ACCORD SUR LE TRAITEMENT DES DONNÉES

« CLIENT » ou **« CONTRÔLEUR » :**

Nom de la société : _____

Adresse : _____

_____

_____

Informations sur la société : _____

« MAPP » ou **« RESPONSABLE DU TRAITEMENT DES DONNÉES »** :

L'entité Mapp indiquée à l'Annexe 3 qui est partie aux MSA.

Le présent Accord sur le traitement de données (**« DPA »**) fait partie de l'Accord-cadre de services ou de tout autre accord pour l'achat des services Mapp (ci-après dénommé « **MSA** ») entre le Client et Mapp.
En signant le présent DPA, le Client adhère au DPA pour son compte et, dans la mesure requise par les Lois et réglementations applicables en matière de protection des données, au nom et pour le compte de ses Affiliés.
Comment conclure le présent DPA :

- Si le présent DPA est présigné au nom de Mapp, veuillez : (1) compléter ci-dessus les informations du Client ; (2) choisir l'entité Mapp qui est partie aux MSA ; (3) revoir l'Annexe 1 et la modifier si nécessaire ; (4) signer le DPA ; et (5) le soumettre par courrier électronique à privacy@mapp.com.
- Dès réception du DPA dûment signé, ce dernier deviendra juridiquement contraignant et fera partie des MSA.
- Si le client apporte au présent DPA des révisions qui n'ont pas fait l'objet d'un accord mutuel, ces dernières seront considérées comme nulles et non avenues. Le signataire du Client déclare à Mapp qu'il possède l'autorité légale nécessaire pour lier le Client. Le présent DPA prendra automatiquement fin au terme des MSA.

1. DÉFINITIONS

1.1 Le terme **Affilié** désigne toute entité qui possède ou contrôle directement ou indirectement, qui est détenue ou contrôlée, ou qui est sous un régime de propriété ou de contrôle commun de la partie en question.

1.2 Le terme **Directive** désigne la Directive européenne 95/46/CE sur la protection des données à caractère personnel.

1.3 Le terme **Législation en matière de protection des données** désigne les Directives européennes 95/46/CE et 2002/58/CE, le RGPD (Règlement (UE) 2016/679), toute législation et/ou réglementation mise en œuvre ou adoptée en vertu de celles-ci qui modifient, remplacent, rééditent, mettent en œuvre, consolident ou dérogent à l'une de celles-ci, ainsi qu'à toutes les autres lois applicables en matière de traitement des données à caractère personnel et de la vie privée qui peuvent exister dans tout pays concerné, y compris, le cas échéant, les directives et codes de pratique publiés par l'Autorité de la protection des données, les autres autorités de contrôle compétentes en matière de protection des données auprès de Nationwide et de son groupe, la Commission européenne, le Groupe de travail Article 29 et le Contrôleur européen de la protection des données.

1.4 Le terme **Lois et réglementations applicables en matière de protection des données** désigne toute législation et toute réglementation mettant en œuvre la Directive susceptible de s'appliquer et, à compter du 25 mai 2018, le règlement de l'Union européenne 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 (le **« Règlement général sur la protection des données »** ou **« RGPD »**), ainsi que toute législation et réglementation subordonnées mettant en œuvre le RGPD qui pourrait s'appliquer.

1.5 Le terme **Personne concernée** a la même signification que celle qui lui est donnée dans la Législation en matière de protection des données.

1.6 Le terme **Violation des données à caractère personnel** désigne une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès illégal ou accidentel à des données à caractère personnel transmises, stockées ou traitées.

1.7 Tous les autres termes portant une majuscule auront la signification qui leur est donnée dans la Législation en matière de protection des données ou dans les MSA.

2. TRAITEMENT DES DONNÉES

2.1 Les parties reconnaissent et acceptent, en ce qui concerne le Traitement des Données à caractère personnel, que le Client est le Contrôleur et que Mapp est le Responsable du traitement des données.

2.2 Chaque partie se doit de se conformer à leurs obligations respectives en vertu des Lois et réglementations applicables en matière de protection des données. Chaque partie se doit, lors de son utilisation des services Mapp, de traiter uniquement les Données à caractère personnel conformément aux exigences des Lois et réglementations applicables en matière de protection des données.

2.3 Les instructions du Client pour le Traitement des Données à caractère personnel doivent être conformes aux Lois et réglementations applicables en matière de protection des données. Mapp informera immédiatement le Client

si, selon lui, une instruction du Client enfreint les Lois et réglementations applicables en matière de protection des données.

2.4 Mapp traitera uniquement les Données à caractère personnel pour le compte et conformément aux instructions documentées du Client à des fins de (i) Traitement conforme aux MSA ; (ii) Traitement initié par les Utilisateurs lors de l'utilisation des Services ; (iii) Traitement pour se conformer à d'autres instructions raisonnables documentées fournies par le Client ; (iv) Protection de la confidentialité, de l'intégrité et de la disponibilité des Données à caractère personnel et des Services conformément au présent accord ; et (v) Collecte de données statistiques non identifiables.

2.5 L'objet, la durée, la nature et la finalité du Traitement, ainsi que le type de Données à caractère personnel et les catégories de Personnes concernées sont définis dans les MSA.

3. DROITS DES PERSONNES CONCERNÉES

3.1 Mapp doit, dans la mesure où la loi le permet, informer rapidement le Client si Mapp reçoit une demande de la part d'une Personne concernée pour exercer un ou plusieurs de ses droits, tels que définis dans le chapitre III du RGPD (33-36) (« **Demande DSR** »).

3.2 Compte tenu de la nature du Traitement, Mapp assistera le Client par des mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour remplir son obligation envers le Client de répondre à une Demande DSR en vertu des Lois et réglementations en matière de protection des données.

3.3 Dans la mesure où le Client, lorsqu'il utilise les Services, n'est pas en mesure de traiter une Demande DSR, Mapp doit, à la demande du Client, déployer des efforts commercialement raisonnables pour aider le Client à répondre à cette Demande DSR, dans la mesure où Mapp est légalement autorisé à le faire et dans la mesure où la réponse à cette Demande DSR est requise en vertu des Lois et réglementations en matière de protection des données. Dans la mesure permise par la loi, le Client sera responsable de tous les coûts découlant de la fourniture d'une telle assistance par Mapp.

4. ÉVALUATIONS DE L'INCIDENCE SUR LA PROTECTION DES DONNÉES

Mapp fournira au Client une assistance raisonnable lors de toute évaluation de l'incidence sur la protection des données et des consultations préalables avec une Autorité de surveillance, requises par les Lois et les réglementations en matière de protection des données, dans chaque cas, et ce, en ce qui concerne le Traitement des données à caractère personnel, et en tenant compte de la nature du Traitement et des informations disponibles.

5. NOTIFICATION D'UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

5.1 Mapp informera le Client, dans les meilleurs délais, après avoir pris connaissance d'une Violation de données à caractère personnel. Mapp fournira au Client des informations suffisantes lui permettant de respecter toute obligation de notifier une Autorité de surveillance de la Violation de données à caractère personnel et/ou de communiquer la Violation de données à caractère personnel aux Personnes concernées conformément à la Législation en matière de protection des données.

5.2 Mapp doit déployer des efforts raisonnables pour identifier la cause d'une Violation de données à caractère personnel et prendre les mesures qu'elle juge nécessaires et raisonnables pour remédier à la cause d'un tel Incident relatif aux données des clients dans la mesure où la réparation relève du contrôle raisonnable de Mapp.

5.3 Les obligations énoncées dans les présentes ne s'appliquent pas aux incidents causés par le Client.

6. SOUS-TRAITEMENT

6.1 Les Affiliés de Mapp et les autres Sous-traitants utilisés par Mapp pour fournir ses services contractuels, y compris leur rôle, la portée du sous-traitement et la zone géographique du sous-traitement, figurent sur la Liste des sous-traitants de Mapp disponible sur demande et/ou accessible sur www.mapp.com/contracts. Ces Sous-traitants doivent être acceptés et consentis par le Client. En signant le présent DPA, le Client accepte la liste des Sous-traitants ci-jointe en Annexe 3 et autorise Mapp à transférer des Données à caractère personnel à ses Affiliés et/ou à d'autres Sous-traitants vers des sites extérieurs à l'Espace économique européen, dans la mesure du nécessaire, pour fournir une assistance, réaliser des projets techniques ou effectuer d'autres types de services dans le cadre des MSA, à condition, si le Client est intégré à l'UE, que : (i) ces sites soient reconnus par la Commission européenne comme offrant une protection adéquate des données ; ou (ii) Mapp ait exécuté les Clauses contractuelles types de l'UE avec de tels Affiliés et/ou d'autres Sous-traitants.

6.2 Mapp a conclu avec chaque sous-traitant un accord écrit contenant des obligations de protection des données assurant un niveau de protection identique à celles du présent DPA en ce qui concerne la protection des Données à caractère personnel dans la mesure applicable à la nature des Services fournis par ce sous-traitant.

6.3 Mapp sera responsable des actes et des omissions de ses sous-traitants dans la même mesure que Mapp sera responsable si les services de chaque sous-traitant étaient rendus directement en vertu des termes du présent DPA, sauf indication contraire dans les MSA.

6.4 Si Mapp anticipe la nécessité de changer ou d'ajouter un sous-traitant, Mapp informera le Client de tout changement de sous-traitant et le Client sera autorisé à s'opposer à tout changement dans un délai raisonnable.

Si le client omet de s'opposer à un tel changement dans le délai imparti, le Client est réputé avoir consenti à un tel changement. Lorsqu'il existe une raison substantiellement importante à cette opposition et en l'absence d'une résolution amiable par les parties, le Client est en droit de mettre un terme au DPA. Mapp veillera à ce que tout nouveau sous-traitant respecte les mêmes normes applicables que les sous-traitants précédemment convenus.

7. SÉCURITÉ

Compte tenu de l'état de la technique, des coûts de mise en œuvre ainsi que de la nature, de la portée, du contexte et des finalités du traitement, ainsi que du risque de probabilité variable et de gravité des droits et libertés des personnes physiques, Mapp doit mettre en place des mesures techniques et organisationnelles appropriées pour la protection de la sécurité (y compris la protection contre tout Traitement non autorisé ou illégal et contre la destruction, la perte ou l'altération accidentelle ou illicite, la divulgation non autorisée, ou l'accès à des Données des clients), la confidentialité et l'intégrité des Données à caractère personnel, tel qu'énoncés dans l'Annexe de sécurité de Mapp (Annexe 2) du présent DPA. Mapp veille régulièrement au respect de ces mesures. Mapp ne diminuera pas de manière significative la sécurité globale des Services pendant la durée des MSA. Mapp limitera l'accès aux Données à caractère personnel à ses employés ou Sous-traitants pour lesquels l'accès à ces données est raisonnablement nécessaire pour respecter les obligations de Mapp envers le Client. Mapp veillera à ce que les personnes autorisées pour le Traitement des Données à caractère personnel soient liées par les mêmes obligations de confidentialité ou par des obligations équivalentes à celles de Mapp ou par une obligation légale de confidentialité appropriée. Des informations sur la Politique de sécurité de Mapp peuvent être fournies sur demande si le Client souhaite des détails supplémentaires concernant la présente section.

8. SUPPRESSION OU RENVOI DES DONNÉES À CARACTÈRE PERSONNEL

8.1 Mapp supprimera les Données à caractère personnel lors de la résiliation/expiration des MSA comme spécifié dans les MSA ou sur demande raisonnable du Client dans un délai de 30 jours et s'assurera que les données supprimées sont irrécupérables. Mapp peut conserver des Données à caractère personnel dans la mesure requise par les lois applicables et uniquement dans la mesure et pour la période requises par les lois applicables et toujours à condition que Mapp garantisse la confidentialité de toutes ces Données à caractère personnel et veille à ce que ces Données à caractère personnel fassent l'objet d'un Traitement nécessaire aux fins spécifiées dans les lois applicables et nécessitant leur conservation et à aucune autre fin.

8.2 Mapp fournira au Client, à la demande de ce dernier, une confirmation écrite que la suppression a eu lieu conformément à la présente section 8.

8.3 Mapp renverra les Données à caractère personnel au Client conformément à la procédure et aux délais spécifiés dans les MSA.

9. VÉRIFICATIONS ET CONTRÔLES

9.1 Mapp mettra à la disposition du Client toutes les informations nécessaires pour démontrer la conformité au présent DPA et permettra et contribuera aux audits du Client ou d'un auditeur tiers mandaté par le Client concernant le Traitement des Données à caractère personnel. Sur demande écrite du Client, Mapp remplira avec précision, pas plus d'une fois par an, un questionnaire de sécurité des informations fourni par le Client concernant les pratiques et politiques de Mapp en matière de protection des données et de sécurité des informations.

9.2 Le Client ou un auditeur tiers mandaté par le Client peut, aux frais de ce dernier et pas plus d'une fois par an, procéder à une inspection sur site des pratiques et politiques de Mapp en matière de protection des données et de sécurité des informations au moyen d'un préavis écrit envoyé au moins dix jours ouvrables à l'avance. L'inspection ne doit pas excéder une journée et doit se dérouler durant les heures normales de bureau de Mapp, selon un calendrier convenu d'un commun accord, de manière à minimiser l'incidence de l'inspection sur les opérations de Mapp. Le Client ou l'auditeur tiers mandaté par le Client doit se conformer aux exigences de sécurité de Mapp concernant l'exécution de l'inspection. En raison des exigences de confidentialité et de sécurité, de telles inspections doivent exclure les inspections sur site des environnements multilocataires (tels que les centres de données IaaS utilisés par Mapp). Les examens sur site de tels environnements peuvent être remplacés par une documentation détaillée fournie par Mapp à la demande du Client concernant les mesures de protection et de sécurité des données respectives prises et des certifications spécifiques émises par des auditeurs tiers réputés.

9.3 Le Client doit notifier rapidement à Mapp tout cas de non-conformité découvert lors d'un tel audit et/ou inspection.

10. RESPONSABILITÉ

10.1 La responsabilité de chaque partie découlant ou liée au présent DPA et à tous les DPA entre les Affiliés et Mapp, que ce soit sous la forme d'un contrat, d'une responsabilité délictuelle ou en vertu de toute autre théorie de la responsabilité, est sujette à la section « Limitation de responsabilité » agréée par les MSA, et toute référence dans la présente section de la responsabilité d'une partie désigne la responsabilité globale de cette partie et de

tous ses Affiliés en vertu des MSA et de tous les DPA réunis.

10.2 Pour éviter toute ambiguïté, la responsabilité totale de Mapp pour toutes les réclamations du Client et de tous ses Affiliés découlant ou liées aux MSA et à chaque DPA s'appliquera à l'échelle mondiale pour toutes les réclamations émises en vertu des MSA et de tous les DPA établis en vertu du présent Accord.

10.3 Lorsqu'une Personne concernée fait valoir ses droits à l'encontre d'une partie pour le présent DPA conformément à l'article 82 du RGPD, l'autre partie doit soutenir, dans la mesure du possible, la défense contre de telles réclamations.

Annexe 1 : Personnes concernées et catégories
Annexe 2 : Annexe de sécurité
Annexe 3 : Liste des Affiliés et des Sous-traitants de Mapp

CONTRÔLEUR		**RESPONSABLE DU TRAITEMENT**	
Signature :		Signature :	
Nom imprimé, titre :		Nom imprimé, titre :	Steven Warren, directeur général
Date :		Date :	

ANNEXE 1 : PERSONNES CONCERNÉES ET CATÉGORIES

Personnes concernées. Les données à caractère personnel traitées concernent les catégories de personnes concernées suivantes :

- Les clients du Client ;
- Les prospects du Client ;
- Les visiteurs du site Internet du Client ;
- Les employés du Client.

Catégories de données. Les données à caractère personnel traitées concernent les catégories de données suivantes :

- L'adresse e-mail ;
- Le numéro de portable ;
- Le numéro de téléphone fixe ;
- Le nom et le prénom ;
- L'adresse postale ;
- La date de naissance ;
- L'ouverture des e-mails reçus ;
- Le nombre de clics sur les liens dans les e-mails reçus ;
- Les adresses IP ;
- Le comportement d'utilisation du site.

ANNEXE 2 :ANNEXE DE SÉCURITÉ

INFORMATIONS TECHNIQUES ET ORGANISATIONNELLES SUR LES MESURES DE SÉCURITÉ VERSION 5.0, 23/05/2019

1. Confidentialité (Article 32, section 1, paragraphe a et b du RGPD et Article 25, paragraphe 1 du RGPD)	
Contrôle d'accès physique	**Mise en œuvre**
Mapp prendra des mesures appropriées pour empêcher les personnes non autorisées d'accéder à l'équipement de traitement de données où les données à caractère personnel sont traitées ou utilisées.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.11.1.x à A.11.6.x. Cela inclut : - Les zones de sécurité établies avec points d'entrée/sortie protégés. - Les procédures d'autorisation pour les employés et les tiers. - Les procédures de gestion des visiteurs pour assurer une authentification et une supervision appropriées. - La vidéosurveillance pour tous les centres de données et les principaux bureaux couvrant tous les points d'entrée et de sortie. - L'accès à l'équipement du centre de données nécessite, au minimum, deux facteurs d'authentification différents. - L'équipement est placé de manière à le protéger efficacement contre la divulgation non autorisée d'informations. - Les systèmes d'alarme de sécurité pour les centres de données et les principaux bureaux. - L'espace de réception et/ou les gardiens de sécurité dans les centres de données. - Les procédures pour l'attribution d'une clé d'authentification sécurisée et/ou l'inscription de données biométriques. - Le système d'accès électronique qui enregistre tous les accès aux centres de données et aux principaux bureaux. - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
Contrôle d'accès au système	**Mise en œuvre**
Mapp doit prendre des mesures appropriées pour empêcher ses systèmes de traitement de données à caractère personnel d'être utilisés par des personnes non autorisées.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.6.2.1, A.9.1.x, A.9.2.x, A.9.3.x, A.10.1.x, A.11.2.8-.9, A.12.2.1, A.12.4.1, A.12.6.1, A.14.2.x et A.18.2.3. Cela inclut : - La politique de contrôle d'accès maintenue. - La procédure de gestion des comptes utilisateurs et des comptes privilégiés conformément au cycle de vie de l'emploi basé sur un répertoire central. - L'authentification multifacteurs requise pour un accès privilégié à l'infrastructure. - La politique de mot de passe qui requiert techniquement au moins 8 caractères ; qui contient au moins trois des quatre éléments suivants : majuscule(s), minuscule(s), numéro(s), symbole(s) ; un mot de passe différent des 8 mots de passe précédemment utilisés ; les mots de passe des utilisateurs internes doivent expirer après 90 jours ; et une longueur minimale de 14 caractères est requise pour les comptes d'administrateur et de service. Les utilisateurs sont tenus de modifier les mots de passe initiaux lors de leur première connexion. - Les employés sont tenus de respecter la politique relative au nettoyage des bureaux. Les écrans sont verrouillés automatiquement au plus tard après 15 minutes d'inactivité. - L'accès au réseau interne est limité aux appareils autorisés de l'entreprise. - Des systèmes anti-programmes malveillants sont installés sur tous les systèmes Windows et les serveurs Linux susceptibles d'être infectés par des programmes malveillants. - La surveillance des événements de sécurité liés aux systèmes internes et de production. - Le non-traitement de données sur les appareils mobiles tels que les téléphones mobiles ou les tablettes. - La politique interdisant le transfert de données sur un support amovible. - Le client reste responsable de la protection des informations d'identification sous son contrôle. - Les processus de gestion des vulnérabilités techniques, y compris l'analyse de code statique, des évaluations internes périodiques des vulnérabilités et des tests d'intrusion tiers. Les clients peuvent effectuer leurs propres évaluations techniques en accord avec Mapp. - Les principes de codage sécurisés conformément au Top 10 de l'OWASP, qui sont régulièrement instruits aux développeurs de logiciels. - Les réseaux de production sont efficacement séparés et protégés par des pare-feu. L'absence de stockage de données dans la zone de présentation d'un réseau. - Le système de détection d'intrusion basé sur l'hôte en place et surveillé (s'applique à Mapp Engage). - Le système de détection et de prévention des intrusions basé sur le réseau en place et surveillé (s'applique à Mapp Engage). - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
Contrôle d'accès aux données	**Mise en œuvre**
Aucune opération non autorisée de lecture, copie, modification ou suppression dans les systèmes d'information	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.6.2.1, A.8.3.2, A.9.1.x, A.9.2.x, A.10.1.1-.2 et A.11.2.7. Cela inclut : - La procédure de gestion des droits d'accès des comptes utilisateurs et des comptes privilégiés conformément au cycle de vie de l'emploi basé sur un répertoire central. - L'accès aux données limitées aux groupes autorisés. - L'attribution de droits d'accès privilégiés suit le principe de moindre privilège. - Le modèle de rôle et de permission optimisé a été implémenté pour permettre la personnalisation de l'accès client en fonction du principe du besoin d'en connaître. - Les comptes de l'annuaire central sont examinés tous les six mois. - Les comptes privilégiés ayant accès à l'infrastructure sont examinés au moins une fois par an. - L'activité des comptes utilisateurs et des comptes privilégiés, ainsi que d'autres événements liés à la sécurité, est enregistrée et les journaux sont protégés contre la perte et la manipulation.

	- Les journaux des comptes privilégiés sont régulièrement examinés, manuellement et/ou automatiquement. - Le client reste responsable des révisions d'accès spécifiques à l'application. - Les systèmes de stockage appliquent un chiffrement de système de fichiers ou d'objet à l'aide de AES-256 (ou équivalent). - L'utilisation de systèmes de fichiers cryptés sur les ordinateurs portables des entreprises. - L'utilisation de supports amovibles techniquement limités. - Les procédures pour la mise au rebut sécurisée des équipements et la suppression définitive des données lors du processus de désinscription du client. - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
Contrôle de séparation	**Mise en œuvre**
Traitement séparé des données collectées à des fins différentes.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.9.4.1, A.12.1.4 et A14.3.1. Cela inclut : - La séparation logique des données du locataire dans les environnements de production et de service. - Les environnements de développement, de test et de production sont séparés. - Aucune utilisation des données de production à des fins de test. - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
Pseudonymisation	**Mise en œuvre**
Traitement des données à caractère personnel empêchant l'association de données à une personne en particulier sans informations supplémentaires, conservées séparément par des mesures techniques ou organisationnelles appropriées.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.6.1.5, A.14.1.1, A.14.2.1 et A.14.2.8. Cela inclut : - Les procédures de développement incluent les principes de conception pour la minimisation des données, la limitation de la collecte et la confidentialité par défaut, y compris l'exigence d'un pseudonymisation dans la mesure du possible. - Les données comportementales sont stockées sous une forme pseudonymisée et séparées du profil de contact correspondant lorsque cela est possible (s'applique à Mapp Engage). - Le suivi en ligne par pseudonyme par défaut (s'applique à Mapp Acquire). - Les journaux système sont anonymisés dans la mesure du possible. - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
2. Intégrité (Article 32, section 1, paragraphe b du RGPD)	
Contrôle de transfert	**Mise en œuvre**
Aucune opération non autorisée de lecture, copie, modification ou suppression pendant le transfert ou le transport.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.8.3.3, A.9.1.x et A.10.1.1-2. Cela inclut : - Les données transférées sur des réseaux publics de transmission de données sont efficacement protégées à l'aide de normes et d'algorithmes conformes aux bonnes pratiques du secteur, tels que TLS ou SSH, avec des configurations sécurisées. - Les données ne sont pas transférées physiquement, ni sur papier ni sur des périphériques de stockage mobiles. - Des messageries électroniques sécurisées sont en place pour les communications internes et externes, mais nous n'autorisons pas le transfert de données (traitées en vertu du présent DPA) par courrier électronique. Si les clients envoient des données par courrier électronique ou demandent à Mapp de le faire, le client sera tenu pour responsable. - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
Contrôle d'entrée	**Mise en œuvre**
Déterminer si les données à caractère personnel ont été saisies, modifiées ou supprimées des systèmes d'information.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.12.2.1, A.12.4.1-.4 et A.12.6.1. Cela inclut : - Les comptes utilisateur et les comptes privilégiés sont uniques et identifiables lorsque cela est techniquement possible. Néanmoins, les comptes racines sont strictement contrôlés. - L'accès aux données au niveau de l'application et de la base de données est journalisé de manière exhaustive et les journaux sont protégés contre la perte et la manipulation. - Les sources de journal utilisent une source de synchronisation du temps (NTP). - Le système de détection d'intrusion basé sur l'hôte en place et surveillé (s'applique à Mapp Engage). - Le système de détection et de prévention des intrusions basé sur le réseau en place et surveillé (s'applique à Mapp Engage). - Les processus de gestion des vulnérabilités techniques, y compris l'analyse de code statique, des évaluations internes périodiques des vulnérabilités et des tests d'intrusion tiers. Les clients peuvent effectuer leurs propres évaluations techniques en accord avec Mapp. - Des systèmes anti-programmes malveillants sont installés sur tous les systèmes Windows et les serveurs Linux susceptibles d'être infectés par des programmes malveillants. - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
3. Disponibilité et résilience (Article 32, section 1, paragraphe b et c du RGPD)	
Contrôle de disponibilité	**Mise en œuvre**
Protection contre la perte ou la destruction accidentelle ou intentionnelle.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.12.1.2, A.12.1.3, A.12.2.1, A.12.3.1, A.12.4.1, A.12.6.1, A.17.1.x et A.17.2.1. Cela inclut : - Des systèmes de détection et de suppression sont installés dans les centres de données afin de minimiser les risques liés aux incendies et à l'eau. Ceux-ci sont entretenus et testés au moins une fois par an. - Les équipements sont situés de manière à les protéger efficacement contre les dommages environnementaux ou le sabotage. - Les composants de système critiques (par exemple, les serveurs Web ou les équilibreurs de charge) sont redondants pour éviter les points de défaillance uniques. - Les données sont répliquées et les données relationnelles sont sauvegardées quotidiennement.

	- Les processus de gestion des vulnérabilités techniques, y compris l'analyse de code statique, des évaluations internes périodiques des vulnérabilités et des tests d'intrusion tiers. Les clients peuvent effectuer leurs propres évaluations techniques en accord avec Mapp. - La planification et la surveillance de la capacité informatique, de stockage et du réseau. - La surveillance de la santé et de la disponibilité du système. - Les procédures de gestion du changement pendant les opérations normales et les urgences. - Des systèmes anti-programmes malveillants sont installés sur tous les systèmes Windows et les serveurs Linux susceptibles d'être infectés par des programmes malveillants. - Un système de détection et de prévention des intrusions basé sur le réseau en place et surveillé pour se protéger contre les attaques par déni de service (s'applique à Mapp Engage). - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
Capacité de récupération	**Mise en œuvre**
Capacité de récupération dans un délai approprié après un événement perturbateur.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.12.3.1, A.17.1.x et A.17.2.1. Cela inclut : - Les plans de continuité des activités et de reprise après sinistre pour les centres de données et les services logiciels sont mis à jour et testés régulièrement. - Les générateurs UPS et diesel sont installés dans les centres de données pour palier aux pannes de courant pendant au moins 24 heures. Ceux-ci sont entretenus et testés au moins une fois par an. - Les données sont répliquées et les données relationnelles sont sauvegardées quotidiennement. Les procédures de récupération de sauvegarde sont régulièrement testées. - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
4. Processus d'évaluation régulière de l'efficacité des mesures (Article 32, section 1, paragraphe d du RGPD, Article 25, section 1 et 2 du RGPD)	
Gestion de la protection des données	**Mise en œuvre**
Approche systématique de la gestion de la protection des données.	Exploitation d'un système de gestion de la sécurité de l'information et de la protection des données conforme aux normes ISO 27001:2013, ISO 27002:2013 et ISO 27018:2014. Cela inclut : - Les rôles et responsabilités clairement définis et communiqués en ce qui concerne la sécurité de l'information et la protection de la vie privée, notamment sans s'y limiter : le responsable de la sécurité des systèmes d'information et le délégué à la protection des données et/ou de la vie privée. - Les procédures de gouvernance pour la gestion des risques liés à l'information, le respect et la communication des politiques, les évaluations de conformité internes et externes des tiers, l'établissement de rapports et d'évaluations de la gestion, ainsi que le suivi des améliorations continues. - Le programme de sensibilisation à la sécurité de l'information et à la protection de la vie privée, comprenant des formations obligatoires pour les nouveaux employés et des formations de mise à jour annuelles, ainsi que des mesures de sensibilisation supplémentaires. - L'audit annuel indépendant du système de gestion de la sécurité de l'information et de la protection des données. - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
Gestion de la réponse aux incidents	**Mise en œuvre**
Approche systématique de la gestion des incidents.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier l'Annexe A.16.1.x. Cela inclut : - La procédure de signalement des incidents, instruite à tous les employés. - La procédure d'intervention en cas d'incident, y compris la vérification, la classification, le confinement, l'éradication et le rétablissement et des guides pour certains types d'incidents. - La procédure de notification conforme aux exigences légales et contractuelles. - L'analyse rétrospective requise pour les incidents significatifs. - Les contrôles de sécurité supplémentaires conformes aux politiques de sécurité des informations de Mapp.
Confidentialité par défaut	**Mise en œuvre**
Le respect de la protection des données doit être intégré tout au long du cycle de vie des technologies et des procédures.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.8.1.3, A.13.2.1 et A.14.2.5. Cela inclut : - Les procédures de développement incluent les principes de conception pour la minimisation des données, la limitation de la collecte et la confidentialité par défaut. Nos services logiciels sont hautement personnalisables. Les options de configuration sont disponibles dans l'aide en ligne respective. - Les clients restent responsables de l'utilisation légale et respectueuse de la vie privée des services logiciels de Mapp. De plus, la Politique d'utilisation acceptable s'applique : https://mapp.com/acceptable-use-policy/
Contrôle de la commande (Article 28 du RGPD)	**Mise en œuvre**
Pas de traitement de données sans l'instruction du contrôleur.	Les mesures sont conçues, appliquées et contrôlées conformément à la norme ISO 27001:2013, en particulier les Annexes A.8.3.2, A.11.2.7, A.13.2.1 et A.18.1.1. Cela inclut : - Mapp traite les données uniquement sur la base des instructions du Client, c'est-à-dire sur la base d'accords contractuels, de commandes ou d'instructions supplémentaires. Les clients doivent fournir des instructions uniquement sous forme écrite ou confirmer par écrit lorsque les instructions ont été communiquées oralement. - Les procédures pour la mise au rebut sécurisée des équipements et la suppression définitive des données lors du processus de désinscription du client. - La limitation effective du traitement des données conservées à des fins juridiques par le biais du cryptage des fichiers de sauvegarde, le cryptage des systèmes de fichiers, des contrôles d'accès stricts, la journalisation d'audit et des procédures de restauration basées sur des tickets.

ANNEXE 3 : LISTE DES SOUS-TRAITANTS ET DES AFFILIÉS DE MAPP DIGITAL

Sous-traitant	Lieu de traitement (et garanties légales si en dehors de l'EEE)	Objectif
Mapp Digital Germany GmbH	Allemagne	Interne : assistance et services, R&D
Mapp Digital France S.A.S.	France	Interne : assistance et services
Mapp Digital Italy SrL.	Italie	Interne : assistance et services
Mapp Digital UK Ltd	Royaume-Uni	Interne : assistance et services
Mapp Digital Poland sp. z.o.o.	Pologne	Interne : R&D
Mapp Digital Netherlands B.V.	Pays-Bas	Interne : R&D
Mapp Digital US, LLC	États-Unis (Clauses contractuelles types de l'UE et certifié par le Bouclier de protection des données UE – États-Unis)	Interne : assistance et services, R&D [Mapp Empower uniquement]
Aprimo/MEMO Marketing Operations Philippines Inc	Philippines (Clauses contractuelles types)	Interne : assistance et services
Aprimo Australia Pty Ltd	Australie (Clauses contractuelles types)	Interne : assistance
Pythian Group Inc.	Canada (Décision d'adéquation)	Externe : R&D [Mapp Empower uniquement]
Amazon Web Services, Inc.	Allemagne et Irlande	Externe : infrastructure de centre de données
Amazon Web Services, Inc.	États-Unis (Clauses contractuelles types)	Externe : infrastructure de centre de données [Mapp Empower uniquement]
Google, LLC.	Traitement principal et stockage des données en Belgique. Collecte et distribution à l'échelle mondiale, techniquement nécessaire en raison de la nature des services (Clauses contractuelles types)	Externe : infrastructure de centre de données [Mapp Acquire uniquement]
Global Access Internet Services GmbH	Allemagne	Externe : infrastructure de centre de données
CLX Networks AB	Suède et États-Unis (Clauses contractuelles types)	Externe : messagerie SMS [Mapp Engage, facultatif]
R&D Communications SrL	Italie	Externe : messagerie SMS [Mapp Engage, facultatif]
Mitto AG	Allemagne et Suisse (Décision d'adéquation)	Externe : messagerie SMS [Mapp Engage, facultatif]
WebTrekk GmbH	Allemagne et Italie	Interne : Mapp Intelligence
Webtrekk Analytics SL	Espagne	Interne : Mapp Intelligence

*Si le Royaume-Uni devenait un pays tiers au cours du Brexit, Mapp conclura des clauses contractuelles types pour garantir la conformité future des transferts transfrontaliers de Données à caractère personnel.

DES FOURNISSEURS SUPPLÉMENTAIRES PEUVENT ÊTRE NÉCESSAIRES POUR CERTAINS SERVICES OU POUR LES CLIENTS DONT LA DEMANDE D'ASSISTANCE EST ÉLEVÉE. CES FOURNISSEURS DOIVENT ÊTRE DÉSIGNÉS DANS L'EDT APPLICABLE POUR CES SERVICES.