CLOUD ADDENDUM

1. PORTEE

La présente Annexe s'applique à la mise à disposition du Logiciel Cloud de MAPP et doit être lue conjointement à l'Accord entre le Client et MAPP.

2. DÉFINITIONS

2.1 « Logiciel Cloud » désigne les logiciels en tant que service « SaaS » et les Logiciels hébergés, à l'exclusion des Logiciels installés sur site.

2.2 « Contrôleur des données » et « Processeur des données » possèdent la signification définie par les lois et réglementations en vigueur sur la protection des données.

2.3 « Point de démarcation » désigne le point auquel l'Internet public se connecte au routeur de limite MAPP

2.4 « Informations financières » désigne toutes les données liées aux comptes bancaires, aux cartes de crédit et de paiement, aux taux de crédit, aux soldes de comptes et à d'autres informations financières sur un individu ou une organisation et cette expression englobe en particulier toutes les données soumises à la norme « Payment Card Industry Data Security Standard (PCI DSS) ».

2.5 « Force Majeure » désigne les événements résultant de catastrophes naturelles, actions du gouvernement, troubles civils, actions militaires, actes de guerre, émeutes, actes de terrorisme, grèves, incendies ou autres événements indépendants de la volonté des parties.

2.6 « Logiciel hébergé » désigne un élément distinct du Logiciel en mode dédié, hébergé et exploité par MAPP et auquel le Client accède à distance.

2.7 « 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.

2.8 « SaaS » signifie « Logiciel en tant que service » et désigne un élément centralisé du Logiciel serveur de plusieurs Clients, hébergé et exploité par MAPP et auquel le Client accède à distance.

2.9 « Assistance programmée » correspond à la définition de la clause 3.3.

2.10 « Données sensibles » désigne l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou physiques, l'appartenance à un syndicat ou les Données personnelles relatives à la santé ou à l'orientation sexuelle.

2.11 « Logiciel » désigne les produits logiciels standard des d'applications marketing de MAPP attribués sous licence au Client en vertu de l'Accord.

3. FOURNITURE DE LOGICIELS CLOUD

3.1 MAPP devra fournir un Logiciel Cloud à l'usage du Client dans un environnement système sécurisé, hébergé et exploité par MAPP et auquel le Client accède à distance. Le Logiciel Cloud n'est pas loué au Client. L'utilisation du Logiciel requiert un navigateur standard conformément aux tableaux de plates-formes prises en charge par MAPP (disponibles sur demande). MAPP devra se conformer à toutes les lois et réglementations applicables à MAPP en matière de fonctionnement et de prestation de services du Logiciel Cloud au Client.

3.2 L'utilisation du Logiciel Cloud et son accès seront limités comme indiqué dans l'Accord (par exemple, en termes d'espace disponible de stockage de données, de puissance de traitement, de nombre d'utilisateurs simultanés). Le Client ne devra pas outrepasser les limites convenues dans l'Accord.

3.3 MAPP établit des périodes de maintenance programmées (« Maintenance programmée ») afin de mener des procédures de maintenance durant lesquelles le Logiciel peut ne pas être disponible. MAPP devra aviser le Client de toute Maintenance programmée à l'avance dans une limite raisonnable (au minimum 24 heures) par courrier électronique et/ou via le portail « MAPP At Your Service ». MAPP devra effectuer des efforts commercialement raisonnables pour effectuer une Maintenance programmée en dehors des heures de bureau (du lundi au vendredi de 9 h à 18 h). La Maintenance programmée devra se limiter à 8 heures par mois civil.

3.4 Sauf stipulation contraire dans l'Accord, le Client n'a pas droit à une adresse IP propre, un serveur physique propre ou une capacité de transmission et une bande passante dédiées.

3.5 Le Client reconnaît (i) que la transmission de données sur Internet comporte des risques de transmission spécifiques et que ces transmissions ne peuvent être entièrement protégées contre les accès réalisés par des

tiers ; le Client ne saurait tenir MAPP pour responsable de toute perte ou corruption de données survenant pendant ou consécutivement à la transmission des données via Internet ; et (ii) que le Logiciel Cloud peut subir des intrusions en raison du piratage et de l'utilisation non autorisée d'identifiants et de mots de passe qui se trouvent sous la seule responsabilité du Client.

3.6 MAPP effectue des sauvegardes du système pour assurer un traitement régulier et approprié des données conformément aux procédures et politiques actuelles de sauvegarde de MAPP (disponibles sur demande), lesquelles peuvent être révisées périodiquement à l'appréciation raisonnable de MAPP.

3.7 MAPP fait appel à ses experts et ressources à travers le monde pour fournir au Client les Produits et Services couverts par l'Accord. Le Client reconnaît et accepte que le Logiciel et toutes les données (y compris les données à caractère personnel) résidant dans le Logiciel et/ou traitées par celui-ci puissent être transférées entre pays différents et hébergées à l'étranger et/ou être accessibles par MAPP depuis un territoire autre que celui du lieu de résidence du Client et/ou de MAPP afin de fournir les Services de MAPP conformément à l'Accord.

3.8 MAPP a le droit, mais non l'obligation, d'accéder au Logiciel et d'installer et d'exécuter des outils de diagnostic sur le Logiciel (i) afin de régler les paramètres du Logiciel et d'améliorer ainsi les performances et/ou la sécurité du Logiciel, à condition que ces ajustements ne nuisent pas à l'utilisation du Logiciel par le Client ; (ii) afin de collecter et de stocker des données d'utilisation et des données système liées au support (et non pas aux Données personnelles) pour aider à la résolution des problèmes et au contrôle des modifications et pour détecter les défauts et en informer MAPP ; (iii) afin de générer une analyse statistique ; (iv) afin d'utiliser le Logiciel dans le cadre de la recherche et du développement.

4. UTILISATION DU LOGICIEL CLOUD

4.1 Le Client doit se conformer à l'ensemble des lois, règlements et normes de meilleures pratiques de l'industrie concernant son utilisation du Logiciel Cloud, notamment son traitement des données personnelles par l'intermédiaire du Logiciel Cloud. Le Client est responsable de l'identification et de l'interprétation des lois, règlements et normes de meilleures pratiques de l'industrie en vigueur qui affectent l'utilisation par le Client du Logiciel Cloud et les performances des Services de MAPP pour le Client et/ou au nom de celui-ci. Le Client doit garantir la conformité avec de telles exigences. Le Client doit rapprocher les paramètres par défaut du Logiciel Cloud de ses propres exigences.

4.2 Le Client doit utiliser le Logiciel Cloud uniquement pour ses besoins internes et ne doit pas (i) exploiter du contenu contrefait, menaçant, diffamatoire, illicite ou délictueux, notamment du spam, des contenus préjudiciables aux enfants ou violant la législation sur le respect de la vie privée des tiers ; (ii) traiter des éléments contenant des virus informatiques, vers, chevaux de Troie ou tout autre code informatique, fichier, script, agent ou programme nuisible ; (iii) entraver sciemment ou perturber l'intégrité ou les performances du Logiciel Cloud ; ou (iv) tenter d'obtenir un accès non autorisé au Logiciel Cloud ou à ses systèmes ou réseaux connexes. Après en avoir fait part au Client, MAPP peut supprimer toute donnée ou tout contenu qu'elle estime, avec raison, enfreindre les principes énoncés dans cette section.

4.3 Le Client doit fournir une connexion sécurisée pour accéder aux données ou les transférer au Logiciel Cloud. Afin d'assurer la confidentialité et l'intégrité des données du Client hébergées/traitées par le Logiciel, le Client doit mettre à jour les informations de connexion dès leur réception et protéger strictement leur confidentialité. Concernant la complexité des mots de passe et la périodicité de leur mise à jour, les informations de connexion du Client doivent être conformes aux exigences de la politique des mots de passe actuelle de MAPP (fournie sur demande). Les informations de connexion ne doivent être transmises à aucun tiers. Les comptes partagés sont interdits. Le Client informe immédiatement MAPP dans le cas où les informations de connexion ont été perdues ou compromises ou si un identifiant spécifique n'est plus nécessaire.

4.4 Le Client ne doit pas traiter des Données sensibles et/ou des Informations financières à l'aide du Logiciel Cloud.

4.5 Le Client doit sauvegarder toutes les données mises à la disposition de MAPP suivant une périodicité proportionnelle aux risques.

4.6 Le Client sera seul responsable :

a) de tout dommage aux données du Client et/ou au Logiciel dû à une négligence ou une faute intentionnelle des employés, consultants ou agents du Client bénéficiant d'un accès au Logiciel attribué par ledit Client ;

b) de la conduite d'un tiers qui a accès au Logiciel à l'aide des mots de passe du Client sans que la responsabilité de MAPP soit engagée ;

c) du non-respect des lois en vigueur de la part du Client dans le cadre de son activité ;

d) de disposer de processus, d'outils et de contrôle de sécurité raisonnables pour les systèmes et réseaux du Client interagissant avec le Logiciel Cloud ;

e) de faire ses choix en matière de stockage de sauvegarde et de capacités de calcul alternatives ainsi que de processus d'affaires dans le cas où le Logiciel Cloud serait indisponible ; et

f) de déterminer les moyens de sécurité, de protection et de sauvegarde des données nécessaires à son activité et son obligation ou ses exigences en matière de protection de ses données.

4.7 Le Client doit s'assurer que les mesures techniques et organisationnelles ainsi que les contrôles de sécurité mis en place par MAPP répondent à ses besoins et obéissent parfaitement à ses obligations ou exigences en matière de protection de ses données.

5. DISPONIBILITE

5.1 MAPP déploiera des efforts commercialement raisonnables pour que le Logiciel Cloud soit disponible 24 heures sur 24, 7 jours sur 7. MAPP fournira une Disponibilité minimale de fonctionnement de 99 % pour son Logiciel Cloud chaque mois civil de l'année.

La Disponibilité de fonctionnement signifie que la connexion entre les serveurs sur lesquels le Logiciel Cloud est hébergé et le Point de démarcation de MAPP est ininterrompue de sorte que le Client puisse se connecter au Logiciel Cloud et y accéder. La Disponibilité minimale de fonctionnement ne concerne pas les serveurs de test et de développement.

5.2 À intervalles fréquents, MAPP mesure la Disponibilité de fonctionnement d'une page de test de disponibilité dans le Logiciel Cloud. Le pourcentage de Disponibilité de fonctionnement pendant le mois civil concerné est obtenu en divisant le nombre de mesures de disponibilité réussies (page de test disponible) par le nombre total de mesures de disponibilité du mois civil concerné, excepté les Heures d'exclusion (tel que défini ci-dessous). La mesure de la Disponibilité de fonctionnement doit être effectuée par MAPP et servir de valeur de référence aux tiers ; MAPP conserve les enregistrements complets de ces mesures de Disponibilité de fonctionnement et doit les transmettre sur demande au Client.

Les Heures d'exclusion sont les heures durant lesquelles le Logiciel Cloud est indisponible pour les raisons suivantes :

- maintenance programmée ;
- pannes ou perturbations provoquées par le Client ou des tiers (sauf dans la mesure où ces pannes ou perturbations sont causées par des sous-traitants de MAPP fournissant des services contractuels de MAPP) et/ou
- pannes ou perturbations attribuables en totalité ou en partie à la Force majeure.

5.3 Si le pourcentage réel de Disponibilité de fonctionnement chute en dessous de la Disponibilité minimale de fonctionnement durant un mois civil donné (Défaut de prestation de services), le Client peut prétendre à un Crédit de service. Le Crédit de service augmente de 1 % les droits de licence des Logiciels de Cloud appartenant au Client pour le mois civil concerné chaque fois que le pourcentage de Disponibilité de fonctionnement baisse de 0,1 % en dessous de la Disponibilité minimale de fonctionnement. Le Crédit de service doit être limité à 25 % des frais applicables pour le mois civil concerné. Les Crédits de service seront imputés sur les factures suivantes uniquement, ne seront pas remboursés au Client et seront annulés à l'expiration de l'Accord. Un Crédit de service ne doit être alloué que si le Client en fait la demande dans les deux mois à compter de la fin du mois civil concerné.

5.4 Le Client reconnaît et accepte que les termes de la présente annexe relatifs aux Crédits de service en cas de Défaut de prestation de services constituent une véritable pré-estimation de la perte ou des dommages que le Client subirait à la suite du Défaut de prestation de services, doivent constituer le recours exclusif à ce Défaut de prestation de services et ne constituent pas un moyen de sanction à ce Défaut de prestation de services.

6. PROTECTION DES DONNÉES

6.1 MAPP traitera les données du Client uniquement selon les termes de l'Accord et uniquement à la demande du Client. MAPP ne traitera pas les données du Client pour son propre compte. Le Client devra toujours être le Contrôleur des données et continuer à exercer ce rôle tandis que MAPP sera le Processeur des données.

6.2 Le Client et MAPP devront individuellement se conformer à de telles réglementations de protection des données statutaires qui leur sont applicables. Le Client devra fournir à MAPP ces instructions qui peuvent être raisonnablement requises par MAPP pour que le Client s'acquitte de ses obligations contractuelles. Le Client reconnaît que MAPP dépend de lui à propos des instructions qu'il lui fournit dans la mesure où MAPP est autorisée à traiter les données du Client. Par conséquent, MAPP ne saurait être tenue pour responsable des données résultant d'un acte ou d'une omission de sa part, dans la mesure où cet acte ou cette omission résulterait directement des instructions du Client. Nonobstant ce qui précède, MAPP ne sera pas tenue de suivre les instructions du Client si cela requiert des Services supplémentaires ou exige que MAPP engage des dépenses supplémentaires, sauf si le Client a accepté de payer ces frais à MAPP.

Le traitement des Données personnelles doit inclure des mesures comme spécifié dans l'Accord. À l'intérieur de sa zone de responsabilité, MAPP mettra en place et maintiendra pendant toute la durée de l'Accord les mesures techniques et organisationnelles suivantes afin de protéger les Données du Client contre le traitement non autorisé ou illégal et/ou la perte accidentelle, la destruction ou les dommages :

- empêcher les personnes non autorisées d'accéder à des systèmes de traitement de données à caractère personnel (contrôle d'accès physique) ;
- empêcher l'utilisation des systèmes de traitement des données personnelles sans autorisation (contrôle d'accès logique) ;
- veiller à ce que les personnes habilitées à utiliser un système de traitement des données personnelles aient accès à ces Données personnellement uniquement si elles y sont autorisées conformément à leurs droits d'accès, et veiller à ce que, dans le cadre du traitement ou de l'utilisation des données et après stockage, les données personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation (contrôle d'accès aux données) ;
- garantir que les données personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation lors de transmission électronique, du transport ou du stockage sur des supports de stockage, et que les entités cibles de tout transfert de données à caractère personnel au moyen d'installations de transmission de données puissent être établies et vérifiées (contrôle de transfert des données) ;
- assurer la mise en place d'un audit pour vérifier si et par qui les données personnelles ont été saisies, modifiées ou retirées des systèmes de traitement de données à caractère personnel (contrôle d'entrée) ;
- garantir que les données à caractère personnel sont traitées conformément aux instructions du contrôleur (contrôle d'instructions) ;
- garantir que les données personnelles sont protégées contre leur destruction ou leur perte accidentelle (contrôle de disponibilité) ;
- veiller à ce que les données personnelles recueillies à des fins différentes puissent être traitées séparément (contrôle de séparation).

De plus amples détails sont disponibles sur demande. Le Client est tenu de vérifier que les mesures de sécurité qui sont prises sont suffisantes pour protéger le caractère sensible, la confidentialité et l'importance de ses données traitées par MAPP.

6.3 La partie qui détecte une faille de sécurité du Logiciel impliquant des données du Client doit en informer le plus vite possible l'autre partie. Les parties doivent convenir ensemble des conditions d'une enquête sur la violation de données et MAPP accepte de coopérer raisonnablement avec le Client durant la gestion du problème, y compris, mais sans s'y limiter : (i) en apportant son aide pour les recherches ; (ii) en organisant des entretiens avec les employés de MAPP et les autres personnes impliquées dans l'affaire ; et (iii) en mettant à disposition tous les documents pertinents, journaux, fichiers, rapports de données et autres ressources nécessaires au respect des lois, règlements et normes en vigueur dans l'industrie. Dès que possible, chaque partie fera de son mieux pour éviter que les données ne soient plus violées.

6.4 Sur demande écrite du Client (pas plus d'une fois par année civile), MAPP doit remplir correctement un questionnaire de sécurité raisonnable des informations que lui fournit le Client et qui concerne les pratiques et politiques de protection de données de MAPP et l'environnement informatique de MAPP. Après examen du questionnaire, le Client peut demander par écrit au moins 4 semaines à l'avance un audit des réponses du questionnaire. L'audit ne devra pas excéder 1 journée pendant les heures de travail de MAPP sur la base d'un planning accepté par les deux parties de sorte que le traitement affecte le moins possible le fonctionnement de MAPP. Le Client ne peut pas effectuer plus d'un audit tous les 2 ans sauf si un audit ou les réponses à un questionnaire révèlent une violation des obligations de MAPP en matière de protection contractuelle des données. Le Client et ses auditeurs devront se conformer aux exigences de sécurité de MAPP en matière de performances de l'audit.

6.5 Si une entité gouvernementale demande la levée de la confidentialité des données du Client hébergées par MAPP au nom de celui-ci, MAPP s'efforcera de mettre l'entité gouvernementale en contact avec le Client préalablement. Si MAPP devait néanmoins répondre à la demande, elle déploiera des efforts raisonnables pour aviser le Client à l'avance sauf si la loi le lui interdit et d'autre part MAPP limitera toute divulgation de données à ces données qu'elle est tenue légalement de transmettre.