prestataire)
Sécurisation des accès serveurs	Les accès aux serveurs sont réalisés par connexion SSH sécurisée et encryptée. Cette connexion peut se réaliser uniquement depuis l'adresse IP Callimedia ou via VPN (sécurisée et encryptée) via Storm Shield	OVEA (prestataire) / NANORESEAUX (prestataire)
Sauvegardes données	Deux sauvegardes journalières sont réalisées chaque jour, une pour les documents et l'autre pour les bases de données. Elles sont transmises vers un autre serveur dans le même datacenter ainsi que vers un serveur externe (localisé aussi en France, Montpellier). Ces sauvegardes sont stockées trente (30) jours.	OVEA (prestataire)
Système de journalisation dès accès serveurs	Les logs systèmes gardent les informations de connexion déconnexion des administrateurs serveurs	OVEA (prestataire)
Mise à jour des OS serveurs	Les systèmes d'exploitation des serveurs Linux sont mis à jour régulièrement par le prestataire de services OVEA.	OVEA (prestataire)
Gestionnaire cookies et traceurs	Mise en place du gestionnaire de cookies et traceurs « tarteaucitron » qui est proposé par la CNIL (https ://www.cnil.fr/fr/cookies-et-traceurs-que-dit-la- loi)	Callimedia (Équipe développeur)
Système de journalisation dès accès à la Plateforme UPILITY	Conservation des logs d'accès à la Plateforme (utilisateurs et administrateurs) concernant la date de connexion et les actions réalisées pour une durée maximale de 6 mois.	Callimedia (Équipe développeur)
Authentification des Utilisateurs de la Plateforme UPILITY	Deux moyens d'authentification : Authentification classique avec un formulaire pour introduire l'Utilisateur et le mot de passe (ce mot de passe est chiffré avec bcrypt). Authentification SSO SAML2, l'authentification est réalisée par un serveur externe et les informations (prénom, nom, mail) sont transmises vers UPILITY	Callimedia (Équipe développeur)

Tentatives de connexion	L'Utilisateur sera bloqué pendant 30 mn après 3 échecs de tentatives d'accès	Callimedia (Équipe développeur)
Droites d'accès des Utilisateurs	Tous les Utilisateurs ont un compte d'accès « Apprenant », leur permettant d'accéder aux éléments auxquels ils sont inscrits. Un système de compte spécifique pour les administrateurs permet de créer des comptes spécifiques afin de limiter l'accès pour chaque administrateur	Callimedia (Équipe développeur)
Suppression des accès obsolètes	Il est possible de désactiver les accès des Utilisateurs / administrateurs obsolètes. Les accès aux serveurs productions sont changés/supprimés sur demande via mail vers notre hébergeur	Callimedia (Équipe développeur) / OVEA (prestataire)
Durée de conservation des données	Les Données personnelles et statistiques seront conservées en base active pendant la durée du contrat entre le Client et Callimedia à l'issue de laquelle elles sont détruites sauf demande d'archivage du client pour une durée à définir et au plus tard 90 jours après la date de fin effective du contrat.	Callimedia

Article 10 – Délégué à la protection des données

Conformément à l'article 37 du RGPD, le Délégué à la Protection des Données (DPD) du Prestataire est un DPD externe Maître Guillaume BENAMARA, avocat au barreau de Nîmes, qui peut être contacté par courrier à l'adresse postale : CALLIMEDIA « RGPD », 1 chemin de Borie Parc de Bellegarde – Bat A 34170 Castelnau-le-Lez, ou par courriel à l'adresse : rgpd@callimedia.fr

Article 11 – Registre des activités de Traitements

Le Prestataire déclare tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Client comprenant l'ensemble des éléments mentionnés à l'article 30 § 2 du RGPD.

Article 12 – Sort des Données personnelles en fin de Contrat

À l'expiration du Contrat ou en cas de résiliation de ce dernier pour tout motif, le Prestataire s'engage à détruire les Données personnelles à l'expiration d'un délai de 90 jours après la cessation du contrat et à certifier par écrit au Client que la destruction a bien été réalisée.

Le Prestataire s'engage à détruire les copies existantes des Données personnelles, à moins que les obligations contractuelles ou légales n'exigent la conservation de celles-ci, notamment à titre de preuve de la validation de formations certifiantes et/ou diplômantes et/ou ouvrant un droit à l'exercice d'une fonction, d'un emploi ou d'une profession.

La présente Annexe comporte douze articles.
Fait au siège de CALLIMEDIA SAS,