CONTRAT POUR LES COMMANDES DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

Entre

Nom at adresse du client

("**Client**" / "**Responsable de traitement**")

Et

Emarsys SAS
67 Rue Anatole France
92300 Levallois Perret
Paris
France
("Prestataire" / "Sous-traitant")

1. PREAMBULE

En tant que contrat distinct et/ou sur la base de commandes particulières séparées ainsi que du MSA, conditions générales d'Emarsys, (ci-après désignés collectivement comme le **"Contrat-Cadre"**), le Prestataire doit fournir au Client des services marketing divers, et plus spécifiquement des services de planification, mise en œuvre, et analyse de la communication par e-mail (ci-après désignés collectivement les **"Services"**). Les Services sont détaillés dans le Contrat-Cadre et décrits pour chaque Service rattaché.

2. OBJET

2.1. Traitement de données à caractère personnel

Le présent contrat (« **Contrat** ») doit prendre en compte la règlementation en vigueur sur le traitement de données à caractère personnel dont le Prestataire réalise le traitement pour le compte du Client lors de la délivrance des Services (« **Données** »). Les données à caractère personnel consistent en toute information relative à une personne physique identifiée ou identifiable. Il s'agit notamment de noms, adresses e-mail, et les centres d'intérêts des destinataires des newsletters du Client ; Le Contrat-Cadre et la description des Services rattachés comportent plus de détails sur les catégories de données à caractère personnel et de personnes concernées.

2.2. Etendue du traitement

L'objet, la durée, la nature et la finalité du traitement des Données sont précisés dans le Contrat-Cadre et la description des Services rattachés.

3. OBLIGATIONS DU CLIENT (RESPONSABLE DE TRAITEMENT)

3.1. Le Client en tant que responsable de traitement

Le Client est le seul responsable de traitement sur les Données, et reste responsable de la licéité du traitement des Données et garant des droits des personnes concernées. Il revient donc au Client d'informer les personnes concernées et d'obtenir leur consentement au traitement de leurs Données, dans le respect des exigences de la règlementation en vigueur sur la protection des données.

3.2. Obligation d'indemnisation

Si un tiers (y compris une autorité étatique) émet une plainte contre le Prestataire et/ou accuse le Prestataire d'une violation du Contrat due à un manquement du Client à ses obligations, les dispositions suivantes s'appliquent, dans le plafond fixé aux conditions générales (MSA): sans délai, le Client s'engage à indemniser et à garantir le Prestataire contre toute réclamation, à fournir une assistance appropriée pour toute défense juridique, et également à indemniser et garantir le Prestataire de tous les coûts supportés par le Prestataire pour cette défense juridique. Cette obligation d'indemnisation est soumise à ce que le Prestataire informe le Client par écrit de ces réclamations dans les meilleurs délais, ne reconnaisse pas sa responsabilité ou fasse des déclarations en ce sens, et permette au Client, dans la mesure du possible compte tenu des contraintes procédurales, d'engager toutes les procédures judiciaires et extra-judiciaires à la charge du Client.

4. OBLIGATIONS DU PRESTATAIRE (SOUS-TRAITANT)

4.1. Respect des instructions

Le Prestataire, y incluant ses employés, doit uniquement traiter les Données dans le cadre de et aux fins de la délivrance des Services pour le Client and conformément aux instructions documentées du Client. Le Prestataire ne peut pas traiter les données à caractère personnel d'une autre manière ni à d'autres fins, sauf obligations légale née de l'UE ou du droit d'un Etat membre de l'UE auquel le Prestataire est soumis ; dans un tel cas, le Prestataire doit informer le Client de cette obligation légale avant le traitement à moins que la loi interdise une telle information pour un motif d'intérêt public.

4.2. Obligation de notification

Le Prestataire, s'il en a connaissance, informe le Client si, selon lui, une instruction constitue une violation des dispositions sur la protection des données à caractère personnel. Dans un tel cas, et en l'absence de réponse satisfaisante du Client, le Prestataire peut suspendre la mise en œuvre de ces instructions jusqu'à ce que ces instructions soient modifiées ou confirmées par le Client. Cependant, le Prestataire n'est pas obligé de vérifier que les instructions données par le Client sont conformes à la loi.

4.3. Obligation de fournir une assistance

Dans les limites de l'article 28 du Règlement Général sur la Protection des Données à caractère personnel n° 2016/679 et sur demande du Client, le Prestataire aide le Client par des mesures techniques et organisationnelles appropriées, compte tenu de la nature du traitement et des informations à la disposition du Prestataire. Le Client valider un devis préalable du Prestataire et prendre à sa charge les coûts engendrés par des demandes dépassant les obligations nées du Bon de commande.

4.4. Rectification, suppression, blocage

Lorsque les données du Client doivent être corrigées, supprimées ou bloquées, le Client procède lui-même à ces mesures en utilisant les fonctions adaptées du logiciel fourni. Lorsque cela n'est pas possible, le Prestataire corrige, supprime ou bloque ces données conformément aux instructions données par le Client, aux risques et aux frais du Client. L'article 7.2 s'applique lors de la suppression des Données à la fin du contrat.

4.5. Localisation du traitement

Les Données ne peuvent être traitées que dans l'Union Européenne (UE) et/ou dans les Etats membres de l'Espace économique européen (EEE), eu égard au fait que le Client n'a pas autorisé le Prestataire, par ce Contrat ou tout autre moyen, à traiter les données dans un pays qui n'est pas un Etat membre de l'UE ou de l'EEE.

4.6. Délégué à la protection des données

Les cocontractants désignent un Délégué à la protection des données, si la loi l'exige et en communique les coordonnées à l'autre partie sur demande.

4.7. Confidentialité des Données

Le Prestataire doit sensibiliser ses salariés impliqués dans le traitement des données à caractère personnel à la législation applicable à la protection des données, et doit déployer des efforts raisonnables pour obliger par écrit ces salariés à respecter le secret et la confidentialité des données. Cette obligation de secret s'applique spécifiquement aux personnes impliquées dans le traitement des données à caractère personnel et pour les données relatives aux entités juridiques ou association.

4.8. Obligation de notification

En cas de violation de données au sens de l'article 33 du RGPD, le Prestataire doit immédiatement en informer le Client.

4.9. Mesures techniques et organisationnelles

En prenant en compte l'état de la technologie, les coûts de mise en œuvre ainsi que la nature, l'étendue, le contexte, les finalités du traitement et les risques probables d'atteinte grave aux droits et libertés des individus, le Prestataire s'engage à mettre en place les mesures techniques et organisationnelles spécifiées en Annexe 1 du Contrat et le Client en choisissant le Prestataire, confirme qu'il s'agit de garanties suffisantes au sens du RGPD.

4.10. Assurance

Le Prestataire peut être assuré pour la durée du Contrat en cas d'action en responsabilité résultant de et en relation directe avec ce Contrat.

4.11. Obligation d'indemnisation

Si un tiers (y compris une autorité étatique) émet une plainte contre le Prestataire et/ou accuse le Prestataire d'une violation du Contrat due à un manquement du Client à ses obligations, les dispositions suivantes s'appliquent, dans le plafond fixé aux conditions générales (MSA): sans délai, le Client s'engage à indemniser et à garantir le Prestataire contre toute réclamation, à fournir une assistance appropriée pour toute défense juridique, et également à indemniser et garantir le Prestataire de tous les coûts supportés par le Prestataire pour cette défense juridique. Cette obligation d'indemnisation est soumise à ce que le Prestataire informe le Client par écrit de ces réclamations dans les meilleurs délais, ne reconnaisse pas sa responsabilité ou fasse des déclarations en ce sens, et permette au Client, dans la mesure du possible compte tenu des contraintes procédurales, d'engager toutes les procédures judiciaires et extra-judiciaires à la charge du Client.

5. LE DROIT DU CLIENT DE PROCEDER A DES AUDITS

5.1. Certification

Le Prestataire s'engage à utiliser un système de gestion de sécurité de l'information certifié ISO 27001 pendant toute la durée du Contrat, et d'en justifier sur demande du Client.

5.2. Audits

Le Client peut prendre des mesures raisonnables pour auditer (ou faire auditer le Prestataire par un tiers mandaté par le Client sous réserve que ce tiers ne soit pas un concurrent direct ou indirect du Prestataire) le respect par le Prestataire a) de la législation relative à la protection des données, b) des dispositions contractuelles des Parties et c) des instructions du Client. Le Prestataire doit contribuer à de tels audits et permettre l'accès du Client aux informations nécessaires pour démontrer sa conformité. Le Client doit avertir le Prestataire par écrit au moins deux semaines avant la réalisation d'un audit dans les locaux du Prestataire. Les audits doivent être effectués par le Client pendant les heures normales de bureau et ne pas entraîner d'importantes perturbations de l'activité du Prestataire. Les frais d'audits et liés aux audits effectués par le Client sont à la charge du Client.

5.3. Coûts

Les frais d'audits et liés aux audits effectués par le Client sont à la charge du Client. Ceci inclut également une rémunération compensatoire des employés du Prestataire mobilisés par l'audit.

5.4. Intérêts légitimes du Prestataire

Lorsqu'un audit peut conduire à la divulgation de secrets d'affaires ou de secrets commerciaux du Prestataire ou menacer les droits de propriété intellectuelle du Prestataire, le Client doit faire appel à un expert, tiers indépendant qui est tenu à l'obligation de secret et de confidentialité concernant le Prestataire.

6. SOUS-TRAITANCE

6.1. Recours à des sous-traitants

Le Prestataire est autorisé par le Client à avoir recours à des sous-traitants pour l'exécution de ses obligations contractuelles, y incluant le traitement des Données, sous réserve que le Prestataire ait conclu un accord écrit ou électronique avec le sous-traitant garantissant un niveau de protection adéquate ou supérieur au niveau prévu par le Contrat et, sur demande du Client que cet accord lui soit communiqué. Le Prestataire doit informer le Client de toute modification envisagée relative à l'ajout ou au remplacement d'un sous-traitant, étant entendu que le Client peut émettre des objections à une telle modification.

6.2. Sous-traitants agréés

Au-delà de l'agrément général prévu ci-dessus, le Client accepte expressément les sous-traitant listés en Annexe 2.

6.3. Responsabilité du Prestataire en cas de défaillance d'un sous-traitant

Quand un sous-traitant ne remplit pas ses obligations contractuelles en matière de protection des données, le Prestataire reste responsable vis-à-vis du Client, de l'exécution des obligations contractuelles par le sous-traitant.

7. FIN DU CONTRAT

7.1. Terme

Le Contrat est automatiquement résilié 30 jours à compter de la fin du Contrat-Cadre.

7.2. Sort des Données au terme du Contrat

Le Prestataire doit supprimer les Données du Client de son support de stockage et détruire la documentation associée dans les 30 jours suivants le terme du Contrat-Cadre et donc le bon paiement des sommes dues ; sauf obligation légale de conservation des Données par le Prestataire. Seul le Client est responsable d'exporter les Données à son rythme avant la fin de la période de 30 jours et de les sauvegarder pour les réutiliser. Tout transfert ou exportation des Données qui ne peut pas être effectué(e) par les fonctions standards du logiciel devra être commandé(e) au Prestataire en temps utile et donne lieu à une facturation complémentaire du Client par le Prestataire (par exemple fichiers téléchargeables).

7.3. Copies de sauvegarde

L'obligation de supprimer les données conformément à l'article ci-dessus ne s'applique pas aux données contenues dans les copies de sauvegarde régulières de l'ensemble complet des données, lorsque la suppression individuelle des données du Client demanderait des efforts trop importants pour le Prestataire et dès lors que les données du Client sont automatiquement supprimées ou remplacées après un maximum de 14 jours dans le cadre du cycle de sauvegarde que le Prestataire met en œuvre. Jusqu'à suppression automatique ou remplacement des données, toute restauration ou autre utilisation de ces copies de données postérieures au terme du Contrat est interdite. Le Client peut demander au Prestataire de supprimer ces copies de sauvegarde à condition que le Client s'engage à rembourser au Prestataire tous les frais engagés dans ce processus, y compris une compensation liée au temps de travail passé par le personnel du Prestataire.

8. DISPOSITIONS DIVERSES

8.1. Loi applicable

Le contrat est exclusivement régi par la loi française (excluant toute convention internationale).

8.2. Juridiction compétente

SAUF DISPOSITIONS D'ORDRE PUBLIC CONTRAIRES OU MENTION CONTRAIRE AU CONTRAT CADRE, LES PARTIES ACCEPTENT DE SOUMETTRE TOUS LITIGES LIES AU PRESENT ACCORD ET A SON INTERPRETATION AUX JURIDICTIONS RELEVANT DU LIEU DU SIEGE SOCIAL D'EMARSYS.

8.3. Invalidité partielle

Si tout ou partie de certaines dispositions du Contrat sont ou deviennent non valables, les autres clauses du Contrat n'en sont pas affectées. Les Parties remplaceront la disposition non valable par une disposition de remplacement convenue par les Parties conformément à leurs intentions économiques initiales. Ce principe s'applique également en cas d'éventuelles omissions dans le Contrat.

Client / Responsable de traitement :		**Prestataire / Sous-traitant :**	**Emarsys SAS**
Signature :		**Signature :**	
Nom :		**Nom :**	Josef Draxler
Fonction :		**Fonction :**	General Manager
Lieu / date :		**Lieu et date :**	7 Mai, 2018

ANNEXE 1 : MESURES TECHNIQUES ET ORGANISATIONNELES POUR ASSURER LA SECURITE DES TRAITEMENTS

1. PSEUDONYMISATION ET ENCRYPTAGE DES DONNEES A CARACTERE PERSONNEL

Mesures qui sont généralement prises pour se prémunir contre un accès non autorisé aux traitements de données à caractère personnel :

- Les données à caractère personnel sont encryptées pour tout transfert.
- Dans la mesure du possible (sans altérer la délivrabilité du service souscrit) les données à caractère personnel sont anonymisées et/ou pseudonymisées par hachage ou référence à une base de données où les données à caractère personnel sont conservées.

2. CAPACITE A GARANTIR LA CONFIDENTIALITE, L'INTEGRITE, LA DISPONIBILITE ET LA RESILIENCE CONSTANTES DES SYSTEMES ET DES SERVICES DE TRAITEMENT

CONTROLE PHYSIQUE DES ACCES

Les mesures suivantes empêchent les tiers non autorisés à accéder physiquement à l'équipement de traitement des données utilisé pour les données à caractère personnel.

- Mise en place d'un contrôle d'accès physique
  - Le bâtiment est construit de telle manière à assurer une protection convenable de la zone en question.
  - Tous les points d'accès potentiels ont été protégés contre les accès non autorisés.
  - Les moyens actuels d'authentification d'accès (carte-clé ou puce) doivent être utilisés par tous.
  - Il est mis en place un système de contrôle d'accès physique.
- Gestion et documentation de l'accès physique autorisé individuellement :
  - Il est mis en place une politique organisationnelle régissant les autorisations d'accès aux zones opérationnelles dans les locaux de l'entreprise.
  - L'attribution de clefs est documentée.
- Surveillance des visiteurs et du personnel externe :
  - Il est mis en place une politique de contrôle des visiteurs et du personnel externe (accompagnement sur les lieux, passes pour les visiteurs temporaires, enregistrement de ces visites, etc.)
  - Il existe une politique de surveillance du personnel de maintenance (accompagnement sur les lieux, notifications préalables, contrôles d'identité, etc.)

CONTROLE DE L'ACCES AU SYSTEME

Les mesures suivantes empêchent les tiers non autorisés à utiliser les systèmes de traitement de données (y compris les méthodes de cryptage) :

- Le contrôle d'admission (authentification) :
  - Tous les systèmes de traitement de données ont un mécanisme d'authentification d'utilisateur opérationnel.
  - La mise en œuvre correcte de ces mesures (authentification) est contrôlée.
  - Un générateur de mots de passe aléatoires est utilisé.
- Transmission sécurisée de données d'authentification (identifiants de connexion) sur le réseau :
  - La transmission de données d'authentification (identifiants de connexion) sur le réseau est effectuée sous forme cryptée.
- Blocage après des tentatives infructueuses/inactivité et processus de déblocage :
  - Il existe une méthode sûre pour débloquer l'accès, par exemple l'attribution d'un nouveau nom d'utilisateur.
- Interdiction de mots de passe et de formulaires d'entrée stockés localement :
  - Les mots de passe d'accès et/ou les formulaires d'entrée ne sont pas conservés sur le Client ou dans son environnement (par exemple dans le navigateur ou sur un Post-it).
  - Les utilisateurs ont été informés de l'interdiction de cette pratique.
- Politique d'autorisation :
  - Il est mis en place un concept de rôle (profils d'utilisateur prédéfinis).
  - Les droits d'admission sont toujours accordés à des particuliers (c'est-à-dire à une personne en particulier).
  - Le nombre de personnes autorisées est réduit au minimum strictement nécessaire pour conduire une opération commerciale normale.
- Gestion et documentation des médias d'authentification personnelle et des droits d'admission :
  - Il est mis en place un process documenté et correctement mis en œuvre qui couvre la mise en place, l'autorisation, l'attribution et le retrait des médias d'authentification et des droits d'admission.
  - Une personne responsable de l'attribution des droits d'admission doit être nommée.
  - Un process de délégation a été mis en place dans le cas où la personne responsable serait indisponible.
- Blocage d'accès automatique :
  - Si un poste de travail ou un terminal a été inactif pendant plus de 30 minutes, un écran de veille protégé par mot de passe est activé automatiquement via les mécanismes du système d'exploitation.
- Blocage d'accès manuel :
  - Il est mis en place une politique qui précise que pendant les absences temporaires, les postes de travail et les terminaux doivent être protégés contre toute utilisation non autorisée, par exemple, via une activation automatique ou manuel de l'écran de veille protégé par mot de passe.
  - Les salariés doivent recevoir une formation et être sensibilisés à la nécessité d'appliquer correctement les mesures décrites ci-dessus.

CONTROLE DE L'ACCES AUX DONNEES

Les mesures suivantes permettent de s'assurer que les personnes autorisées à utiliser un système de traitement des données peuvent seulement accéder aux données relevant de leur autorisation d'accès, et que lors du traitement et de l'utilisation des données, ainsi qu'après le stockage des données, les données à caractère personnel ne peuvent pas être lues, copiées, modifiées ou supprimées sans autorisation (y compris les méthodes de chiffrement) :

- Le système d'autorisation / la mise en œuvre des restrictions d'accès :
  - Il existe des lignes directrices pour la création, la modification et la suppression des profils d'accès.
  - Les utilisateurs autorisés ne peuvent accéder qu'aux données dont ils ont besoin pour la bonne exécution de la tâche à accomplir, et comme spécifié dans les profils d'autorisation individuelle.
  - Si une base de données contient des données appartenant à plus d'un Client, ou si les données de plus d'un Client sont en cours de traitement dans le même système de traitement de données, une restriction d'accès logique a été mise en œuvre pour limiter le traitement aux données du Client concerné (capacité multi-client).
- Gestion et documentation de l'accès physique autorisé individuellement :
  - Un process qui couvre la mise en place, l'autorisation, l'attribution et le retrait des autorisations d'accès a été mis en place.
  - Les autorisations sont liées à un nom d'utilisateur personnel et à un compte.
  - Si la base sur laquelle l'autorisation a été accordée ne s'applique plus (par exemple un changement de fonction), l'autorisation est immédiatement retirée.
- Enregistrement de l'accès aux données :
  - Toutes les opérations de lecture, d'entrée, de modification et de suppression sont enregistrées.
  - Pour la détection d'une mauvaise utilisation, des évaluations sont régulièrement effectuées de manière aléatoire.

CONTROLE DES TRANSFERTS

Les mesures suivantes permettent d'assurer que les données personnelles ne peuvent pas être lues, copiées, modifiées ou supprimées par des tiers non autorisés pendant la transmission électronique, le transport ou le stockage sur un support de données, et qu'il peut être vérifié et déterminé vers quels sites une telle transmission de données à caractère personnel est prévue et effectuée (y compris les méthodes de chiffrement) :

- Enregistrement :
  - Les sites d'émission et de réception sont enregistrés
  - Les deux sites sont précisément décrits et documentés ; tous les salariés concernés ont connaissance de ces indications.
- Transmission des données sécurisée entre le serveur et le client :
  - La transmission des données entre le serveur et le client est effectuée sous forme cryptée (SSL or SSH or SFTP or VPN).
- Transmission au back-end :
  - La connexion au système de back-end est sécurisée
  - Les données qui exigent un degré de protection élevé sont cryptées
- Réduction des risques par la segmentation du réseau :
  - Une segmentation du réseau est en place et garantit que la transmission des données s'effectue par l'intermédiaire d'un nombre réduit d'éléments de réseau.
  - Un diagramme du réseau a été mis en place.
  - Le système concerné se trouve dans une zone démilitarisée.
- Passerelles de sécurité aux points d'interconnexion du réseau :
  - Des pare-feux sont installés aux points d'interconnexion du réseau
  - Les pare-feux sont activés en permanence.
  - Les pare-feux ne peuvent pas être désactivés par un utilisateur.
- Renforcement des systèmes de back-end :
  - Les comptes et mots de passe prédéfinis ont été désactivés.
  - Il existe des directives indiquant le comportement à adopter lorsqu'un détournement est suspecté
  - Une protection anti-virus mise à jour est en place.
- Description de toutes les interfaces et champs de données personnelles devant être transmis :
  - Il existe une description documentée de l'interface.

- Il existe des instructions quant à la procédure de transmission à suivre.
- Il existe une description de tous les champs de données personnelles devant être transmis.

- Authentification homme-machine :
  - L'authentification mutuelle se fait via un procédé cryptographique.
- Accès à des caches locaux :
  - Tout accès à un(e) potentiel(le) cache local ou base de données contenant les données de consommateurs d'un client, via des applications que le client n'a pas expressément approuvées, a été bloqué par des moyens techniques.
- Un transfert de données personnelles ne peut et ne pourra pas être effectué par voie postale.
- Processus de collecte et de destruction :
  - Il est mis en place une politique de destruction des supports de données conforme à la règlementation en matière de protection des données.
  - Il est mis en place une politique de destruction des documents conforme à la règlementation en matière de protection des données.
- Procédure de suppression/destruction conforme à la règlementation en matière de protection des données :
  - Avant que les supports de données ne soient réutilisés par d'autres utilisateurs, ceux-ci sont vidés/supprimés d'une manière qui est conforme à la règlementation sur la protection des données ; une récupération des données supprimées est rendue impossible ou exigerait du temps, des moyens disproportionnés et des efforts excessifs.
  - Les composants ou les documents matériels sont détruits de manière à ce que la récupération soit impossible ou exigerait du temps, des moyens disproportionnés et des efforts excessifs.

ACTEUR DES CONTROLES

Les mesures suivantes permettent d'assurer qu'il est possible de vérifier et de déterminer si et par qui les données personnelles ont été saisies, modifiées ou retirées des systèmes de traitement des données (contrôle du traitement) :

- Il existe une documentation indiquant les personnes qui, en raison de leur fonction et de leur rôle, ont l'autorisation et la responsabilité d'accéder, de modifier et de supprimer des données personnelles dans le système de traitement de données.

CONTROLE DE CONFORMITE AU COURS DES COMMANDES

Les mesures suivantes permettent d'assurer que les données personnelles qui sont traitées pour le compte d'un client ne peuvent être traitées que conformément aux instructions du client (contrôle du contrat) :

- Seul le Client est autorisé à gérer les commandes au sein du système.
- Exécution des obligations de contrôle :
  - Le Prestataire doit assister le Client pour la réalisation des obligations de contrôle.
  - Tous les incidents doivent faire l'objet d'un rapport au client.
  - Le Prestataire doit informer tous ses salariés de leur obligation de participer au rapport de tels incidents.
- Enregistrement de l'exécution des commandes par le Prestataire :
  - Il existe des documents qui assurent la traçabilité complète de toutes les étapes de travail nécessaires pour l'exécution d'une commande. Sur demande, il peut être apporté la preuve qu'une commande a été exécutée en totale conformité avec les instructions du client (information minimum : client/consommateur, action/objet de la commande, détail des étapes de travail/paramètres du process, salarié en charge du traitement, dates, destinataire/ si applicable).

3. CAPACITY A RESTAURER LA DISPONIBLITE ET L'ACCES AUX DONNES A CARACTERE PERSONNEL DANS UN TEMPS SUFFISANT EN CAS D'ATTEINTE PHYSIQUE OU TECHNIQUE

CONTROLE DE LA DISPONIBILITE

Les mesures suivantes permettent d'assurer que les données personnelles sont protégées contre la destruction ou la perte accidentelle (contrôle de la disponibilité).

- Procédure de sauvegarde :
  - Il est mis en place une procédure de sauvegarde.
  - Les sauvegardes sont effectuées régulièrement.
  - Une personne responsable de la sauvegarde ainsi qu'un remplaçant ont été désignés.
  - Il doit être régulièrement vérifié qu'une sauvegarde peut être restaurée.
- Plan d'urgence :
  - Il est mis en place un plan d'urgence qui détaille toutes les mesures nécessaires ainsi que les personnes, en particulier du côté Client, qui doivent être informées en cas d'incident.
- Contrôle des installations d'urgence :
  - Les générateurs électriques de secours et les systèmes de protection contre les surtensions sont régulièrement contrôlés et les paramètres d'exploitation doivent être surveillés en permanence.

LIMITATION A L'USAGE

Les mesures suivantes permettent de s'assurer que les données qui ont été recueillies pour des finalités différentes peuvent être traitées séparément :

- Les données appartenant à différents clients du Prestataire sont stockées dans des fichiers séparés et des répertoires distincts, qui ne sont ni groupés ni fusionnés.

4. PROCEDURES REGULIERES DE TEST, ANALYSE ET EVALUATION DE L'EFFECTIVITE DES MESURES TECHNIQUES ET ORGANISATIONNELLES POUR ASSURER LA SECURITE DES TRAITEMENTS

CONTROLE ORGANISATIONNEL

- Définition et contrôle du traitement :
  - Il existe des instructions de traitement
  - Pour le traitement des données au sein de l'entreprise, les traitements et flux de travail ont été déterminés.
  - La mise en œuvre et le respect de ces traitements sont contrôlés.
- Formation/obligation :
  - Principes de protection des données, comprenant les mesures techniques et organisationnelles.
  - Obligation de secret pour ce qui relève du secret d'affaires, notamment toutes les opérations effectuées par le Client.
  - Manipulation correcte et attentive des données, fichiers, supports de données et autres types de documentation.
  - Les formations sont documentées.
  - Des formations sont régulièrement dispensées, au moins tous les trois ans.
- Formation/obligation pour les intervenants extérieurs :
  - Les intervenants extérieurs ne se verront accorder l'accès aux systèmes de traitement des données qu'après avoir été informés, formés et s'être engagés par écrit au secret des données et, le cas échéant, au secret des télécommunications et autres obligations de secret.
- Répartition interne des tâches :
  - Les fonctions opérationnelles et administratives ont été séparées.
- Système de remplacement :
  - Un remplaçant a été désigné pour toutes les tâches et fonctions importantes de l'entreprise.

ANNEXE 2 : SOUS-CONTRACTANTS

Sous-contractant	Services des sous-contractants
Emarsys eMarketing Systems AG **Märzstraße 1** **1150 Vienne** **L'Autriche**	Développement et approvisionnement de la plateforme marketing.
Emarsys Technologies Kft **Kossuth Lajos utca 7-9** **First Site Hotel & Business Complex Floor 2** **1053 Budapest** **Hongrie**	Développement et approvisionnement de la plateforme marketing.
Emarsys Interactive Services GmbH **Stralauer Platz 34** **10243 Berlin** **Allemagne**	Services d'agence liés à la planification, l'exécution et l'analyse de la communication marketing.
Emarsys UK Ltd **Focus Point** **21 Caledonian Road** **Londres** **N1 9DX** **Royaume-Uni**	Support client.
LINFORGE Technologies GmbH **Brehmstraße 10** **1110 Vienne** **L'Autriche**	Partenaire de service pour l'administration du système opérationnel.
CloudAMQP / 84codes AB **Sveavägen 98** **113 50 Stockholm** **Suède**	Le courtage de message conçu comme un service.
CDNetworks Europe, Co. Ltd. **85 Gresham St** **Londres** **EC2V 7NQ** **Royaume-Uni**	Réseau de livraison de contenu.
Heroku, Inc. **The Landmark @ 1 Market St.** **Suite 300** **San Francisco, CA 94105** **USA**	La plateforme conçue comme un service. Tout le traitement des données personnelles est effectué au sein de l'union européenne.
Google LLC **1600 Amphitheatre Parkway** **Mountain View, CA 94043** **USA**	Moteur de stockage de données. Tout le traitement des données personnelles est effectué au sein de l'union européenne.
Compose / IBM Corp. **1 New Orchard Road** **Armonk, New York 10504-1722** **USA**	La base de données conçue comme un service. Tout le traitement des données personnelles est effectué au sein de l'union européenne.