Contrat de Traitement de Données Personnelles

Contrat de Traitement de Données Personnelles

I. PRÉAMBULE

Étant préalablement exposé que :

A. La Législation Applicable sur la Protection des Données permet à tout Responsable de Traitement en charge du Traitement de Données Personnelles de désigner une personne physique ou morale, une administration publique ou toute autre entité ou association pour agir en qualité de Sous-Traitant en vue du Traitement de Données Personnelles pour le compte du Responsable de Traitement, parmi des entités qui sont en mesure de garantir de manière adéquate, en raison de leur expérience, de leurs capacités et de leur fiabilité, la conformité à la Législation Applicable sur la Protection des Données, en ce compris en matière de sécurité.

B. Le Sous-Traitant désigné doit présenter des garanties suffisantes pour la mise en œuvre de mesures techniques et organisationnelles appropriées visant à assurer la protection des Données Personnelles et des droits des Personnes Concernées.

C. Le présent contrat de traitement de données, conjointement avec ses annexes (collectivement le « **CTD** »), est conclu entre le client (ci-après : le « **Client** »), à savoir la personne physique ou morale qui a souscrit au Service (tel que défini ci-après) et dont les données de contact sont précisées ci-après, et la société AGENCE DES MEDIAS NUMERIQUES (« **AMEN** »), société par actions simplifiée de droit français, dont le siège social est situé 12 rond-point des Champs-Élysées, 75008 Paris, immatriculée au Registre du commerce et des sociétés de Paris sous le numéro de 421 527 797. Le Client et AMEN, désignés collectivement les « **Parties** », et individuellement la/une « **Partie** », concluent le présent CTD afin de refléter l'accord des Parties concernant le Traitement des Données Personnelles du Client, en conformité avec les exigences de la Législation Applicable sur la Protection des Données.

D. AMEN fournit au Client le(s) service(s) (« **Service(s)** ») activé(s) par ce dernier conformément aux conditions contractuelles figurant dans le(s) Bon(s) de Commande et les Conditions Générales de Services, collectivement accessibles à partir de ce lien (« **Contrat-Cadre de Services** » ou « **CCS** ») et, afin de fournir le Service susmentionné au titre du présent CTD, AMEN peut Traiter des Données Personnelles pour le compte du Client.

E. Plus précisément, la/les finalité(s) du Traitement des Données Personnelles du Client dans le cadre du Service est/sont décrite(s) en Annexe 1.

F. Le Client reconnaît que son utilisation du Service peut être soumise à la Législation Applicable sur la Protection des Données en vigueur dans des pays ou territoires qui imposent certaines exigences en matière de Traitement de Données Personnelles.

G. Les Parties ont conclu le présent CTD afin de s'assurer de leur conformité à la Législation Applicable sur la Protection des Données et de mettre en place des mesures de protection et procédures pour le Traitement licite des Données Personnelles. Le Client confirme que les stipulations figurant dans le présent CTD reflètent les obligations imposées à AMEN au titre de la Législation Applicable sur la Protection des Données, concernant le Traitement des Données Personnelles du Client dans le cadre de la fourniture du Service. En conséquence, AMEN s'engage à respecter les stipulations énoncées dans le présent CTD.

Le préambule ci-dessus fait partie intégrante du CTD.

1. DÉFINITIONS

Sauf définition contraire dans le présent CTD, tous les termes en majuscules dans le présent document ont le sens qui leur est attribué dans le Contrat-Cadre de Services. En cas de conflit ou d'incohérence entre le présent CTD et le Contrat-Cadre de Services concernant les garanties de protection des données, le présent CTD prévaudra.

« **Autorité de Contrôle** » désigne toute autorité compétente pour surveiller et faire respecter l'application de la Législation Applicable sur la Protection des Données en ce qui concerne le Traitement des Données Personnelles Client dans le cadre de la fourniture du Service.

« **Catégories Particulières de Données Personnelles** » désigne les Données Personnelles qui révèlent 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, en ce compris les données relatives à des condamnations pénales et à des infractions ou encore à des mesures de sûreté connexes.

« **Clauses Contractuelles Types** » désigne les clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du Règlement, telles qu'approuvées par la Commission européenne dans la Décision d'exécution (UE) 2021/914 de la Commission.

« **Client** » désigne la personne qui a souscrit au Service.

« **Contrat-Cadre de Services** » ou « **CCS** » désigne les stipulations et conditions prévues dans le(s) Bon(s)de Commande et dans les Conditions Générales de Services relatives à la fourniture du Service convenu entre les Parties, et disponibles au lien suivant : les Conditions Générales de Service.

« **CTD** » désigne le présent contrat global de traitement des données conjointement avec ses Annexes 1, 2 et 3.

« **Décision d'Adéquation** » désigne une décision juridiquement contraignante émise par la Commission européenne qui autorise le transfert de Données Personnelles depuis l'Espace économique européen vers un pays tiers considéré comme offrant des garanties adéquates en matière de protection des données.

« **Données Personnelles** » signifie toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Par souci de clarté, les « Données Personnelles » ont le sens qui leur est attribué dans le Règlement et la Législation Applicable sur la Protection des Données.

« **Données Personnelles Client** » désigne les Données Personnelles relatives aux Personnes Concernées, Traitées dans le cadre du Service fourni par AMEN au Client.

« **Droits de la Personne Concernée** » désigne les droits reconnus à la Personne Concernée en vertu de la Législation Applicable sur la Protection des Données. Dans la mesure où le Règlement est applicable, « Droits de la Personne Concernée » désigne, par exemple, le droit de demander au Responsable de Traitement l'accès aux Données Personnelles et leur rectification ou leur effacement, ou la limitation du Traitement relatif à la Personne Concernée ou le droit d'opposition au Traitement, ainsi que le droit à la portabilité des données.

« **EEE** » désigne l'Espace économique européen.

« **Exportateur de Données** » a le sens qui lui est attribué dans les Clauses Contractuelles Types.

« **Importateur de Données** » a le sens qui lui est attribué dans les Clauses Contractuelles Types.

« **Législation Applicable sur la Protection des Données** » désigne, dans les pays membres de l'UE, le Règlement et les lois complémentaires sur la protection des données dans les pays membres de l'UE, en ce compris toute directive et/ou tout code de bonne pratique émis par l'Autorité de Contrôle compétente au sein de l'UE ; et/ou, dans les pays non-membres de l'UE, toute loi en matière de protection des données relative à la protection et au traitement licite de Données Personnelles.

« **Liste des Sous-Traitants Ultérieurs** » désigne la liste figurant en Annexe 3 du présent CTD.

« **Personne Concernée** » a le sens qui lui est attribué dans le Règlement.

« **Règlement** » désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

« **Responsable de Traitement** » désigne, en général, la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles.

« **Responsable de Traitement Hors EEE** » désigne toute entité, agissant en qualité de Responsable de Traitement, auquel AMEN fournit les Services et qui est établie dans un pays situé en dehors de l'EEE, dans lequel ladite entité n'est pas soumise au Règlement en vertu de son article 3, paragraphe 2.

« **Service/s** » a la sens figurant à la lettre D. du Préambule.

« **Services Impliquant des Sous-Traitants Ultérieurs Hors EEE** » désigne les services fournis par des Sous-Traitants Ultérieurs situés en dehors de l'Union européenne.

« **Sous-Traitant** » désigne, en général, une personne physique ou morale, une autorité publique, un service ou un autre organisme qui traite des données personnelles pour le compte du responsable de traitement.

« **Sous-Traitant Ultérieur** » désigne une entité à laquelle AMEN a recours pour l'assister dans le Traitement de Données Personnelles Client (ou qui met en œuvre un tel Traitement de Données Personnelles Client) en exécution des obligations d'AMEN au titre du CTD, telle que figurant dans la Liste des Sous-Traitants Ultérieurs qui a été approuvée par le Client en vertu de l'article 5 du présent CTD.

« **Sous-Traitant Ultérieur Hors EEE** » désigne toute entité, agissant en qualité de Sous-Traitant (ou de Sous-Traitant Ultérieur) et Traitant les Données Personnelles Client, dans le cadre de la fourniture du Service, dans un pays situé en dehors de l'EEE, dans lequel ladite entité n'est pas soumise au Règlement en vertu de son article 3, paragraphe 2.

« **Traite(r)** » ou **Traitement** » désigne toute opération ou tout ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés et appliquée(s) à des Données Personnelles ou des ensembles de Données Personnelles, telle(s) 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.

« **UE** » désigne l'Union européenne.

« **Violation de Données Personnelles** » désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données Personnelles.

2. ROLES EN MATIERE DE PROTECTION DES DONNEES

2.1. Les Parties acceptent que :

a) Le Client est le Responsable de Traitement au regard des Données Personnelles Client, sauf si et dans la mesure où le Client agit en qualité de Sous-Traitant au regard des Données Personnelles Client pour le compte d'un tiers qui agit lui-même en qualité de Responsable de Traitement ou de Sous-Traitant. Le Client, ou le Responsable de Traitement concerné, détermine les finalités de la collecte et du Traitement des Données Personnelles Client ;
b) AMEN agit, dans tous les cas, en qualité de Sous-Traitant des Données Personnelles Client dans le cadre de la fourniture du Service ; et
c) le présent CTD régit les relations entre les Parties au regard de leurs obligations et devoirs respectifs dans le cadre du Traitement des Données Personnelles Client par AMEN, agissant en qualité de Sous-Traitant, pour les besoins de la fourniture du Service.

3. OBLIGATIONS D'AMEN

3.1. Le Client ou le Responsable de Traitement concerné détermine les finalités du Traitement des Données Personnelles Client pour les besoins de la fourniture du Service.

3.2. Dans le cadre de la fourniture du Service, AMEN s'engage à respecter les obligations suivantes, en ce compris celles figurant dans les Annexes 1 et 2 jointes aux présentes :

a) AMEN Traite les Données Personnelles Client uniquement dans la mesure nécessaire à la fourniture du Service, sous réserve des instructions écrites du Client figurant dans le présent CTD ;
b) AMEN informe le Client si elle considère qu'une instruction écrite du Client constitue une violation de la Législation Applicable sur la Protection des Données. En aucun cas AMEN n'est tenue d'effectuer u examen juridique exhaustif des instructions écrites du Client ;
c) AMEN, en sa qualité de Sous-Traitant, notifie au Client dans les meilleurs délais tout contact établi par ou toute communication reçue d'une Autorité de Contrôle relatif au Traitement des Données Personnelles Client. À cet égard, les Parties reconnaissent et acceptent que le Client, et non AMEN, est responsable de répondre à de telles demandes ;
d) AMEN a mis en œuvre des mesures opérationnelles, techniques et organisationnelles, y compris telles que décrites en Annexe 2 des présentes, destinées à protéger les Données Personnelles Client. Les Parties reconnaissent et acceptent qu'AMEN est expressément autorisée à mettre en œuvre des mesures alternatives adéquates ou à utiliser des sites alternatifs, dès lors que le niveau de sécurité de ces mesures ou sites est maintenu ou renforcé par rapport aux mesures déclarées ;
e) En cas de divulgation par AMEN de Données Personnelles Client à son personnel directement et exclusivement impliqué dans l'exécution du Service, AMEN s'assure que ce personnel : i) s'engage à respecter la confidentialité ou est soumis à une obligation légale de confidentialité appropriée et ii) Traite les Données Personnelles Client conformément aux instructions d'AMEN en conformité avec ses obligations au titre du présent CTD.

4. OBLIGATIONS DU CLIENT

4.1. Le Client reconnaît et accepte que, pour permettre à AMEN de fournir le Service, le Client doit communiquer à AMEN les Données Personnelles Client. Le Client s'engage à vérifier que les mesures de

sécurité énumérées en Annexe 2 du présent CTD sont compatibles avec les types de Données Personnelles que le Client entend confier à AMEN.

4.2. Le Client déclare et garantit :

a) qu'il dispose d'une base légale appropriée (par ex., le consentement de la Personne Concernée, des intérêts légitimes, l'autorisation de l'Autorité de Contrôle compétente, etc.) afin de Traiter les Données Personnelles Client et de les divulguer à AMEN dans le cadre de la fourniture du Service ; et,

b) que les stipulations figurant dans le présent CTD reflètent les obligations imposées à AMEN au titre de la Législation Applicable sur la Protection des Données, concernant le Traitement de Données Personnelles Client dans le cadre de la fourniture du Service.

5. CONSENTEMENT AU TRAITEMENT ULTÉRIEUR

5.1. Le Client reconnaît, accepte et consent à ce que, dans le seul et unique but de fournir le Service et sous réserve de toujours respecter les stipulations du présent CTD, les Données Personnelles Client puissent être Traitées par AMEN ou ses Sous-Traitants Ultérieurs tels que décrits dans la Liste des Sous-Traitants Ultérieurs.

5.2. En vertu de l'article 5.1, AMEN dispose d'une autorisation générale de recourir à des Sous-Traitants Ultérieurs, à condition qu'AMEN :

a) fournisse au Client une information préalable sur l'identité des Sous-Traitants Ultérieurs tel que décrit dans la Liste des Sous-Traitants Ultérieurs et notifie au Client toute mise à jour de la Liste des Sous-Traitants Ultérieurs, afin que le Client puisse s'opposer à la désignation de ces Sous-Traitants Ultérieurs ;
b) conclue avec les Sous-Traitants Ultérieurs des accords incluant les mêmes obligations relatives au Traitement des Données Personnelles Client que celles figurant dans le présent CTD ;
c) fasse preuve d'une diligence appropriée dans le choix des Sous-Traitants Ultérieurs et reste responsable du respect par les Sous-Traitants Ultérieurs des obligations figurant dans le présent CTD ;
d) fournisse au Client, à sa demande, les informations raisonnablement requises concernant les actions et mesures qu'AMEN et ses Sous-Traitants Ultérieurs ont mises en œuvre afin de se conformer sur le plan pratique aux stipulations figurant dans le présent CTD.

6. TRANSFERT DE DONNÉES PERSONNELLES

6.1. Lorsque le Client souscrit à un ou plusieurs Services Impliquant des Sous-Traitants Ultérieurs Hors EEE, AMEN est autorisée, en vertu des articles 5.1 et 5.2 ci-dessus, à transférer les Données Personnelles Client à un ou plusieurs Sous-Traitants Ultérieurs qui sont des Sous-Traitants Ultérieurs Hors EEE et qui seront considérés comme des Importateurs de Données dans le cadre des Clauses Contractuelles Types. Dans ce cas, s'il n'existe pas de Décision d'Adéquation applicable au Sous-Traitant Ultérieur hors EEE, AMEN s'engage à conclure les Clauses Contractuelles Types avec le Sous-Traitant Ultérieur Hors EEE, et à ce que seules les clauses des Clauses Contractuelles Types MODULE 3 : Transfert de sous-traitant à sous-traitant s'appliquent (à l'exclusion des autres MODULES).

6.2. Aucune stipulation du présent CTD ne sera interprétée comme prévalant sur une clause contradictoire des Clauses Contractuelles Types.

6.3. Sur demande, le Client peut solliciter l'opportunité d'examiner les Clauses Contractuelles Types. AMEN pourra, dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, en ce compris des Données Personnelles, expurger une partie du texte des Clauses Contractuelles Types avant d'en partager un exemplaire.

6.4. Le Client reconnaît qu'il est de sa responsabilité de respecter toute obligation et tout devoir supplémentaire applicable afin de rendre licite le transfert de Données Personnelles à AMEN et aux Sous-Traitants Ultérieurs Hors EEE conformément à la Législation Applicable sur la Protection des Données.

6.5. Dans la mesure où le Client est un Responsable de Traitement Hors EEE, AMEN et le Responsable de Traitement Hors EEE acceptent que les Clauses Contractuelles Types sont, en vertu des présentes, acceptées comme ayant été intégrées au présent CTD par référence, pour tout transfert de Données Personnelles Client du Responsable de Traitement Hors EEE à AMEN dans le cadre de la fourniture des Services. Dans ce cas, les stipulations particulières suivantes s'appliquent aux Clauses Contractuelles Types :

(i) La clause 7 des Clauses Contractuelles Types est applicable ;
(ii) Seules les clauses des Clauses Contractuelles Types MODULE 4 : Transfert de sous-traitant à responsable du traitement sont applicables (à l'exclusion des autres MODULES) ;
(iii) Les clauses 14 et 15 ne s'appliquent pas, étant donné que les Services n'impliquent pas de combiner des Données Personnelles Client reçues de la part du Responsable de Traitement Hors EEE avec d'autres Données Personnelles collectées par AMEN dans l'UE.
(iv) En vertu de la clause 17 des Clauses Contractuelles Types, le droit français s'appliquera.
(v) En vertu de la clause 18 des Clauses Contractuelles Types, le Tribunal de commerce de Paris (France) sera compétent.
(vi) Seule l'Annexe 1 du présent CTD sera applicable et sera considérée comme étant l'Annexe I des Clauses Contractuelles Types.

7. OBLIGATIONS EN MATIERE DE COOPERATION ET DE RESPONSABILITE

7.1. Les Parties collaborent de bonne foi afin d'assurer le respect des stipulations du présent CTD, en ce compris, sans limitation, en assurant l'exercice correct et opportun des Droits des Personnes Concernées et en gérant les incidents en cas de violation de sécurité/Violation de Données Personnelles, afin d'en atténuer les éventuels effets négatifs.

7.2 Les Parties collaborent de bonne foi afin de mettre chacune à la disposition de l'autre et des Autorités de Contrôle les informations nécessaires pour démontrer le respect de la Législation Applicable sur la Protection des Données.

8. DROITS DES PERSONNES CONCERNÉES

8.1. En tenant compte de la nature du Traitement, AMEN assiste le Client au moyen de mesures techniques et organisationnelles appropriées dans l'exécution de son obligation de répondre aux demandes d'exercice des Droits de la Personne Concernée.

8.2. AMEN fournira au Client une coopération et une assistance raisonnables ainsi que les informations raisonnablement requises pour répondre aux Personnes Concernées ou permettre au Client de respecter ses obligations au titre de la Législation Applicable sur la Protection des Données relatives aux Droits des Personnes Concernées. Le Client reconnaît et accepte que, dans l'hypothèse où cette coopération et cette assistance nécessitent des ressources significatives de la part d'AMEN, ces ressources seront facturées après notification préalable au Client et accord de ce dernier.

9. RESTITUTION ET SUPPRESSION DES DONNEES PERSONNELLES

9.1. AMEN restituera ou détruira les Données Personnelles Client, sans frais pour le Client, à sa demande et à l'expiration ou à la résiliation anticipée du présent CTD, sous réserve d'une demande écrite du Client avec un préavis raisonnable, à moins que des lois impératives applicables (en ce compris, sans limitation, la Législation Applicable sur la Protection des Données ou toute autorité chargée de l'application des lois y compris, notamment, l'Autorité de Contrôle), n'empêchent AMEN de le faire.

9.2. En cas de demandes spécifiques du Client concernant la restitution des Données Personnelles Client, de telles demandes seront satisfaites dans la mesure du possible, sous réserve des contraintes techniques et organisationnelles commercialement raisonnables, qui sont fonction du volume, de la catégorisation et de la quantité de Données Personnelles Traitées.

9.3. Les Données Personnelles Client restituées conformément à la procédure interne standard d'AMEN le seront sans frais pour le Client. À défaut, elles seront restituées moyennant des frais raisonnables pour le Client.

9.4. Si le Client opte pour la suppression des Données Personnelles Client, et sous réserve de l'article 9.5, AMEN fournira une déclaration attestant de ladite suppression.

9.5. AMEN pourra conserver les Données Personnelles Client, qui seront stockées en vertu d'opérations régulières de sauvegarde informatique conformément aux protocoles de reprise après sinistre et de continuité d'activité d'AMEN (voir article 12), à condition qu'AMEN ne Traite pas, et ne permette pas à ses Sous-Traitants Ultérieurs de Traiter, activement ou intentionnellement, de telles Données Personnelles Client pour des finalités autres que l'exécution du Service.

10. TRANSMISSIONS

10.1. Les Données Personnelles transmises par AMEN dans le cadre du Service par le biais d'Internet seront chiffrées de manière raisonnable. Les Parties reconnaissent toutefois que la sécurité des transmissions par Internet ne peut être garantie. AMEN ne sera pas responsable de l'accès du Client à Internet, de toute interception ou interruption de toute communication par Internet, ou des modifications ou pertes de Données Personnelles par Internet.

10.2. Si une Violation de Données Personnelles est suspectée, AMEN se réserve le droit de suspendre immédiatement l'utilisation par le Client du Service via Internet dans l'attente d'une investigation, sous réserve qu'AMEN notifie une telle suspension dès que raisonnablement possible, et prenne toutes les mesures raisonnables pour rétablir promptement l'usage du Service via Internet et pour coopérer avec le Client en vue de poursuivre la fourniture du Service via d'autres canaux de communication.

10.3. Le Client s'engage à prendre toutes les mesures adéquates et raisonnables qui sont nécessaires afin de préserver la confidentialité des noms et mots de passe de son personnel dans le cadre des Services. Le Client est responsable des conséquences de toute mauvaise utilisation du Service par un membre de son personnel.

11. VIOLATION DE DONNÉES PERSONNELLES

11.1 Le Client reconnaît et accepte qu'AMEN ne sera pas considérée comme responsable d'une Violation de Données Personnelles qui ne serait pas imputable à une négligence d'AMEN.

11.2 Si AMEN a connaissance d'une Violation de Données Personnelles, AMEN :

a) prendra les mesures appropriées pour contenir et atténuer une telle Violation de Données Personnelles, en ce compris en la notifiant au Client, dans les meilleurs délais, afin de lui permettre de mettre en œuvre rapidement son programme de réponse. Nonobstant ce qui précède, AMEN se réserve le droit de déterminer les mesures à prendre pour se conformer à la Législation Applicable sur la Protection des Données ou pour protéger ses droits et intérêts ;
b) coopérera avec le Client pour investiguer sur : la nature, les catégories et le nombre approximatif de Personnes Concernées qui ont été impactées, les catégories et le nombre approximatif d'enregistrements de Données Personnelles concernés et les conséquences probables d'une telle Violation de Données Personnelles, dans une mesure proportionnée à sa gravité et à son impact global sur le Client et sur la fourniture du Service dans le cadre du présent CTD ;

c) s'en remettra au Client et suivra ses instructions lorsque la Législation Applicable sur la Protection des Données exige la notification d'une telle Violation de Données Personnelles aux Autorités de Contrôle compétentes et aux Personnes Concernées impactées, dans la mesure où elle concerne les Données Personnelles Client, le Client ayant le droit exclusif de déterminer les mesures à mettre en œuvre en vue de se conformer à la Législation Applicable sur la Protection des Données ou de remédier à tout risque, en ce compris, mais sans limitation :

i. que la notification doive être transmise à des individus, organismes de régulation, autorités chargées de l'application des lois, agences d'études sur la consommation ou à d'autres entités, conformément aux exigences de la Législation Applicable sur la Protection des Données, ou à la discrétion du Client ; et

ii. le contenu de cette notification, si un quelconque type d'action correctrice peut être proposé aux Clients Personnes Concernées impactées, ainsi que la nature et l'étendue d'une telle action correctrice.

12. CONTINUITE DE L'ACTIVITE ET REPRISE APRES SINISTRE

12.1 AMEN met en œuvre des protocoles de reprise après sinistre et de continuité d'activité commercialement raisonnables, qui diffèrent selon chaque Service proposé. Une copie du résumé de ces protocoles est disponible sur demande par le Client, pour examen par ses soins. AMEN se réserve le droit de modifier ces protocoles à tout moment, sous réserve de ne pas réduire sa capacité de reprise après sinistre à un niveau inférieur à la capacité de reprise après sinistre en vigueur au titre du protocole applicable à la date de prise d'effet.

13. MANDAT

13.1 Par la signature du présent CTD, en ce compris les Annexes 1, 2 et 3, le Client mandate expressément AMEN en vue de la mise en œuvre, pour le compte du Client, des opérations décrites à l'article 5 ci-dessus.

13.2 Par la signature de ce CTD, AMEN accepte le mandat, qui sera exécuté sans rémunération financière dans la mesure où il est en lien avec le Service, et signifie légalement qu'AMEN a lu et compris les instructions qui lui sont données.

Le Client	AGENCE DES MEDIAS NUMERIQUES
Prénom et nom / nom de la société _____	
Code fiscal / n° de TVA intracommunautaire _____	N° TVA _____
Date et lieu _____	Date et lieu, _____
(Signature) _____	(Signature) _____

ANNEXE 1

1. PERSONNES CONCERNÉES

Les Données Personnelles Traitées se rapportent aux catégories de Personnes Concernées suivantes (cochez les cases correspondantes) :

☐ les clients et/ou les prospects

☐ les fournisseurs

☐ les salariés et/ou candidats au recrutement

☐ les conseils externes

☐ autres (à détailler ci-après) :

---

2. CATÉGORIES DE DONNÉES PERSONNELLES TRAITÉES DANS LE CADRE DE CHAQUE SERVICE

Les Données Personnelles Traitées concernent les catégories de Données Personnelles suivantes (cochez la case correspondantes) :

☐ données de contact (nom et prénom, adresse email, adresse postale, numéro de téléphone)

☐ date de naissance

☐ âge

☐ genre

☐ autre (à détailler ci-après) :

---

3. CATÉGORIES PARTICULIÈRES DE DONNÉES

Les Données Personnelles Traitées concernent les catégories particulières de Données Personnelles suivantes (cochez les cases correspondantes) :

☐ les handicaps et/ou les accidents

☐ les opinions politiques

☐ les convictions religieuses ou philosophiques

☐ la vie sexuelle ou l'orientation sexuelle en ce compris également les relations et liens conjugaux

☐ l'appartenance syndicale

☐ l'état de santé et/ou maladie

☐ les condamnations pénales

☐ Autre (à détailler ci-après) :

---

4. FINALITÉS DU TRAITEMENT

Les Données Personnelles peuvent être Traitées uniquement aux fins de fourniture du Service tel que décrit dans le Contrat-Cadre de Services.

5. NATURE DU TRAITEMENT

La nature des opérations de Traitement varie en fonction du Service spécifique activé au titre du Contrat-Cadre de Services.

6. FRÉQUENCE DU TRAITEMENT

La fréquence des opérations de Traitement varie en fonction du Service spécifique activé au titre du Contrat-Cadre de Services.

7. DURÉE DU TRAITEMENT

Les Données Personnelles Client seront conservées aussi longtemps que le Service restera actif.

ANNEXE 2

Description des mesures de sécurité techniques et organisationnelles

AMEN et/ou les Sous-traitants Ultérieurs s'engagent à mettre en place, au minimum, les mesures techniques et organisationnelles décrites ci-dessous.

1) MESURES ORGANISATIONNELLES

a. Politique de sécurité informatique
Les politiques de sécurité sont communiquées à l'ensemble du personnel. Elles sont réexaminées à la suite d'incidents et sont régulièrement mises à jour.

Une politique sur l'utilisation acceptable des actifs de l'entreprise et leur conservation est disponible.

b. Rôles et responsabilités en matière de sécurité
Les rôles en matière de sécurité ont été identifiés et formellement attribués, et sont toujours disponibles en cas de besoin ou d'incident.

La structure de ces rôles en matière de sécurité est réexaminée régulièrement.

Le personnel est informé que, pour des raisons de sécurité informatique, il doit contacter le personnel désigné, pour lequel il dispose d'un contact de référence.

c. Vérification des antécédents à l'occasion des entretiens et pour les nouveaux membres du personnel
Toute information fournie par les candidats est vérifiée pendant l'entretien.

d. Politiques de l'entreprise
Un membre du personnel est formellement chargé de vérifier la conformité interne aux politiques de l'entreprise et de les mettre à jour régulièrement.

e. Gestion des incidents et/ou des violations de données
Un système de gestion des informations et événements de sécurité (SIEM) a été mis en place pour détecter et signaler les anomalies.

Les incidents de sécurité sont gérés selon une procédure formalisée et mise à jour régulièrement.

Un registre des incidents a été établi. Il contient des informations relatives à la détection, l'analyse, la maîtrise, l'atténuation et la remise en état à la suite de chaque incident de sécurité.

À cette fin, un modèle est mis à disposition pour la rédaction de rapports relatifs aux incidents de sécurité. Ce modèle est conforme aux articles 33 et 34 du RGPD et fait l'objet de mises à jour régulières, le cas échéant.

Le personnel sait qui contacter en cas d'urgence.

Pour mesurer l'efficacité d'une réponse à un incident de sécurité, des exercices de cybersécurité sont réalisés et documentés.

f. Changements de personnel

Les nouveaux membres du personnel reçoivent une formation sur les processus et politiques de l'entreprise, en ce compris par le biais de procédures spécifiques destinées à accompagner la bonne compréhension de ces processus et politiques. L'attribution et la modification des autorisations d'un utilisateur sont effectuées par l'intermédiaire des groupes de domaine.

Les identifiants et les actifs des membres du personnel doivent être restitués lorsque la relation de travail prend fin ou que ces derniers n'en ont plus besoin, par le biais d'une procédure spécifique de révocation des identifiants et des actifs de l'entreprise, qui fait l'objet d'une révision régulière.

L'effectivité de la révocation des actifs ou identifiants des utilisateurs qui ne sont plus actifs fait l'objet d'un contrôle régulier.

g. Inventaire et surveillance des outils informatiques
Il existe une politique de gestion des actifs, qui est revue régulièrement.

Les systèmes critiques au sein du périmètre de l'entreprise ont été identifiés.

Les machines virtuelles et physiques sont initialisées avec une configuration de base, qui est mise à jour au fil du temps.

Une politique sur l'utilisation acceptable des outils électroniques est en vigueur. Cette politique inclut une procédure pour l'affectation et la restitution appropriées des actifs de l'entreprise.
Le stock réel des actifs restitués est vérifié régulièrement.

h. Continuité de l'activité
La continuité des services proposés - ou en tout état de cause des activités de l'entreprise - est assurée au moyen de plans d'urgence destinés à rétablir les activités de l'entreprise.

Une redondance de base a été mise en place pour la connectivité, l'électricité, les services et les données ; ces redondances en place sont cartographiées et régulièrement adaptées.

L'utilisation des ressources est surveillée et fait l'objet de projections afin de planifier une mise à l'échelle adéquate et d'éviter les goulets d'étranglement.

i. Gestion des modifications
Des politiques et procédures adéquates sont mises en place par l'entreprise pour apporter des modifications aux systèmes critiques, de telle sorte que leur mise en œuvre se déroule de manière prévisible et sécurisée.

En outre, elles sont fonction de l'importance critique des systèmes auxquels elles se rapportent.

Les modifications apportées sont documentées de manière adéquate et des outils automatisés sont utilisés pour la gestion des demandes de changement (RFC).

Les utilisateurs sont informés en cas de changements significatifs relatifs à leur expérience utilisateur.

j. Évaluation des vulnérabilités et tests de pénétration
Les logiciels et les systèmes font l'objet de tests appropriés avant d'être intégrés dans l'environnement de production, grâce à une procédure formalisée et à l'utilisation d'outils d'automatisation des tests.

L'installation et la désinstallation des correctifs et des restaurations (rollbacks) s'effectuent selon des procédures spécifiques, qui sont régulièrement revues.

Les données utilisées dans les bases de données de test sont régulièrement mises à jour.

Des balayages automatisés sont effectués à l'aide d'outils de recherche de vulnérabilités, ainsi que des sessions régulières d'évaluation des vulnérabilités et de tests de pénétration (VA/PT), selon un calendrier formellement établi.

Les sessions d'évaluation des vulnérabilités et de tests de pénétration génèrent de la documentation, qui est analysée et partagée avec toutes les autres fonctions de l'entreprise concernées, afin d'identifier d'autres vulnérabilités similaires dans les systèmes de l'entreprise et de procéder à leur élimination. Une formation spécifique à la sécurité est dispensée régulièrement.

Les points de contact uniques auprès des fabricants et des vendeurs de systèmes ont été identifiés.

k. Contrats avec les fournisseurs
Des contrats appropriés ont été signés avec les principaux fournisseurs de logiciels, de matériels et d'assistance connexe, incluant des engagements de niveaux de service et des exigences de sécurité.

Un modèle est utilisé pour solliciter des mesures de sécurité aux fournisseurs, et le droit d'effectuer des audits auprès des fournisseurs est maintenu.

l. Gestion des risques
Les méthodologies d'évaluation des risques ont été suivies et prennent en compte les menaces qui ont un impact sur la protection des données.

Une procédure d'analyse des risques a notamment été élaborée et est régulièrement mise à jour.
Les principaux risques et leurs mesures d'atténuation possibles ont été analysés : les mesures d'atténuation identifiées ont été mises en œuvre.

Ces opérations d'évaluation des risques sont renouvelées régulièrement.

m. Conformité
Le respect des normes et règlements est contrôlé au moyen de procédures spécifiques, qui sont réexaminées régulièrement.

Les audits et les évaluations sont planifiés à l'avance et en accord avec le personnel concerné, afin de minimiser l'impact sur les processus opérationnels.

n. Interopérabilité et portabilité
Un processus mis en place permet à la Personne Concernée de demander ses données dans un format interopérable, garantissant ainsi le droit à la portabilité.

o. Formation en matière de sécurité
Les salariés reçoivent régulièrement de la documentation sur les questions de sécurité ; en particulier, afin d'accroître leur sensibilisation à la sécurité, des plans de formation ont été préparés, avec un contenu personnalisé selon les rôles exercés par le personnel, et sont mis à jour régulièrement. Les connaissances du personnel en matière de sécurité sont contrôlées régulièrement.

À cet égard, les salariés peuvent entreprendre, par l'intermédiaire de l'entreprise, des opérations de certification en matière de sécurité.

p. Autorisation
Chaque personne autorisée à traiter des données reçoit des profils d'autorisation clairement définis.

Ces profils sont définis selon le principe de minimisation, et il est possible de lister les personnes autorisées affectées à une ressource donnée.

q. Supports amovibles
L'utilisation de supports amovibles est réglementée.

Les supports amovibles sont détruits avant d'être mis en décharge ou désinfectés avant d'être réaffectés.

2) MESURES TECHNIQUES

Les mesures de sécurité techniques appliquées au sein du périmètre de l'entreprise sont décrites ci-après.

Ces mesures, sauf indication contraire, doivent être considérées comme applicables à tous les outils et applications relevant du périmètre de l'entreprise.

a. Sécurité de l'approvisionnement de secours
Afin d'assurer la continuité des opérations, l'approvisionnement en carburant pour les groupes électrogènes terrestres et en batteries pour les alimentations électriques sans interruption est garanti.

À cet égard, des procédures de gestion du carburant et des batteries ont été élaborées et des contrats de fourniture spécifiques ont été prévus.
Ces procédures et contrats sont réexaminés en tant que de besoin.

b. Contrôle de l'accès aux réseaux et aux systèmes
L'authentification est gérée de manière centralisée. Tous les utilisateurs sont des personnes physiques et il est nécessaire de s'authentifier avant de traiter toute donnée personnelle.

Les utilisateurs sont associés à un ou plusieurs profils d'autorisation qui, à leur tour, sont attribués selon les principes du « besoin d'en connaître » (minimisation) et du moindre privilège.

L'efficacité des mécanismes d'accès est régulièrement réévaluée.

Le réseau est segmenté et les machines sont authentifiées avant d'autoriser l'accès au réseau.

c. Sécurité des données au repos
Les données critiques et les systèmes dans lesquels elles résident ont été identifiés.

Les données personnelles accessibles dans les systèmes de l'entreprise sont classées selon les catégories « communes », « particulières » et « judiciaires ». En outre, pour les différents types de données, des durées de conservation ont été définies.

Des procédures sont également prévues pour la suppression sécurisée des données au repos.

Tous les actifs ont été recensés et classés.

L'utilisation de dispositifs amovibles est réglementée. Ils sont soumis à des contrôles de sécurité avant leur utilisation et les données sur les supports de stockage amovibles sont chiffrées.

Il existe des procédures spécifiques pour l'élimination des actifs. En particulier, l'élimination des actifs est planifiée à l'avance, afin d'éviter la perte d'informations ou le ralentissement des opérations.

Le personnel est informé des dispositions relatives au chiffrement et de leurs justifications.

d. Sécurité de l'interface
Tous les utilisateurs ont un identifiant unique.

Toutes les interfaces utilisent des algorithmes de communication sécurisés et les mécanismes de protection adoptés pour assurer leur sécurité sont régulièrement réévalués.

e. Sauvegardes de sécurité et reprise après sinistre
Nous disposons d'un système de restauration des données et services en cas de sinistre.

Plus précisément, un ensemble de politiques sur les sauvegardes, leur conservation et leur sécurité ont été élaborées.

En particulier, la procédure de sauvegarde inclut un site de réplication externe contenant la sauvegarde par zone géographique de toutes les données et l'option de reprise après sinistre pour certains services.

f. Accès au centre de traitement des données et aux bureaux
Conformément à la loi, des précautions ont été prises pour lutter contre les incendies (portes coupe-feu, extincteurs, détecteurs de fumée, etc.), en consignant les procédures d'urgence correspondantes (par exemple, la lutte contre l'incendie).

Des dispositifs antivol et/ou de vidéo-protection sont opérationnels ; les conditions du centre de données (humidité, température, réglages du système de refroidissement, niveaux sonores, consommation d'énergie, etc.) sont constamment contrôlées, et le fonctionnement et l'efficacité des mesures environnementales mises en œuvre sont régulièrement vérifiés.

Une liste du personnel autorisé à accéder aux structures de l'entreprise a été établie.

Des registres d'accès des visiteurs ont été établis. Ils sont conservés et stockés selon un délai de conservation préétabli, avant d'être ensuite effacés ou détruits.

Les visiteurs sont authentifiés avant de pouvoir accéder au centre de traitement des données et/ou aux bureaux et sont toujours escortés/accompagnés au sein des locaux de l'entreprise.

g. Intégrité des réseaux et des systèmes
Les éléments suivants ont été mis en œuvre : anti-virus, anti-spam, système de gestion des informations et événements de sécurité (SIEM), pare-feu avec fonctionnalité IDS ou IPS.

La mise à jour et la gestion du logiciel anti-virus se font de manière centralisée.
Les salariés ne peuvent pas désactiver les mesures de protection sur leurs machines. Les éventuelles désactivations dues à des raisons organisationnelles sont contrôlées régulièrement.

Les entrées dans les applications et les interfaces sont correctement nettoyées.

Toutes les mesures de protection sont régulièrement mises à jour ou remplacées si nécessaire.

h. Systèmes de surveillance et d'enregistrement
Des outils de surveillance et de journalisation sont en place pour les systèmes identifiés comme critiques et pour les actions des utilisateurs finaux sur la plateforme, avec conservation des informations sur l'auteur de chaque action.

Ces outils déclenchent automatiquement des alertes s'il y a lieu et, à l'exception des actions des utilisateurs, génèrent des journaux complets et inaltérables, dont l'intégrité peut être vérifiée.

L'ensemble des machines qui doivent faire l'objet d'une consignation et d'une surveillance est régulièrement mis à jour.
Les règles de génération des alertes et la liste des informations à surveiller sont régulièrement mises à jour.

i. Exigences de sécurité (sécurité dès le stade de la conception) et directives sur l'écriture de code sécurisé
Nous utilisons des directives pour écrire du code sécurisé.

Des outils de gestion du cycle de vie du développement des systèmes (SDLC) sont utilisés ; les environnements de développement, de test et de production sont séparés et, en particulier, le passage en production s'effectue par le biais de procédures de test formalisées.

Les résultats des évaluations sont partagés avec les développeurs, afin d'améliorer leurs connaissances et de prévenir la récurrence de problèmes connus.

j. Authentification
Chaque personne autorisée à traiter les données est soumise à une procédure d'authentification rigoureuse avant de pouvoir accéder au traitement des données proprement dit : un mot de passe alphanumérique est requis, d'une longueur d'au moins huit (8) caractères, contenant des majuscules, des minuscules et des caractères spéciaux.

Les identifiants d'authentification sont individuels pour chaque personne autorisée à traiter des données.
Le mot de passe attribué à une personne autorisée à traiter des données est modifié par cette personne lors de la première utilisation et, par la suite, tous les trois (3) mois.

Les identifiants d'une personne autorisée à traiter des données sont signalés à un administrateur système si la personne autorisée ne les utilise pas pendant au moins quatre (4) mois.

En fonction de tout changement de poste de la personne autorisée, ses identifiants sont désactivés ou les profils d'autorisation qui lui sont attribués sont modifiés.

Un administrateur est autorisé à accéder, pour des raisons impérieuses de continuité des activités, aux données traitées par une personne autorisée qui est absente pendant une longue période, à condition de respecter la confidentialité du mot de passe de cette personne - s'il est utilisé - et d'informer promptement la personne absente de l'accès qui a eu lieu.

k. Sauvegarde des données et des appareils
Chaque personne autorisée à traiter des données protège tous les appareils qui lui sont attribués contre des détériorations accidentelles ou le vol, ainsi que ses sessions de traitement des données et la confidentialité de ses identifiants.

l. Systèmes de protection
Les systèmes matériels/logiciels de l'entreprise pris en charge par leurs fabricants sont constamment maintenus à jour.
Les systèmes de l'entreprise développés en interne sont conformes aux directives de protection des données dès la conception.
Des programmes de protection de pointe sont utilisés, tels que : anti-virus sur tous les postes de travail, pare-feu périmétrique, modules IDS/IPS actifs, pare-feu personnel.

m. Disponibilité des données
Toutes les données font l'objet d'une sauvegarde quotidienne par zone géographique.

n. Protection des données

Toutes les données personnelles sont transférées par voie électronique uniquement sous une forme chiffrée.

ANNEXE 3

Sous-Traitants Ultérieurs	Pays d'établissement	Opérations de Traitement
UBILIBET	Espagne	Fourniture de services Online Brand Protection (OBP) aux clients d'AMEN
AMEN NEDERLAND	Pays-Bas	Gestion de domaines
AMENWORLD	Portugal	Gestion de domaines
NAMESCO Inc.	Royaume-Uni	Gestion de domaines
NAMESCO IRELAND Inc.	Irlande	Gestion de domaines
NETWORK SOLUTIONS	États-Unis	Noms de domaine, conception de sites web, hébergement
ALNILAM	France	Services de télécommunication
REGISTER S.p.A.	Italie	• Gestion de centres de données ; • Gestion des cartes de crédit des clients (plateforme de facturation unique) ; • Gestion des services de serveur ; • Gestion des services de courrier électronique, d'hébergement, de sites web et de commerce électronique (dans le cadre de la gestion infrastructures du groupe) ; • Services d'assistance aux clients, incluant la gestion des demandes d'assistance, les retraits par carte de crédit, la gestion des demandes émanant des autorités compétentes ; • Services d'assistance aux clients pour accéder aux données de trafic à des fins d'audit interne ; • Assistance ponctuelle relative à tout chargement, modification, saisie et suppression de données (l'accès aux Données Personnelles n'est qu'occasionnel, à des fins d'assistance spécifique) ; • Refacturations, coûts du Directeur Général du groupe et de la direction du groupe, analyses statistiques ; • Administration et finances, gestion civile et fiscale de la comptabilité, rédaction du rapport financier ; • Coordination relative aux bénéfices et pertes, gestion des données du support administratif ;

		• Enregistrement et gestion des noms de domaine (REGISTER gère la plateforme technique du groupe pour les opérations relatives aux noms de domaine) ; • Lutte anti-fraude, consistant à recouper les informations recueillies sur le site Internet d'AMEN au moyen de cookies, d'empreintes digitales et de balises (e-tags) avec le code de facturation
NOMINALIA INTERNET S.L.	Espagne	Gestion de domaines Services d'assistance aux clients
AWIN AG	Allemagne	Services de publicité, génération de leads (prospects) en ligne
DUDA Inc.	États-Unis	Mise à disposition d'une plateforme pour héberger et fournir des sites aux clients d'AMEN
BASEKIT	Royaume-Uni	Services de développement de sites web
ePages GmbH	Allemagne	Services de construction de sites web de commerce électronique
LOGICA CONSULTING	Italie	Création de sites web
SITELOCK	États-Unis	Mise à disposition d'un système informatique pour l'évaluation de la présence de logiciels malveillants et la détection des attaques
WEBKORNER	Italie	Assistance technique et maintenance du matériel