Annexe - Accord de traitement des données Medius

Cette annexe de traitement des données (l' « Accord ») fait partie du **Contrat Cadre de Services Medius**, des Conditions d'utilisation du Portail Fournisseur ou de tout autre accord écrit entre une entité du groupe Medius et le client pour refléter l'accord des parties en ce qui concerne le traitement des Données Personnelles et contient certaines modalités relatives à la protection des données, à la vie privée et à la sécurité conformément aux exigences du RGPD, du RGPD britannique, du CCPA et d'autres lois ou réglementations relatives au traitement des Données Personnelles par Medius pour le compte du Client, le cas échéant.
En cas de conflit entre l'une quelconque de ces lois et réglementations sur la protection des données, les parties se conformeront à l'exigence la plus contraignante ou à la norme la plus élevée.
Tous les termes en majuscules non définis dans le présent document, auront la signification énoncée dans l'Accord.
Dans le cadre de la fourniture de services au Client conformément à l'Accord, Medius peut traiter des Données Personnelles pour le compte du Client, et les parties conviennent de se conformer aux dispositions ci-dessous concernant ces Données Personnelles, agissant chacune de bonne foi.

1. DÉFINITIONS

Les termes suivants auront les significations suivantes dans la présente Annexe de traitement des données.

1.1 **"Affilié"** désigne toute entité qui contrôle directement ou indirectement, qui est contrôlée par, ou qui est sous le contrôle commun de l'entité concernée. "Contrôle", aux fins de la présente définition, signifie la propriété ou le contrôle direct ou indirect de plus de 50 % des droits de vote de l'entité concernée.
1.2 **"Responsable du traitement"** désigne l'entité qui détermine les finalités et les moyens du traitement des Données Personnelles.
1.3 **"CCPA"** désigne la California Consumer Privacy Act de 2018 (Cal. Civ. Code §§ 1798.100 et suiv.), tel qu'amendé en 2020 par le California Privacy Rights Act.
1.4 **"Lois et Règlements sur la Protection des Données"** désigne : i) le RGPD et toutes les autres lois ou réglementations applicables de l'UE, de l'EEE ou des États membres du marché unique européen ou toute mise à jour, modification ou remplacement de celles-ci qui s'appliquent au traitement des Données Personnelles en vertu de l'Accord ; (ii) toutes les lois et réglementations américaines qui s'appliquent au traitement des Données Personnelles en vertu de l'Accord, y compris, mais sans s'y limiter, le CCPA ; (iii) toutes les lois et réglementations qui s'appliquent au traitement des Données Personnelles en vertu de l'Accord en vigueur de temps à autre au Royaume-Uni (y compris le RGPD britannique), et les termes "responsable du traitement", "traiter", "traitement", "sous-traitant", "autorité de contrôle" ont la même signification que dans le RGPD ou le RGPD britannique et en ce qui concerne le CCPA (tel que défini ci-dessus) selon les cas, les Parties conviennent que Medius est un "prestataire de services" et que le client est le "Business", comme défini par le CCPA en ce qui concerne les informations personnelles (telles que définies par le CCPA).
1.5 **"Personne Concernée"** désigne la personne physique identifiée ou identifiable à qui les Données Personnelles se rapportent.
1.6 **"RGPD"** désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (Règlement général sur la protection des données). Les références au RGPD dans la présente Annexe seront, dans la mesure applicable, réputées être des références aux lois correspondantes du Royaume-Uni (y compris le RGPD britannique et la loi de 2018 sur la protection des données).
1.7 **" Données personnelles "** désigne toute information se rapportant à une personne physique identifiée ou identifiable lorsque ces données sont les données du Client.
1.8 **"Violation de données à caractère personnel"** signifie une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé aux Données Personnelles transmises, stockées ou traitées d'une autre manière.
1.9 **"Traitement"** désigne toute opération ou ensemble d'opérations effectuées sur des Données Personnelles, que ce soit ou non par des moyens automatisés (tels que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou l'altération, la récupération, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou la mise à disposition d'une autre manière, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction).
1.10 **"Sous-traitant"** désigne l'entité qui traite des Données Personnelles pour le compte du responsable du traitement.
1.11 **"Transfert restreint/Transferts fondés sur une décision d'adéquation"** signifie i) un transfert de Données Personnelles du client à Medius ou ii) un transfert ultérieur de Données Personnelles de Medius à un sous-traitant, dans chaque cas, lorsque ce transfert serait interdit par les lois et réglementations sur la protection des données en l'absence des clauses contractuelles types, de l'Addenda britannique ou de tout autre mécanisme de transfert référencé au chapitre 5 du RGPD. Pour plus de clarté, lorsqu'un transfert de Données Personnelles est d'un type autorisé par les lois ou réglementations sur la protection des données dans le pays exportateur, par exemple dans le cas de transferts au sein de l'Union européenne vers un pays (comme la Suisse ou le Royaume-Uni) approuvé par la Commission

comme assurant un niveau de protection adéquat, ou tout transfert qui relève d'une dérogation autorisée, un tel transfert ne sera pas considéré comme un transfert restreint.
1.12 **"Services"** désigne les services fournis au client en vertu de l'Accord.
1.13 **"Clauses contractuelles types"** désigne les clauses contractuelles types conformément à la Décision de la Commission (UE) 2021/914 du 4 juin 2021, en conjonction avec l'Addendum britannique aux clauses contractuelles types de l'UE disponible sur https://www.medius.com/legal/uk-addendum-to-dpa/ (l'"Addendum britannique").
1.14 **"Sous-traitant"** désigne tout sous-traitant engagé par Medius ou par l'Affilié de Medius.
1.15 **"Autorité de contrôle"** désigne une autorité publique indépendante établie par un État membre de l'UE conformément au RGPD.
1.16 **"RGPD britannique"** désigne la Loi de 2018 sur la protection des données, ainsi que le RGPD tel qu'il fait partie du droit de l'Angleterre et du Pays de Galles, de l'Écosse et de l'Irlande du Nord en vertu de l'article 3 de la Loi de 2018 sur le retrait de l'Union européenne telle que modifiée par le Règlement de 2019 sur la protection des données, la vie privée et les communications électroniques (modifications, etc.) (retrait de l'UE) (SI 2019/419).
1.17 **"Medius"** désigne la société Medius avec laquelle le client a conclu l'Accord.
1.18 **"Client"** désigne la société ou toute autre entité juridique qui exécute l'Accord avec Medius.

2. TRAITEMENT DES DONNÉES PERSONNELLES

2.1 Rôles des Parties. Les Parties reconnaissent et conviennent qu'en ce qui concerne le traitement des Données Personnelles par Medius pour le compte du Client, le Client est le responsable du traitement et Medius est le sous-traitant.

2.2 Traitement des Données Personnelles par le Client. Le Client traitera les Données Personnelles conformément aux exigences des lois et réglementations sur la protection des données, et les instructions du Client concernant le traitement des Données Personnelles seront conformes aux lois et réglementations sur la protection des données. Le Client sera seul responsable de l'exactitude, de la qualité et de la légalité des Données Personnelles, ainsi que des moyens par lesquels le Client a collecté ces Données Personnelles.

2.3 Traitement des Données Personnelles par Medius. Medius traitera les Données Personnelles en tant qu'information confidentielle et ne traitera les Données Personnelles que pour le compte du Client et conformément aux instructions documentées du Client aux fins suivantes : (a) Traitement conformément à la Sous-Annexe 1 (Détails du traitement) et à l'Accord ; (b) Traitement initié par les Utilisateurs dans le cadre de leur utilisation des services ; et (c) Traitement pour se conformer à d'autres instructions raisonnables documentées fournies par le Client lorsque de telles instructions sont conformes aux termes de l'Accord. Medius informera immédiatement le Client si, selon l'opinion de Medius, l'une des instructions du Client enfreint les lois et réglementations sur la protection des données. Medius sera responsable du respect de toutes les lois et réglementations sur la protection des données applicables à la prestation des Services par Medius en tant que sous-traitant de données. Cependant, Medius n'est pas responsable du respect des lois applicables au Client ou à l'industrie du Client qui ne sont pas généralement applicables aux fournisseurs de services de technologie de l'information en gestion des dépenses. Dans la mesure où Medius traitera les données du Client qui sont des "Informations personnelles" soumises au CCPA, Medius le fera en tant que prestataire de services (au sens défini dans le CCPA) et reconnaît les restrictions suivantes : a) Medius traitera, conservera, utilisera et divulguera les informations personnelles, y compris les données du Client, uniquement dans le but de fournir les Services ou tel que par ailleurs autorisé en vertu de l'Accord, ou de cet Accord annexé au Contrat Cadre de Services tel que spécifié dans la Sous-Annexe 1 (Détails du traitement) ; b) Medius ne vendra ni ne partagera les informations personnelles, y compris les données du Client, à des fins autres que celle spécifiées dans le présent Accord, et ce, même à un tiers à titre onéreux ; c) Medius ne traitera, ne conservera, n'utilisera ni ne divulguera les informations personnelles, y compris à un tiers moyennant une contrepartie précieuse, , y compris les données du Client, à des fins autres que celles spécifiées dans l'Accord; d) Medius ne traitera, ne conservera, n'utilisera ni ne divulguera les informations personnelles, y compris les données du Client, à des fins en dehors de la relation commerciale directe entre le Client et Medius ; et e) Medius fournira un soutien raisonnable et répondra aux demandes du Client concernant les obligations de traitement des données de Medius.

2.4 Détails du traitement. L'objet du traitement des Données Personnelles par Medius est l'exécution des services. Les détails de la durée du traitement, de la nature et de la finalité du traitement, des types de Données Personnelles et des catégories de personnes concernées traitées dans le cadre du présent Accord sont spécifiés plus en détail dans la Sous-Annexe 1 (Détails du traitement) de cet Accord.

2.5 Affiliés et tiers. Dans le cas où il est expressément convenu dans le Contrat Cadre que les Affiliés du Client ou tout autre tiers bénéficieront également des Services, le Client agit à cet égard au nom et pour le compte des Affiliés du Client et/ou des tiers en leur qualité de responsables du traitement, et le Client doit, dans la mesure nécessaire, conclure des accords de traitement des données avec de tels responsables du traitement, nécessaires pour permettre à Medius et aux sous-traitants de Medius de traiter les Données Personnelles comme décrit dans cet Accord annexé au Contrat Cadre de Services. Le Client servira de point de contact unique pour Medius et sera seul responsable de la coordination interne, de l'examen et de la soumission des instructions ou demandes d'autres responsables du traitement à Medius, et Medius sera en droit de refuser toute demande ou instruction fournie directement par un responsable du traitement qui n'est pas le Client. Medius n'aura en outre aucune obligation d'informer ou de notifier un responsable du traitement lorsque Medius aura fourni de telles informations ou notifications au Client.

3. DROITS DES PERSONNES CONCERNÉES

3.1 Demande de la Personne Concernée. Dans la mesure légalement autorisée, Medius notifiera promptement le Client en cas de réception d'une demande d'une Personne Concernée pour exercer le droit d'accès, le droit de rectification, le droit de limitation du

traitement, le droit à l'effacement (« droit à l'oubli »), le droit à la portabilité des données, le droit d'opposition au traitement, ou le droit de ne pas être soumis à une décision individuelle automatisée, ou tout autre droit en vertu des lois et réglementations sur la protection des données (« Demande de la Personne Concernée »). Compte tenu de la nature du traitement, Medius assistera le Client par des mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour satisfaire à l'obligation du Client de répondre à une Demande de la Personne Concernée en vertu des lois et réglementations sur la protection des données. De plus, dans la mesure où le Client, dans l'utilisation des Services, n'a pas la capacité de traiter une Demande de la Personne Concernée, Medius s'engage, sur demande du Client, à déployer des efforts commercialement raisonnables pour aider le Client à répondre à une telle Demande de la Personne Concernée, dans la mesure où Medius est légalement autorisé à le faire et que la réponse à une telle Demande de la Personne Concernée est requise en vertu des lois et réglementations sur la protection des données. Le Client assumera tous les coûts associés à cette assistance, dans la mesure permise par la loi.

4. SÉCURITÉ ET CONFIDENTIALITÉ

4.1 Protection des Données Personnelles. Medius maintiendra des mesures techniques et organisationnelles appropriées pour protéger la sécurité (y compris contre un traitement non autorisé ou illégal, et contre la destruction, la perte ou l'altération accidentelles ou illégales, ou les dommages, la divulgation non autorisée ou l'accès aux Données Personnelles du Client), la confidentialité et l'intégrité des Données Personnelles du Client. Ces mesures prendront en compte la nature, la portée, le contexte et les finalités du traitement ainsi que les risques de probabilité et de gravité variables pour les droits et la liberté des personnes physiques. Les mesures seront examinées et mises à jour si nécessaire.

4.2 Confidentialité. Medius veillera à ce que le personnel de Medius impliqué dans le traitement des Données Personnelles soit informé de la nature confidentielle des Données Personnelles, ait reçu une formation appropriée sur ses responsabilités et se soit engagé à la confidentialité ou soit soumis à une obligation statutaire de confidentialité appropriée. Medius prendra des mesures commercialement raisonnables pour garantir la fiabilité du personnel de Medius impliqué dans le traitement des Données Personnelles et s'assurera que l'accès de Medius à ces données est limité au personnel chargé d'effectuer les services.

5. SOUS-TRAITANTS

5.1 Nomination de sous-traitants. Le Client reconnaît et accepte que (a) les Affiliés de Medius peuvent être retenus en tant que sous-traitants ; et (b) Medius et les Affiliés de Medius respectifs peuvent engager des sous-traitants tiers dans le cadre de la prestation des Services et (c) que Medius peut continuer à utiliser les sous-traitants déjà engagés par Medius ou les Affiliés de Medius à la date de cet Accord, qui sont répertoriés à l'adresse https://www.medius.com/legal/medius-sub-processors/. Medius ou ses Affiliés ont conclu un accord écrit avec chaque sous-traitant contenant des obligations de protection des données au moins aussi protectrices que celles de cet Accord en ce qui concerne la protection des Données Personnelles du Client dans la mesure applicable à la nature des services fournis par un tel sous-traitant. Le Client reconnaît et accepte que Medius peut retirer des sous-traitants à sa propre discrétion.

5.2 Nouveaux sous-traitants. Le Client peut s'opposer à l'utilisation d'un nouveau sous-traitant par Medius en informant Medius par écrit dans les dix (10) jours ouvrables suivant la réception des informations concernant les changements envisagés par Medius concernant l'ajout d'un nouveau sous-traitant. Dans le cas où le Client s'oppose à un nouveau sous-traitant, comme le permet la phrase précédente, Medius fournira des efforts raisonnables pour mettre à la disposition du Client une modification des Services ou recommander une modification commercialement raisonnable de la configuration ou de l'utilisation des Services par le Client afin d'éviter le traitement des Données Personnelles par le nouveau sous-traitant auquel le Client s'est opposé sans imposer de charge déraisonnable au Client. Si Medius est incapable de mettre en place un tel changement dans un délai raisonnable, qui n'excédera pas soixante (60) jours, le Client peut résilier l'Accord uniquement pour les Services qui ne peuvent pas être fournis par Medius sans le recours au nouveau sous-traitant auquel le Client s'est opposé en fournissant un avis écrit à Medius. Medius remboursera au Client tous les frais prépayés couvrant le reste de la durée de cet Accord à compter de la date d'effet de la résiliation pour les Services résiliés, sans imposer de pénalité au Client pour une telle résiliation.

5.3 Responsabilité. Medius sera responsable des actes et omissions de ses sous-traitants dans la même mesure que Medius serait responsable s'il exécutait les services de chaque sous-traitant directement en vertu des termes de cet Accord.

6. NOTIFICATION DES VIOLATIONS DE DONNÉES PERSONNELLES ET AUTRE ASSISTANCE

6.1 Medius notifiera le Client sans délai indu et, si possible, au plus tard dans les quarante-huit (48) heures, après avoir pris connaissance d'une violation de Données Personnelles affectant les Données Personnelles du Client, à moins que la violation de Données Personnelles ne soit pas susceptible d'entraîner un risque pour les droits et libertés des personnes concernées. Medius fournira au Client des informations suffisantes pour lui permettre de respecter ses obligations de notifier les personnes concernées ou l'autorité de contrôle conformément à l'article 33 du RGPD ou à toute autre loi ou réglementation applicable visant à informer les autorités de contrôle ou les personnes concernées. Medius enquêtera sur la violation de Données Personnelles et prendra des mesures raisonnables pour atténuer les effets et minimiser les dommages résultant de la violation.

6.2 Dans la mesure où cela n'est pas déjà explicitement couvert par les obligations de Medius dans le cadre de cet Accord, Medius assistera le Client pour garantir le respect des obligations découlant des articles 32 à 36 du RGPD, en tenant compte de la nature du traitement et des informations mise à la disposition de Medius.

7. RESTITUTION ET SUPPRESSION DES DONNÉES PERSONNELLES

7.1 Sauf accord explicite contraire stipulé dans le Contrat Cadre de Services, Medius s'engage, à l'expiration ou à la résiliation du Contrat Cadre de Services ou à la demande du Client, fournir au Client ses Données Personnelles dans un format standard, aux frais du Client. Si le Client demande les données dans un autre format, Medius s'engage à examiner les possibilités d'effectuer une telle exportation. Medius s'engage à conserver les données pendant une période d'un (1) mois après l'expiration ou la résiliation du Contrat, ou jusqu'à ce que tout transfert de données demandé ait été effectué, et les données seront supprimées au plus tard quatre-vingt-dix (90) jours après, sauf accord sur une autre période de conservation. Nonobstant ce qui précède, les données du Clients sauvegardés peuvent être conservées conformément aux politiques standards de sauvegarde de Medius pendant une période pouvant aller jusqu'à deux (02) ans suivant la résiliation du Contrat, à condition que de telles sauvegardes soient maintenues de manière sécurisée.

8. TRANSFERTS RESTREINTS

8.1 Les Parties comprennent et acceptent que les Données Personnelles traitées conformément à cet Accord, peuvent être transférées vers, ou respectivement consultées depuis, des pays situés en dehors de l'UE/EEE, du Royaume-Uni, des États-Unis et de la Suisse par Medius, les Affiliés de Medius et les Sous-traitants lors de la fourniture des Services conformément aux termes du Contrat Cadre de Services.

8.2 Pour les Transferts Restreints (qualifiés de « Transferts fondés sur une décision d'adéquation » par le RGPD) depuis l'Espace Économique Européen qui sont soumis aux Clauses Contractuelles Types, Medius et les Affiliés de Medius, ainsi que les Sous-traitants tiers, exécuteront et respecteront le Module Trois (de Traitant à Traitant) des Clauses Contractuelles Types. Pour les Transferts Restreints depuis le Royaume-Uni qui sont soumis aux Clauses Contractuelles Types, Medius et les Affiliés de Medius, ainsi que les Sous-traitants tiers, exécuteront et respecteront le Module Trois (de Traitant à Traitant) des Clauses Contractuelles Types en conjonction avec le UK Addendum. À la demande du Client, Medius fournira des informations sur le transfert, et le cas échéant, des copies des conditions de confidentialité et de sécurité pertinentes de l'accord de Medius avec le Sous-traitant, sans délai indu.

8.3 Medius aura le droit de modifier cette section 8 en cas de modification, de révocation ou d'invalidation par un tribunal compétent des Clauses Contractuelles Types et/ou de l'Addendum UK.

9. AUDIT

9.1 Medius effectuera régulièrement des audits des mesures de sécurité mises en place par Medius pour protéger les données du Client, y compris les Données Personnelles, lors de la fourniture des Services. Sur demande écrite du Client, Medius fournira au Client un rapport confidentiel des résultats de cet audit, par exemple sous la forme d'un rapport SOC, afin de permettre au Client de vérifier la conformité de Medius avec les obligations de sécurité définies dans cet Accord. Le rapport est réputé « information confidentielle » de Medius et est protégé par la clause de confidentialité énoncée dans le Contrat Cadre de Services.

9.2 Le Client accepte d'exercer son droit d'audit en demandant à Medius d'effectuer l'audit tel que décrit dans la section 9.1 ci-dessus. Si le Client conclut raisonnablement que la fourniture du rapport d'audit de Medius n'est pas suffisante pour démontrer la conformité de Medius avec les stipulations de cet Accord, Medius et les Affiliés de Medius devront, sous réserve de la section 9.3, mettre à la disposition du Client, sur demande, toutes les informations nécessaires pour démontrer la conformité avec cet Accord et permettre et contribuer aux audits, y compris les inspections, par le Client ou un auditeur indépendant mandaté par le Client concernant le traitement des Données Personnelles du Client par Medius. Les droits d'information et d'audit du Client n'existent que dans la mesure où le Contrat Cadre de Services ne confère pas par ailleurs au Client des droits d'information et d'audit répondant aux exigences pertinentes des lois et règlements relatifs à la protection des données (y compris, le cas échéant, l'article 28, paragraphe 3, lettre h) du RGPD).

9.3 Le Client notifiera à Medius raisonnablement à l'avance tout audit ou inspection à effectuer en vertu de la section 9.2 et s'engage (et veillera à ce que chacun des auditeurs mandatés par le Client fasse de même) à fournir des efforts raisonnables pour éviter de causer (ou, s'il ne peut pas éviter, pour minimiser) tout dommage, préjudice ou perturbation aux locaux audités, à l'équipement, au personnel et à l'activité pendant que son personnel est sur ces lieux dans le cadre d'un tel audit ou d'une telle inspection. Medius n'est pas tenu de donner accès aux locaux à des fins d'un tel audit ou d'une telle inspection en dehors des heures normales d'activité sur ces lieux, ou à des fins de plus d'un audit ou d'une inspection au cours d'une année civile, sauf pour tout audit ou inspection supplémentaire que le Client est tenu ou invité à effectuer par les lois et règlements relatifs à la protection des données ou une autorité de contrôle.

9.4 Le Client aura le droit, sur notification, de prendre des mesures raisonnables et appropriées pour arrêter et remédier à toute utilisation non autorisée par Medius des Informations Personnelles.

10. RESPONSABILITÉ

10.1 La responsabilité des parties en vertu de cet Accord sera soumise à la même limitation de responsabilité que celle convenue entre les parties dans le Contrat Cadre de Services.

10.2 Rien dans le présent Accord ou le Contrat Cadre de Services ne décharge l'une ou l'autre des parties de ses propres responsabilités et obligations directes en vertu des lois et règlements relatifs à la protection des données.

11. DIVERS

11.1 Sans préjudice des dispositions des clauses contractuelles types relatives à la loi applicable et à la juridiction compétente, les parties de cet Accord se soumettent par la présente au choix de juridiction stipulé dans le Contrat Cadre de Services à l'égard de tout litige ou réclamation découlant du présent Accord, quel que soit le motif.

11.2 Aucune disposition du présent Accord ne réduit les obligations de Medius en vertu du Contrat en ce qui concerne la protection des Données Personnelles ni ne permet à Medius de traiter (ou de permettre le traitement de) Données Personnelles d'une manière interdite par le Contrat Cadre de Services. En cas de conflit ou d'incompatibilité entre la présent Accord et les clauses contractuelles types, les clauses contractuelles types en conjonction avec l'Addendum UK prévaudront. En ce qui concerne l'objet du présent Accord, en cas d'incohérence entre les dispositions du présent Accord et tout autre accord entre les parties, y compris le Contrat Cadre de Services et y compris (sauf accord explicite contraire par écrit, signé au nom des parties) les accords conclus ou prétendument conclus après la date du présent Accord, les dispositions du présent Accord prévaudront.

11.3 Si une disposition du présent Accord est invalide ou inapplicable, le reste de l'Accord demeurera valide et en vigueur. La disposition invalide ou inapplicable sera soit (i) modifiée si nécessaire pour assurer sa validité et son applicabilité, tout en préservant autant que possible les intentions des parties, soit, si cela n'est pas possible, (ii) interprétée comme si la partie invalide ou inapplicable n'avait jamais été incorporé dans le présent Accord.

SOUS-ANNEXE 1

1. Objet du traitement

L'objet du traitement concerne l'automatisation des comptes fournisseurs (la capture, le traitement et le paiement des factures), l'intégration des fournisseurs, les achats, la gestion des contrats, les Services E-invoicing et/ou la gestion des dépenses.

2. Personnes concernées

Le client peut soumettre des Données Personnelles à Medius, dont l'étendue est déterminée et contrôlée par le Client à la seule discrétion du Client, et qui peut inclure, sans s'y limiter, des Données Personnelles relatives aux catégories de personnes suivantes :

- Employés, consultants ou autres représentants du Client
- Utilisateurs des Services du Client
- Personnes de contact des fournisseurs du Client et autres individus référencés sur les factures
- Représentants des fournisseurs du Client.
- Personnes référencées dans les contrats traités pour signature via les Services
- Signataires du Client et de la partir cocontractante du Client

3. Catégories de données

Le client peut soumettre des Données Personnelles à Medius, dont l'étendue est déterminée et contrôlée par le Client à la seule discrétion du Client, et qui peut inclure, sans s'y limiter, les catégories suivantes de Données Personnelles :

- Prénom et Nom
- Titre
- Coordonnées (société, e-mail, téléphone, adresse)
- Identifiant utilisateur (User ID)
- Toutes informations référencées dans les factures ou les contrats traités via les Services
- Numéro IP
- Banque et coordonnées bancaires
- Données de facturation et de paiement
- Données de localisation (mouvements, données GPS, GSM data, etc.)
- Numéros d'identification

4. Catégories particulières de données (signifiant des informations personnelles sensibles telles que définies à l'article 9 et 10 du RGPD et d'autres lois applicables en matière de protection des données ou des informations sur la santé ou l'état médical d'une personne ou la prestation de soins de santé à une personne)

Les Données Personnelles transférées concernent les catégories particulières de données suivantes (veuillez préciser) :

- N/A, sauf si défini par le Client.

5. Opérations de traitement

Les Données Personnelles transférées seront soumises aux opérations de traitement de base suivantes (veuillez préciser) :
L'objectif du traitement des Données Personnelles est de fournir, maintenir et développer les Services conformément au présent Accord.

6. Durée

Selon la demande du Client - cependant, pas plus longtemps que la durée du présent Accord additionnée à la période allant de la résiliation de l'Accord jusqu'à la suppression des données du Client conformément au présent Accord.

SOUS-ANNEXE 2

Description des mesures de sécurité techniques et organisationnelles mises en place par Medius

Medius maintient des mesures de sécurité appropriées pour protéger les Données Personnelles contre la destruction ou la perte accidentelle, l'altération, la divulgation ou l'accès non autorisés, en particulier lorsque le traitement implique la transmission de données sur un réseau, et contre toutes les autres formes illégales de traitement. Ces mesures garantissent un niveau de sécurité approprié aux risques présentés par le traitement et à la nature des données à protéger, en tenant compte de l'état de l'art et du coût de la mise en œuvre. Les mesures sont soumises aux progrès techniques et au développement, et Medius est donc expressément autorisé à mettre en place des mesures alternatives adéquates tant que le niveau général de sécurité décrit dans cette Sous-Annexe 2 est maintenu.

Les mesures de sécurité techniques et organisationnelles actuellement en place chez Medius pour tout système traitant des Données Personnelles afin de prévenir la destruction, l'altération, la divulgation, l'accès et d'autres formes inappropriées de traitement des informations exportées par le responsable du traitement vers le sous-traitant comprennent les domaines suivants :

Gouvernance et gestion des risques

- Programme de sécurité documenté approuvé par la direction et révisé au moins annuellement.
- Évaluations des risques effectuées au moins annuellement et lors de changements significatifs des Services ou du Traitement.
- Politiques et normes portant sur le contrôle d'accès, la gestion des actifs, la cryptographie, le développement sécurisé, la réponse aux incidents, la continuité d'activité, la gestion des fournisseurs et la protection des données.

Contrôle d'accès et gestion des identités

- Accès basé sur les rôles avec application du principe du moindre privilège et du besoin de savoir (need-to-know).
- Identifiants d'utilisateurs uniques, authentification forte pour tout accès à des systèmes qui la supportent.
- Mise en place formelle du provisionnement et du retrait des utilisateurs avec révocation en temps utile en cas de changement de rôle ou de cessation de contrat.
- Revues périodiques (au moins trimestrielles) des accès pour les rôles privilégiés et sensibles.

Cryptographie

- Chiffrement des données personnelles des clients en transit à l'aide de protocoles robustes (par exemple, TLS 1.2+).
- Chiffrement des données personnelles des clients au repos dans les bases de données de production en utilisant des algorithmes reconnus comme étant conformes aux normes industrielles (par exemple, AES 256).
- Gestion sécurisée des clés avec un accès restreint, une séparation des tâches et une rotation périodique des clés.

Sécurité du réseau et de l'infrastructure

- Segmentation du réseau, utilisation de pare-feu et de groupes de sécurité afin de limiter le trafic au strict nécessaire.
- Accès distant administratif sécurisé (par exemple, VPN avec authentification multi-facteurs).
- Protection contre les attaques DDoS et limitation du trafic quand cela s'applique.
- Systèmes synchronisés temporellement et configurations renforcées conformes aux référentiels reconnus.

Sécurité des applications et SDLC

- Cycle de développement sécurisé incluant la modélisation des menaces, la revue de code et la gestion des dépendances.
- Réalisation de tests de sécurité applicatifs statiques et dynamiques selon une cadence basée sur le risque.
- Processus de remédiation des vulnérabilités avec des délais établis selon le niveau de gravité.
- Environnements de développement, de test et de production distincts ; aucune utilisation de données personnelles réelles dans des environnements hors production, sauf si elles sont correctement pseudonymisées/anonymisées.

Gestion des vulnérabilités et des correctifs

- Analyse régulière des vulnérabilités de l'infrastructure et des applications.
- Délais de déploiement des correctifs basés sur une approche par niveau de risque pour les systèmes d'exploitation et les applications.
- Suivi et vérification des activités de remédiation.

Journalisation et surveillance

- Journalisation centralisée des événements ayant une importance pour la sécurité (par exemple, authentification, accès aux données sensibles, actions des administrateurs).
- Mise en place d'alertes et de mécanismes de surveillance pour détecter toute activité anormale ou suspecte.

- Protection des journaux contre toute altération non autorisée et conservation pour une durée définie afin de faciliter les enquêtes.

Sécurité des postes de travail

- Gestion des postes de travail avec solutions anti-malware/EDR, chiffrement des disques et renforcement de la sécurité.
- Gestion des appareils mobiles pour ceux accédant aux données personnelles des clients.
- Mises à jour régulières des systèmes d'exploitation et des applications.

Sécurité physique et environnementale

- Traitement des données dans des centres de données certifiés dotés de contrôles d'accès physiques, de registres de visiteurs et d'une surveillance permanente.
- Contrôles environnementaux (alimentation, climatisation, détection et suppression d'incendie) et mesures de protection contre les risques environnementaux.

Ségrégation et minimalisation des données

- Ségrégation logique des données des clients dans les environnements multi-tenants.
- Collecte limitée aux seules données nécessaires ; conservation alignée sur les exigences contractuelles et légales.

Sauvegardes et reprise après sinistre

- Réalisation régulière de sauvegardes chiffrées et immuables des données personnelles des clients, avec des durées de conservation définies.
- Tests périodiques de restauration.
- Plans de continuité des activités et de reprise après sinistre documentés avec des objectifs de récupération ; ces plans sont révisés et testés selon une fréquence déterminée.

Réponse aux incidents

- Plan documenté de réponse aux incidents couvrant la détection, le confinement, l'investigation, la remédiation et la reprise.
- Analyse des causes profondes et mise en œuvre d'actions correctives en cas d'incidents majeurs.
- Notification de toute violation au client conformément aux dispositions de l'Accord de traitement des données.

Sécurité du personnel et formation

- Vérifications des antécédents autorisées par la loi et adaptées aux exigences de chaque rôle.
- Engagements de confidentialité pour le personnel ayant accès aux données personnelles des clients.
- Formation régulière sur la sécurité et la protection de la vie privée dès l'intégration et par la suite.

Gestion des sous-traitants

- Réalisation d'une diligence raisonnable concernant les contrôles de sécurité et de confidentialité des sous-traitants.
- Transmission contractuelle aux sous-traitants des obligations en matière de protection des données et des exigences de sécurité.
- Tenue d'une liste actualisée des sous-traitants et notification des modifications conformément à l'Accord de traitement des données.

Suppression et restitution des données

- Suppression sécurisée des données personnelles des clients lors de la résiliation du contrat ou selon les instructions du client, incluant la suppression des copies résiduelles issues des sauvegardes selon des procédures définies de rétention et de cycle de vie des supports.
- Restitution des données personnelles des clients sur demande, dans la mesure du possible, dans un format standard.

Transferts internationaux

- Utilisation de mécanismes de transfert appropriés pour les transferts vers des pays tiers, le cas échéant, et mise en place des garanties pertinentes.
- Fourniture d'informations pour aider le client dans ses évaluations d'impact sur le transfert, dès lors qu'une demande raisonnable est formulée.

Audit et assurance

- Mise à disposition, sur demande du client et sous réserve de confidentialité, des rapports d'audit réalisés par des tiers et de la documentation de sécurité disponible.
- Soutien aux audits du client, comme prévu dans l'accord de traitement des données, tout en garantissant qu'aucune donnée ou information confidentielle appartenant à d'autres clients ne soit accessible.