DIGITAL MARKETING ADDENDUM

1. PORTEE

La présente Annexe s'applique à l'utilisation de Logiciels MAPP, en particulier, mais sans s'y limiter, à Digital Marketing Center (DMC) de MAPP, à des fins de marketing numérique, en particulier, mais sans s'y limiter, à des fins de marketing direct numérique par le biais de messages électroniques et pour les Envois en général. Cette Annexe doit être lue conjointement à l'Accord entre le Client et MAPP.

2. DÉFINITIONS

2.1 « Adresse » désigne une adresse électronique, un numéro de téléphone portable ou toute autre information d'adresse ou tout numéro de télécopieur permettant d'envoyer des Messages à l'aide des Logiciels.

2.2 « Jour ouvré » désigne une journée travaillée autre qu'un samedi, dimanche ou jour férié au siège social de MAPP.

2.3 « Délivrabilité » désigne la capacité à livrer des messages électroniques aux boîtes de réception des destinataires et à éviter que les messages soient perdus, bloqués ou dirigés vers le dossier spam.

2.4 « Adresse IP » désigne l'adresse de protocole Internet attribuée aux serveurs de courrier utilisé pour les Envois.

2.5 « FAI » désigne les fournisseurs de services de webmail et de courrier électronique, tels que HoMappil, Gmail, etc.

2.6 « Liste » désigne une liste d'adresses réellement utilisée ou destinée à être utilisée pour les Envois via le Logiciel.

2.7 « Message » désigne un message électronique (y compris, mais sans s'y limiter, un message de courrier, un SMS/MMS, un message push, un message d'application, un message instantané, un message, une publication ou une notification sur une plate-forme de réseau social) ou un message de télécopie.

2.8 « Données personnelles » désigne toute information concernant une personne physique identifiée ou identifiable tel que défini par la législation en vigueur sur la protection des données.

2.9 « Rebond rejeté » désigne les informations de rétroaction émanant d'un serveur de messagerie dont l'adresse à laquelle un message électronique a été envoyé n'existe pas ou est désactivé de façon permanente.

2.10 « Envoi » désigne l'envoi/la diffusion d'un message par le biais du Logiciel.

2.11 « Plainte pour spam » désigne le message qu'envoie un FAI pour informer MAPP qu'un message électronique envoyé par le biais du Logiciel a été marqué comme « pourriel » ou « spam » par le destinataire.

3. DISPONIBILITÉ ET UTILISATION DE DMC

3.1 Le système DMC du client est fourni dans un sous-domaine délégué par le Client (par ex. news.customer.com). Le Client doit déléguer le sous-domaine à MAPP et fournir toutes les informations et coopérer en vue de la configuration du système au moins cinq (5) jours ouvrables avant la configuration prévue du système.

3.2 Le transfert des données en clair peut mettre en danger la confidentialité de celles-ci. Ainsi, les données transférées à MAPP en vue de leur importation dans DMC doivent être envoyées par le biais d'une connexion sécurisée (sFTP, par ex.). MAPP se charge seulement de stocker les données fournies par le Client dans l'environnement DMC sécurisé. Par sécurité, les données fournies par le biais de serveurs FTP/sFTP sont supprimées de ceux-ci régulièrement.

3.3 Le stockage des informations et des rapports relatifs aux envois nécessite de grandes capacités de stockage dans l'environnement DMC. Les informations et rapports sont donc archivés 12 mois après l'Envoi spécifique et ne sont plus directement accessibles par le biais de DMC. MAPP doit récupérer les sauvegardes et les informations archivées soumises à l'application des tarifs horaires en vigueur. Les images et graphiques intégrés aux Messages ainsi que les pièces jointes sont supprimés 6 mois après la date de l'Envoi.

3.4 Toutes les données hébergées et traitées par MAPP pour le compte du Client sont supprimées du système DMC du Client immédiatement à la demande du Client et à l'expiration de l'Accord. La suppression de données sur le système DMC n'affecte pas les données des sauvegardes système DMC. En cas d'expiration de l'Accord, le Client doit télécharger/exporter ses données à partir du système DMC avant la date effective d'expiration. Une fois l'Accord arrivé à expiration, le Client ne pourra plus accéder à son système DMC. Le Client est responsable du respect de la conformité concernant les obligations et exigences de conservation. MAPP n'a pas l'obligation de stocker ou de conserver les enregistrements au nom du Client.

3.5 MAPP a le droit d'analyser les Envois du Client sous une forme agrégée/anonyme et d'utiliser ces analyses pour la maintenance et l'amélioration de DMC et à des fins statistiques, pour les études de marché et les publications (par ex., pour déterminer le taux d'ouverture moyen de bulletins électroniques dans le secteur de la grande consommation). Le Client ne sera pas identifié dans de telles publications.

4. POLITIQUE DE CONFORMITÉ

4.1 Le Client doit se conformer à l'ensemble des lois, règlements et normes de meilleures pratiques de l'industrie dans le cadre de l'utilisation du Logiciel, notamment son traitement des données personnelles par l'intermédiaire de DMC, le transfert d'Envois via DMC et son utilisation de services connexes comme l'hébergement de sites/de pages d'accueil. Le Client est responsable de l'identification et de l'interprétation des lois, règlements et normes de meilleures pratiques de l'industrie qui affectent l'utilisation de DMC par le Client et les prestations de services MAPP pour et/ou au nom du Client. Le Client doit garantir la conformité avec de telles exigences.

4.2 MAPP n'est pas tenue de fournir DMC aux clients qui effectuent des Envois qui sont non conformes aux lois, règlements et normes des meilleures pratiques de l'industrie et/ou n'est pas tenue de traiter ces Envois.

4.3 Les Messages commerciaux/marketing tels qu'ils sont définis par les lois, règlements et normes de meilleures pratiques de l'industrie ne peuvent être envoyés via DMC que si le destinataire a consenti à recevoir le Message commercial/marketing ou si l'envoi du Message commercial/marketing est conforme par ailleurs aux lois et règlements applicables, en particulier à ceux qui se rapportent à la protection des données et au commerce équitable et aux normes de meilleures pratiques applicables dans l'industrie. Le consentement du destinataire, si nécessaire, doit se conformer aux exigences légales en matière de forme et de contenu et être documenté et vérifiable conformément aux lois, règlements et normes de meilleures pratiques de l'industrie. Le caractère commercial de Messages commerciaux/marketing ne doit pas être travesti ou caché.

4.4 Les Messages commerciaux/marketing doivent contenir les coordonnées du client conformément aux lois, règlements et normes de meilleures pratiques industrielles en vigueur et ils doivent contenir un lien de désabonnement ou tout autre moyen de contact approprié pour que les destinataires renoncent à recevoir les messages et/ou annulent leur abonnement à des messages commerciaux/marketing ultérieurs. Les désinscriptions soumises par le biais de la fonction de désabonnement DMC intégrée seront traitées automatiquement et l'adresse concernée sera exclue des Envois futurs. Les autres processus de désabonnement fournis par le Client ne doivent pas être trop compliqués. Les désinscriptions reçues directement par le Client doivent être traitées dans un délai de (3) trois jours ouvrés. Le Client doit s'assurer que tous les messages destinés à l'adresse de l'expéditeur et à l'adresse de réponse mentionnées sont traités immédiatement. Si un Message envoyé par le biais de DMC est marqué en tant que « pourriel » ou « spam » par le destinataire (appelé « boucle de rétroaction »), certains FAI en informeront MAPP. DMC assimilera un tel marquage à un désabonnement, ce qui écartera l'Adresse correspondante de tout nouvel Envoi.

4.5 Dans le cas où un Message envoyé par le Client (i) conduit à une plainte d'un destinataire de MAPP, (ii) conduit à une mise à l'index (liste noire) par une organisation anti-spam (comme Spamhaus ou Spamcop) ou (iii) si MAPP reçoit une plainte ou une requête par une autorité de contrôle ou de réglementation ou toute association pertinente (comme les associations de marketing direct ou les associations de défense des consommateurs), le Client doit, à la première demande de MAPP et dans un délai d'un jour ouvré, fournir les éléments prouvant la légalité de l'Envoi concerné. MAPP est le droit de divulguer ces éléments de preuve à des tiers si besoin et dans la mesure nécessaire.

4.6 Le Client ne doit pas (i) envoyer, enregistrer, lier ou fournir de quelque manière que ce soit du contenu pornographique, sexuellement suggestif, menaçant, insultant, harcelant, diffamatoire, frauduleux, vulgaire, obscène, extrémiste ou faisant l'apologie de la violence, ou empiétant sur les droits individuels et ne doit pas contrevenir aux lois de la protection des mineurs ou encourager la violation des lois, (ii) envoyer, enregistrer ou fournir de quelque manière que ce soit du contenu qui viole les droits des tiers, y compris, mais sans limitation, les droits des marques commerciales ou autres, les droits d'auteur, les brevets, les dessins et les modèles d'utilité et les secrets commerciaux, ni (iii) envoyer, enregistrer, lier tout logiciel malveillant (tel que les virus) ou renvoyer à un logiciel malveillant.

4.7 DMC offre de nombreuses caractéristiques et fonctionnalités (telles que le suivi de la campagne, les profils utilisateur et le ciblage comportemental ou géographique). L'utilisation de ces caractéristiques et fonctionnalités peut nécessiter la notification ou le consentement préalable de la personne concernée. Le Client doit s'assurer que toutes les caractéristiques et fonctionnalités sont utilisées conformément aux lois et règlements en vigueur et aux normes de meilleures pratiques en vigueur dans l'industrie. Le Client rapprochera les paramètres par défaut du Logiciel de ses exigences propres. Le Client est tenu de s'inscrire auprès des autorités compétentes et/ou d'obtenir leur approbation lorsque cela est requis par les lois et réglementations en vigueur.

4.8 Le Client effectue tous les Envois en son propre nom et sous sa marque. Le message ne doit donc pas faire mention de MAPP comme expéditeur officiel du Message. MAPP n'est pas tenue et n'est pas en mesure de contrôler la conformité des Envois avec les lois, règlements et normes de meilleures pratiques de l'industrie. Le Client doit détenir tous les permis, licences et autorisations nécessaires pour les services ou produits promus par DMC.

5. POLITIQUE DE DÉLIVRABILITÉ

5.1 La Délivrabilité dépend de nombreux facteurs. MAPP gère la délivrabilité avec excellence et attache une grande importance à sa réputation sur Internet. MAPP fera des efforts commercialement raisonnables et utilisera la technologie appropriée pour assurer la délivrabilité de tous les messages envoyés par l'intermédiaire de DMC. Néanmoins, le Client accepte que la délivrabilité des messages dépende de facteurs qui sont hors du contrôle et de l'influence de MAPP et que, par conséquent, MAPP n'ait pas d'obligation de fin quant à la prestation fournie.

5.2 La Délivrabilité dépend en grande partie de la qualité des Listes de Clients. Par conséquent, les Listes doivent répondre aux exigences suivantes :

a) Les Adresses qui n'ont pas été utilisées par leurs titulaires pendant longtemps sont bloquées par certains fournisseurs de services Internet qui envoient ensuite un message de rebond rejeté pendant une courte période. Par la suite, certaines de ces Adresses sont converties en pièges à spam si bien que de telles adresses peuvent être bloquées si

elles continuent d'être écrites à l'adresse ou au domaine IP de l'expéditeur. Par conséquent, les Adresses qui sont destinées à être écrites via le Logiciel exigent que soit un consentement ait été donné dans les deux derniers mois précédant le premier Envoi ou que ces adresses fassent régulièrement l'objet d'écritures, c'est-à-dire au moins tous les deux mois.

b) Les Adresses entraînant des rejets de Rebonds doivent être supprimées des Listes. Le Client doit s'assurer que les Adresses engendrant des Rebonds rejetés ont été régulièrement bloquées (tous les deux mois au moins) ou effacés de ses Listes aussi avant l'utilisation du Logiciel. Les paramètres par défaut du Logiciel prévoient le blocage automatique des Adresses ayant provoqué un Rebond rejeté après le premier rebond rejeté.

c) Un Envoi à une Liste spécifique ne doit pas dépasser 5 % de Rebonds rejetés. Le taux de Rebonds rejetés est déterminé par le calcul de la proportion du nombre de Rebonds rejetés par rapport au volume total d'Envois à la Liste. Si une liste contient plus de 5 % d'Adresses engendrant des Rebonds rejetés, on peut supposer que la Liste n'a pas été mise à jour depuis longtemps. Pour la plupart des FAI, un taux de Rebonds rejetés supérieur à 10 % a pour effet de bloquer les Adresses ou les domaines IP de l'expéditeur ou de les placer dans une liste noire.

d) Un Envoi à une Liste en particulier ne doit pas excéder 3 % de Plaintes pour spam. Le taux de Plaintes pour spam est déterminé individuellement pour chaque FAI (participant) en calculant la proportion du nombre de Plaintes pour spam reçues par un FAI en particulier par rapport au volume total d'Envois à ce FAI (les deux étant liés à un Envoi spécifique à une Liste spécifique). Pour la plupart des FAI, un taux de Plaintes pour spam supérieur à 3 % a pour effet de bloquer les Adresses ou les domaines IP de l'expéditeur ou de les placer dans une liste noire. Cela ne dispense pas de nettoyer les listes de Rebonds refusés, tel qu'énoncé à la clause 5.6.

e) Les Listes doivent répondre à des critères d'acceptation de qualité spécifiques et ne doivent pas contenir plus de 10 % (i) d'Adresses génériques (comme tech@domain.com, root@domain.com), (ii) d'« adresses jetables », qui sont valables pendant une courte période et qui sont utilisées, entre autres, pour la participation à des tirages au sort (comme @mytrashmail.com ou @10minutemail.com), (iii) d'adresses avec des noms de domaine inexistants (comme @lycos.de), (iv) d'adresses dont la syntaxe est erronée (comme les adresses e-mail sans @), et (v) d'adresses qui ne sont pas autorisées par le FAI concerné (par exemple, certains FAI imposent qu'une adresse électronique comporte au moins (4) quatre caractères avant le signe @).

5.3 Pour optimiser de façon continue la délivrabilité pour tous les Clients, MAPP a le droit, mais n'est pas obligée, d'ajouter des adresses dirigeant les Rebonds rejetés vers une Liste générale de rebonds et d'empêcher l'envoi de Messages à des Adresses qui ont engendré des Rebonds rejetés en s'appuyant sur une Liste générale de rebonds utilisée comme liste noire générale pour tous les Envois de tous les Clients.

6. AUDIT DE LISTE ET NON-CONFORMITÉ

6.1 MAPP se réserve le droit de vérifier la Liste afin de tester une liste pour sa conformité avec la Politique de conformité et/ou la Politique de délivrabilité. À la demande de MAPP, le Client doit fournir des informations détaillées prouvant la conformité d'une Liste avec la Politique de conformité (par ex., les informations sur la source des adresses et l'utilisation précédente de la Liste). MAPP peut comparer une Liste à la Liste générale des rebonds afin d'identifier les adresses de la Liste qui engendreront des Rebonds rejetés et afin d'évaluer ainsi le taux potentiel de Rebonds rejetés d'une liste.

6.2 Avec l'approbation préalable du Client, MAPP peut utiliser un Envoi de test sur une Liste. Les Envois de test sont traités à une vitesse de transmission réduite (pour un volume maximal de 10 000 messages électroniques par heure) pour être envoyés à un maximum de 10 % des Adresses d'une Liste (dans la limite de 50 000 adresses).

6.3 Toute violation de la Politique de conformité et/ou de la Politique de délivrabilité identifiée lors d'un audit de la Liste ou d'un Envoi de test ou de l'affichage pendant un Envoi régulier et résultant d'un tel Envoi donne le droit à MAPP, mais ne l'oblige pas, à bloquer les Envois ultérieurs et à arrêter immédiatement les Envois en cours à la Liste concernée. Le blocage sera limité à la portée nécessaire afin d'empêcher de nouvelles violations. Un blocage n'entraîne pas une baisse des frais. Des frais récurrents continuent à s'appliquer.

6.4 En cas de violation de la Politique de conformité et/ou de la Politique de délivrabilité, MAPP a le droit, mais non l'obligation, de réduire la vitesse de transmission pour les Envois à la Liste (dans la limite de 10 000 messages par heure) au lieu de bloquer la Liste.

6.5 MAPP lève le blocage d'une Liste ou la réduction de la vitesse de transmission si aucune nouvelle violation de la Politique de conformité et/ou de la Politique de délivrabilité n'est attendue. Tout risque de nouvelle violation est écarté dès que le Client fournit la liste des mesures prises pour éviter de tels problèmes (par ex., le nettoyage de la Liste afin de supprimer les Adresses engendrant des Rebonds rejetés). Le Client peut demander à MAPP d'effectuer un Audit de délivrabilité. Un Audit de délivrabilité est l'analyse détaillée et le nettoyage d'une Liste destiné à améliorer la délivrabilité et à assurer le respect de cette Politique de conformité et de délivrabilité (disponible moyennant un supplément).

6.6 En cas de violations graves ou répétées de la Politique de conformité et/ou de la Politique de délivrabilité, MAPP a le droit, mais non l'obligation, d'affecter le système du Client à un pool d'adresses IP dédié distinct dont la réputation IP est inférieure à celle du pool IP général de MAPP, ce qui peut avoir une incidence sur la délivrabilité des Envois du Client.

6.7 Une infraction grave et/ou répétée à la Politique de conformité et/ou à la Politique de délivrabilité sera assimilée à une infraction grave à l'Accord.

6.8 Pour éviter toute ambiguïté, le Client reste seul responsable du respect de cette Politique de conformité et de délivrabilité également/même si MAPP effectue un Audit de liste, un Audit de délivrabilité et/ou un Envoi de test et qu'elle ne bloque pas une Liste et/ou lève le blocage d'une Liste.