

Accord de traitement des données

CONSIDÉRATIONS

Le présent accord de traitement des données (ci-après : « l'Accord de traitement ») constitue une annexe aux Conditions Générales de Payflip. Les Conditions Générales et l'Accord de traitement font ensemble partie intégrante de l'Accord conclu entre le Client et Payflip.

Par le présent Accord de traitement, les Parties souhaitent formaliser par écrit leurs accords mutuels concernant (i) la gestion, la sécurité et/ou le Traitement de ces Données à caractère personnel et (ii) l'obligation des Parties de respecter la Législation sur la vie privée.

Article 1 : définitions

Dans le présent Accord de traitement, les termes suivants (lorsqu'ils sont écrits avec une majuscule) ont la signification décrite dans cet Article :

Les termes « Accord », « Client », « Partie »/« Parties », « Services », « Payflip », « Durée », « Informations confidentielles », « RGPD », « Beneficiary Provider », « Employé » et « Outil » ont la signification qui leur est donnée dans les Conditions Générales.

Les termes « Responsable du traitement », « Personne concernée »,

« Violation de Données à caractère personnel », « Tiers », « Analyse d'impact relative à la protection des données », « Autorité de contrôle », « Sous-traitant » et « Traiter/Traitement » ont la signification qui leur est donnée dans la Législation sur la vie privée.

« **Données à caractère personnel** » : toutes les données à caractère personnel, telles que définies à l'Article 4(1) du RGPD, dont le Client est responsable en tant que Responsable du traitement et que Payflip s'attend à Traiter pour le compte du Client dans le cadre de la fourniture de ses Services, dont une liste non exhaustive figure à l'Annexe 1.

« **Sous-traitant ultérieur** » : tout Sous-traitant engagé par Payflip en tant que sous-traitant et autorisé à obtenir, dans le cadre du présent Accord de traitement, un accès logique à certaines Données à caractère personnel et à les traiter en vue de la fourniture de (parties des) Services ou d'un support technique, et qui s'engage à traiter ces Données à caractère personnel exclusivement pour et au nom du Responsable du traitement conformément au présent Accord de traitement.

« **Sous-traitant ultérieur substantiel** » : un Sous-traitant ultérieur qui constitue une composante essentielle et indispensable des Services, en ce qu'il Traite structurellement des Données à caractère personnel dans le cadre des Services. Cela comprend notamment (mais pas exclusivement) les fournisseurs impliqués dans l'hébergement, la gestion de bases de données, la fourniture de fonctionnalités essentielles ou intégrées et le support client. Les Sous-traitants ultérieurs qui ne Traitent des Données à caractère personnel que de manière incidente, complémentaire ou dans une mesure très limitée via Payflip, ou qui ne sont pas nécessairement liés à la fonctionnalité principale de l'Outil et/ou des Services, ne sont expressément pas considérés comme des Sous-traitants ultérieurs substantiels.

Le présent Accord de traitement contient les annexes suivantes :

- **Annexe I** : Aperçu de (i) les Données à caractère personnel que les Parties s'attendent à ce qu'elles soient traitées par Payflip dans le cadre des Services, (ii) les catégories de Personnes concernées auxquelles se rapportent les Données à caractère personnel, (iii) l'utilisation prévue (c'est-à-dire le(s) mode(s) de Traitement) des Données à caractère personnel et (iv) les finalités et moyens convenus de ce Traitement.
- **Annexe II** : Aperçu et description des mesures de sécurité techniques et organisationnelles prises par Payflip dans le cadre du présent Accord de traitement.
- **Annexe III** : Aperçu des différents Sous-traitants ultérieurs substantiels auxquels Payflip fait appel.

Article 2 : qualité des parties

2.1 Pour la fourniture des Services, Payflip traite les Données à caractère personnel mentionnées à l'Annexe I. Le Client agit en tant que Responsable du traitement au sens de la Législation sur la vie privée et confie le traitement de ces Données à caractère personnel à Payflip, qui les traite au nom et pour le compte du Client en tant que Sous-traitant.

2.2 Le présent Accord de traitement concerne exclusivement le rôle de Payflip en tant que Sous-traitant. Pour plus d'informations sur le traitement des Données à caractère personnel par Payflip dans son

rôle de Responsable du traitement, nous renvoyons à la Politique de confidentialité.

2.3 Le Client et Payflip sont désignés respectivement comme le « RESPONSABLE DU TRAITEMENT » et le « SOUS-TRAITANT » pour la suite du présent Accord de traitement.

Article 3 : obligations mutuelles

3.1 Les deux Parties s'engagent expressément à respecter les dispositions de la Législation sur la vie privée et à ne rien faire ou omettre qui pourrait amener l'autre Partie à violer la Législation sur la vie privée. Les deux Parties s'engagent à prendre des mesures appropriées pour garantir que les Données à caractère personnel ne sont pas utilisées de manière inappropriée ou obtenues par un Tiers non autorisé.

3.2 Le SOUS-TRAITANT traitera les Données à caractère personnel de manière appropriée et soigneuse, conformément à la Législation sur la vie privée, aux dispositions du présent Accord de traitement et aux instructions écrites du RESPONSABLE DU TRAITEMENT. Plus particulièrement, le SOUS-TRAITANT mettra tout son savoir-faire à disposition lors de l'exécution des Services pour exécuter les Services selon les règles de l'art, comme il convient à un Sous-traitant spécialisé et « de bonne qualité ».

3.3 Le RESPONSABLE DU TRAITEMENT est propriétaire et entièrement responsable du Traitement des Données à caractère personnel, y compris la nature et la finalité du Traitement, la proportionnalité, les durées de conservation, et l'exactitude, la qualité et la licéité des Données à caractère personnel ainsi que la manière dont il a acquis ces Données à caractère personnel. Cette responsabilité et ce contrôle n'incombent jamais à Payflip.

Article 4 : durée du traitement

4.1 Le présent Accord de traitement reste applicable tant que le SOUS-TRAITANT traite des Données à caractère personnel au nom et pour le compte du RESPONSABLE DU TRAITEMENT dans le cadre de l'Accord. Lorsque l'Accord prend fin, le présent Accord de traitement prend également fin.

4.2 En cas de violation du présent Accord ou des dispositions applicables de la Législation sur la vie privée par le SOUS-TRAITANT, le RESPONSABLE DU TRAITEMENT peut ordonner au SOUS-TRAITANT de cesser immédiatement le Traitement des Données à caractère personnel.

4.3 Le SOUS-TRAITANT ne conserve les Données à caractère personnel que pendant la durée nécessaire à l'exécution des Services.

(i) Pendant la durée de l'Accord, le SOUS-TRAITANT pseudonymise ou anonymise les Données à caractère personnel dès qu'elles ne sont plus pertinentes pour l'exécution des Services. À la demande du RESPONSABLE DU TRAITEMENT ou de la Personne concernée, le SOUS-TRAITANT supprime définitivement les Données à caractère personnel concernées.

(ii) Après l'expiration de l'Accord, le SOUS-TRAITANT supprime toutes les Données à caractère personnel dans un délai de trente (30) jours calendaires, ou plus tôt si le Client en fait la demande. Si le droit applicable exige une conservation plus longue, le SOUS-TRAITANT peut conserver les Données à caractère personnel aussi longtemps que légalement nécessaire. Les copies de sauvegarde contenant des Données à caractère personnel peuvent être conservées pendant un maximum d'un (1) an. À la demande expresse du RESPONSABLE DU TRAITEMENT, le SOUS-TRAITANT peut restituer les Données à caractère personnel au RESPONSABLE DU TRAITEMENT au moyen d'une exportation. Cette exportation s'effectue selon les modalités décrites dans les Conditions Générales.

Article 5 : assistance au responsable du traitement

5.1 **Respect de la législation.** Compte tenu de la nature du Traitement et des informations à sa disposition, le SOUS-TRAITANT assiste le RESPONSABLE DU TRAITEMENT dans l'exécution des obligations découlant des Articles 32 à 36 du RGPD.

5.2 **Violation de Données à caractère personnel.** En cas de Violation de Données à caractère personnel concernant l'objet du Traitement du présent Accord, le SOUS-TRAITANT informe le RESPONSABLE DU TRAITEMENT sans délai, dès qu'il a pris connaissance d'une Violation de Données à caractère personnel.

Cette notification contient au minimum les informations suivantes :

- (a) La nature de la Violation de Données à caractère personnel ;
- (b) Les catégories de Données à caractère personnel concernées par

la Violation de Données à caractère personnel ;
 (c) Les catégories de Personnes concernées en question et, approximativement, le nombre de Personnes concernées en question ;
 (d) Les catégories de registres de données à caractère personnel en question et, approximativement, leur nombre ;
 (e) Les conséquences probables de la Violation de Données à caractère personnel ;
 (f) Les mesures proposées ou prises pour remédier à la Violation de Données à caractère personnel, y compris, le cas échéant, les mesures visant à limiter les éventuelles conséquences négatives de celle-ci.

5.3 Si le SOUS-TRAITANT fait appel à un Sous-traitant ultérieur, le SOUS-TRAITANT imposera au Sous-traitant ultérieur de lui fournir les mêmes informations en cas de Violation de Données à caractère personnel chez le Sous-traitant ultérieur. Le SOUS-TRAITANT transmet immédiatement au RESPONSABLE DU TRAITEMENT les informations qu'il reçoit du Sous-traitant ultérieur.

5.4 Le SOUS-TRAITANT et son/ses Sous-traitant(s) ultérieur(s) désignent parmi leurs Employés une personne qui constitue un point de contact unique (single point of contact) et qui est responsable de toute communication entre le SOUS-TRAITANT, le(s) Sous-traitant(s) ultérieur(s) et le RESPONSABLE DU TRAITEMENT en cas d'incident ayant entraîné ou pouvant entraîner une destruction ou une perte accidentelle ou illicite, un accès, une modification ou une transmission non autorisés de Données à caractère personnel traitées pour le compte du RESPONSABLE DU TRAITEMENT.

5.5 Seul le RESPONSABLE DU TRAITEMENT décide, à sa discrétion et conformément à la Législation sur la vie privée, si les Personnes concernées dont les Données à caractère personnel sont affectées par une Violation de Données à caractère personnel en sont informées. Il appartient au RESPONSABLE DU TRAITEMENT de notifier l'Autorité de contrôle d'une Violation de Données à caractère personnel.

5.6 Les Parties, et le cas échéant le(s) Sous-traitant(s) ultérieur(s), garantissent qu'elles coopèrent de bonne foi pour limiter les éventuelles conséquences négatives d'une Violation de Données à caractère personnel.

5.7 Analyse d'impact relative à la protection des données (AIPD). De plus, le SOUS-TRAITANT assiste le RESPONSABLE DU TRAITEMENT lorsque celui-ci effectue une Analyse d'impact relative à la protection des données conformément à l'Article 35 du RGPD.

Article 6 : obligations d'information

6.1 Le SOUS-TRAITANT fournira à tout moment, sur demande du RESPONSABLE DU TRAITEMENT (une telle demande devant toutefois accorder au SOUS-TRAITANT un délai raisonnable pour satisfaire à la demande), au RESPONSABLE DU TRAITEMENT toutes les informations dont il a besoin et au minimum les informations déterminées par les dispositions de cette clause :

- Toutes les données pertinentes sur sa propre structure d'entreprise ainsi que des données d'identification exactes et actualisées sur toutes les entités du SOUS-TRAITANT impliquées dans le traitement de Données à caractère personnel, y compris l'emplacement de leur siège principal ;
- Les aspects du traitement pour lesquels on fait ou souhaite faire appel aux services du Sous-traitant ultérieur et les données d'identification d'un Sous-traitant ultérieur, y compris l'emplacement de son siège principal. Le SOUS-TRAITANT transmet au RESPONSABLE DU TRAITEMENT l'accord avec le(s) Sous-traitant(s) ultérieur(s) qui concerne ou est pertinent pour le traitement de Données à caractère personnel, à moins qu'un tel accord avec le(s) Sous-traitant(s) ultérieur(s) ne contienne des Informations confidentielles, auquel cas il peut supprimer ces Informations confidentielles ;
- Les données géographiques sur les emplacements du traitement, y compris les possibilités de sauvegarde et les possibilités de détruire les données ;
- Les mesures de sécurité physiques, organisationnelles, techniques et logiques prises par le SOUS-TRAITANT et son/ses Sous-traitant(s) ultérieur(s), telles que déterminées à l'Article 11 du présent Accord.

Article 7 : obligations du sous-traitant

7.1 Le SOUS-TRAITANT traite immédiatement ou dans un délai raisonnable (selon les obligations légales déterminées dans le RGPD) et de manière appropriée toutes les demandes raisonnables du RESPONSABLE DU TRAITEMENT concernant le traitement de Données à caractère personnel liées au présent Accord.

7.2 Le SOUS-TRAITANT garantit qu'aucune obligation ne découle de la législation applicable qui l'empêcherait de respecter les obligations du présent Accord.

7.3 Le SOUS-TRAITANT s'engage à traiter les Données à caractè-

ère personnel uniquement dans le but de fournir les Services et de satisfaire aux responsabilités du présent Accord conformément aux instructions écrites du RESPONSABLE DU TRAITEMENT. Le SOUS-TRAITANT ne peut et ne traitera que les Données à caractère personnel mentionnées à l'Annexe 1, conformément aux activités de Traitement convenues et exclusivement pour les finalités qui y sont déterminées, sauf si la législation en dispose expressément autrement, auquel cas le SOUS-TRAITANT en informe immédiatement le RESPONSABLE DU TRAITEMENT.

7.4 Le RESPONSABLE DU TRAITEMENT peut apporter unilatéralement des modifications limitées aux instructions. Le SOUS-TRAITANT est consulté avant que des modifications importantes ne soient apportées aux instructions. Les deux Parties doivent consentir aux modifications qui ont un impact sur les principales dispositions de l'Accord. Le SOUS-TRAITANT peut refuser de suivre les instructions du RESPONSABLE DU TRAITEMENT si le SOUS-TRAITANT juge raisonnablement que les instructions sont potentiellement contraires à la Législation sur la vie privée (cf. art. 8.3) ou à d'autres législations impératives (cf. Article 8.5), auquel cas le SOUS-TRAITANT en informe immédiatement le RESPONSABLE DU TRAITEMENT.

7.5 Le SOUS-TRAITANT garantit que l'accès, l'inspection, le traitement et la fourniture de Données à caractère personnel ne se font que conformément au principe de proportionnalité et au principe du « besoin de savoir » (c'est-à-dire que les données ne sont fournies qu'aux personnes qui ont besoin des Données à caractère personnel pour exécuter les Services).

7.6 Le SOUS-TRAITANT s'engage à ne fournir des Données à caractère personnel qu'aux Employés du RESPONSABLE DU TRAITEMENT qui ont besoin des Données à caractère personnel pour satisfaire aux obligations du présent Accord et veille à ce que l'Employé concerné s'engage à respecter la confidentialité ou soit lié par une obligation légale de confidentialité, sauf si une telle fourniture est prévue en vertu de l'Accord principal.

Article 8 : obligations du responsable du traitement

8.1 Le RESPONSABLE DU TRAITEMENT fournit toute l'assistance nécessaire au SOUS-TRAITANT et coopère de bonne foi avec lui pour garantir que lors de chaque Traitement de Données à caractère personnel, les prescriptions du RGPD sont respectées, en particulier les principes relatifs au Traitement de Données à caractère personnel.

8.2 Le RESPONSABLE DU TRAITEMENT convient avec le SOUS-TRAITANT de canaux de communication appropriés pour garantir que les instructions, directives et autres communications concernant les Données à caractère personnel traitées par le SOUS-TRAITANT pour le compte du RESPONSABLE DU TRAITEMENT sont bien reçues par les Parties. Le RESPONSABLE DU TRAITEMENT informe le SOUS-TRAITANT de l'identité de la personne qui constitue le point de contact unique (le « single point of contact ») du RESPONSABLE DU TRAITEMENT avec qui le SOUS-TRAITANT doit prendre contact en application de cet Article 8.2.

8.3 Le RESPONSABLE DU TRAITEMENT fera de son mieux pour ne donner au SOUS-TRAITANT que des instructions, directives ou communications conformes aux dispositions du RGPD.

8.4 Le RESPONSABLE DU TRAITEMENT fournit au SOUS-TRAITANT et/ou à son/ses Sous-traitant(s) ultérieur(s) l'assistance nécessaire dans la mesure où une demande, un ordre, une enquête ou une citation à comparaître d'une autorité nationale compétente (telle qu'une Autorité de contrôle) ou d'une instance judiciaire concerne le Traitement de Données à caractère personnel dont le RESPONSABLE DU TRAITEMENT est responsable et que l'intervention du RESPONSABLE DU TRAITEMENT est nécessaire pour s'y conformer.

8.5 Le RESPONSABLE DU TRAITEMENT fera de son mieux pour ne pas donner d'instructions, de directives ou de demandes au SOUS-TRAITANT qui obligerait le SOUS-TRAITANT et/ou son/ses Sous-traitant(s) ultérieur(s) à violer des obligations imposées par la législation nationale impérative applicable au SOUS-TRAITANT et/ou à son/ses Sous-traitant(s) ultérieur(s).

8.6 Le RESPONSABLE DU TRAITEMENT garantit qu'il coopère de bonne foi avec le SOUS-TRAITANT pour limiter les effets négatifs d'un incident de sécurité ayant un impact sur les Données à caractère personnel traitées pour le compte du RESPONSABLE DU TRAITEMENT par le SOUS-TRAITANT et/ou son/ses Sous-traitant(s) ultérieur(s).

Article 9 : l'utilisation de sous-traitants ultérieurs

9.1 Le SOUS-TRAITANT ne peut engager des Sous-traitants ultérieurs substantiels pour effectuer des traitements spécifiques de Données à caractère personnel pour le compte du RESPONSABLE DU TRAITEMENT qu'avec l'autorisation écrite préalable du RESPONSABLE DU TRAITEMENT. En signant le présent Accord de traitement, le

RESPONSABLE DU TRAITEMENT consent par la présente à la liste des Sous-traitants ultérieurs substantiels telle que mentionnée à l'Annexe 1 du présent Accord.

9.2 Le SOUS-TRAITANT informe le RESPONSABLE DU TRAITEMENT par écrit de toute modification envisagée (ajout ou remplacement ; pas : suppression) de Sous-traitants ultérieurs substantiels, le RESPONSABLE DU TRAITEMENT ayant la possibilité de formuler une objection motivée à de telles modifications dans un délai de dix (10) jours calendaires.

9.3 Si le RESPONSABLE DU TRAITEMENT, conformément à l'Article 9.2, formule une objection motivée à l'engagement d'un nouveau Sous-traitant ultérieur substantiel, et que cette objection n'est pas jugée déraisonnable ou infondée, le SOUS-TRAITANT, en consultation avec le RESPONSABLE DU TRAITEMENT, fera tous les efforts raisonnables pour trouver une solution appropriée. Si aucune solution ne peut être trouvée, le Client a le droit de résilier l'Accord, dans la mesure où les Services concernés ne peuvent être fournis sans recourir au Sous-traitant ultérieur substantiel contesté.

9.4 Le SOUS-TRAITANT veille à ce que son/ses Sous-traitant(s) ultérieur(s) (substantiel(s)) soient liés par les mêmes obligations concernant les Données à caractère personnel que celles qui lient le SOUS-TRAITANT en vertu du présent Accord.

9.5 Le SOUS-TRAITANT transmettra avec exactitude et immédiatement les finalités déterminées et les instructions données par le RESPONSABLE DU TRAITEMENT au(x) Sous-traitant(s) ultérieur(s) (substantiel(s)) lorsque et où ces finalités et instructions concernent la partie du traitement à laquelle le(s) Sous-traitant(s) ultérieur(s) (substantiel(s)) est (sont) associé(s).

Article 10 : droits des personnes concernées

10.1 Compte tenu de la nature du traitement, le SOUS-TRAITANT assiste le RESPONSABLE DU TRAITEMENT au moyen de mesures techniques et organisationnelles appropriées, dans la mesure du possible, dans l'accomplissement de son devoir de répondre aux demandes d'exercice des droits de la Personne concernée établis au chapitre III du RGPD ;

10.2 Les conditions suivantes s'appliquent à chaque demande de Personnes concernées concernant leurs droits relatifs au Traitement par le SOUS-TRAITANT et/ou son/ses Sous-traitant(s) ultérieur(s) de Données à caractère personnel les concernant :

- Le SOUS-TRAITANT fera de son mieux pour informer immédiatement le RESPONSABLE DU TRAITEMENT de toute demande d'une Personne concernée concernant des Données à caractère personnel que le SOUS-TRAITANT et/ou son/ses Sous-traitant(s) ultérieur(s) traitent pour le compte du RESPONSABLE DU TRAITEMENT, sans donner suite à une telle demande sauf si le RESPONSABLE DU TRAITEMENT y consent expressément ;
- Le SOUS-TRAITANT donne immédiatement suite et impose à son/ses Sous-traitant(s) ultérieur(s) de donner immédiatement suite à toute demande du RESPONSABLE DU TRAITEMENT afin que le RESPONSABLE DU TRAITEMENT puisse donner suite à une demande de la Personne concernée qui souhaite exercer l'un de ses droits ;
- Le SOUS-TRAITANT veille à ce que lui-même ainsi que son/ses Sous-traitant(s) ultérieur(s) disposent des compétences techniques et organisationnelles requises pour bloquer l'accès aux Données à caractère personnel et détruire physiquement les données sans aucune possibilité de les récupérer si et quand le RESPONSABLE DU TRAITEMENT en fait la demande ;
- Le SOUS-TRAITANT fournit, sur simple demande du RESPONSABLE DU TRAITEMENT et au mieux de ses efforts, toute l'assistance nécessaire et toutes les informations requises dont le RESPONSABLE DU TRAITEMENT a besoin pour défendre ses intérêts dans toute forme de procédure – procédure judiciaire, arbitrage ou autre – intentée contre le RESPONSABLE DU TRAITEMENT ou son Employé en raison d'une violation des droits fondamentaux à la vie privée et à la protection des Données à caractère personnel des Personnes concernées.

Article 11 : mesures de sécurité

11.1 Pendant la durée du présent Accord, le SOUS-TRAITANT prend et maintient des mesures techniques et organisationnelles appropriées de telle manière que le traitement réponde aux exigences du RGPD et que la protection des droits de la Personne concernée soit garantie.

Le SOUS-TRAITANT prendra notamment des mesures techniques et organisationnelles pour protéger (i) les Données à caractère personnel, y compris la sécurité contre une utilisation et/ou un Traitement négligent, inapproprié, non autorisé ou illicite et contre la perte, la destruction ou les dommages involontaires, et (ii) la confidentialité et l'intégrité des Données à caractère personnel, comme exposé à l'Annexe 2.

11.2 Le SOUS-TRAITANT prendra plus particulièrement des mesures techniques et organisationnelles appropriées pour garantir un niveau

de sécurité adapté au risque, conformément à l'Article 32 du RGPD.

11.3 Lors de l'évaluation du niveau de sécurité approprié, il a notamment été tenu compte des risques de traitement, notamment en raison de la destruction, de la perte, de la modification ou de la divulgation non autorisée de, ou de l'accès non autorisé à des Données à caractère personnel transmises, stockées ou autrement traitées, que ce soit accidentellement ou illicitement.

11.4 Le RESPONSABLE DU TRAITEMENT se réserve le droit de suspendre et/ou de résilier l'Accord lorsque le SOUS-TRAITANT ne peut plus fournir de mesures techniques et organisationnelles adaptées au risque de traitement.

Article 12 : audit

12.1 Le SOUS-TRAITANT reconnaît que le RESPONSABLE DU TRAITEMENT est sous la surveillance d'une/de plusieurs Autorité(s) de contrôle. Le SOUS-TRAITANT reconnaît que chaque Autorité de contrôle concernée a le droit d'effectuer un audit à tout moment et en tout cas pendant les heures de bureau normales du SOUS-TRAITANT, pendant la durée du présent Accord, pour évaluer si le SOUS-TRAITANT respecte la Législation sur la vie privée et les dispositions du présent Accord. Le SOUS-TRAITANT fournira la coopération nécessaire.

12.2 Le RESPONSABLE DU TRAITEMENT a le droit de vérifier ou de faire vérifier le respect par le SOUS-TRAITANT du présent Accord de traitement et de la Législation sur la vie privée applicable. Un tel audit peut avoir lieu au maximum une (1) fois par Durée, sauf s'il existe des raisons fondées d'effectuer un audit supplémentaire (comme en cas de suspicion d'une Violation de Données à caractère personnel non signalée, d'une enquête en cours par une Autorité de contrôle ou de soupçons sérieux de fraude). Le RESPONSABLE DU TRAITEMENT informe le SOUS-TRAITANT par écrit au moins trente (30) jours à l'avance de son intention d'effectuer un audit. La notification mentionne le nom de l'auditeur, ainsi que l'objectif et la portée de l'audit.

12.3 Le SOUS-TRAITANT met à disposition du RESPONSABLE DU TRAITEMENT, dans le cadre de l'Accord, toutes les informations raisonnables pour démontrer qu'il respecte ses obligations en vertu du présent Accord ou de la Législation sur la vie privée. Si les informations et rapports fournis par le SOUS-TRAITANT en vertu de cet Article sont insuffisants pour permettre au RESPONSABLE DU TRAITEMENT de démontrer que les obligations en vertu de la Législation sur la vie privée sont respectées, le SOUS-TRAITANT et le RESPONSABLE DU TRAITEMENT se réunissent pour convenir des conditions opérationnelles, de sécurité et financières d'une inspection technique sur place. Les conditions de cette inspection ne peuvent en aucun cas porter atteinte à la sécurité des autres clients du SOUS-TRAITANT.

12.4 Sur demande écrite du RESPONSABLE DU TRAITEMENT, le SOUS-TRAITANT fournit au RESPONSABLE DU TRAITEMENT, à un tiers indépendant, à un auditeur reconnu ou à un auditeur désigné par le RESPONSABLE DU TRAITEMENT ou l'Autorité de contrôle concernée, l'accès aux parties pertinentes de l'administration du SOUS-TRAITANT et à toutes les informations et tous les emplacements pertinents pour le SOUS-TRAITANT (et à ceux de ses agents, filiales et sous-traitants) pour déterminer si le SOUS-TRAITANT respecte la Législation sur la vie privée et les dispositions du présent Accord. À la demande du SOUS-TRAITANT, les parties concernées concluent un accord de confidentialité.

12.5 Le RESPONSABLE DU TRAITEMENT garantit que l'audit est effectué d'une manière qui perturbe le moins possible les opérations commerciales du SOUS-TRAITANT et la prestation de services à ses clients. L'audit a lieu pendant les heures de bureau normales du SOUS-TRAITANT et dans des conditions de stricte confidentialité.

12.6 Si le SOUS-TRAITANT et le RESPONSABLE DU TRAITEMENT s'accordent sur une lacune substantielle dans le respect de la Législation sur la vie privée et/ou de l'Accord, comme cela ressort de l'audit, le SOUS-TRAITANT remédie à cette lacune aussi rapidement que possible. Les Parties peuvent convenir d'établir un plan, incluant un calendrier pour sa mise en œuvre, pour remédier aux lacunes mises en lumière lors de l'audit.

12.7 Le RESPONSABLE DU TRAITEMENT supporte les coûts de chaque audit effectué au sens de cet Article, sauf si l'audit révèle que le SOUS-TRAITANT n'a manifestement pas respecté la Législation sur la vie privée et/ou les dispositions du présent Accord, auquel cas le SOUS-TRAITANT supporte les coûts d'un tel audit.

Article 13 : transfert à des tiers

13.1 Le transfert de Données à caractère personnel à des Tiers de quelque manière que ce soit est interdit, sauf s'il est légalement prescrit ou si le SOUS-TRAITANT a obtenu l'autorisation expresse du RESPONSABLE DU TRAITEMENT pour ce faire. Si une obligation légale s'applique au transfert à des Tiers de Données à caractère personnel couvertes par

le présent Accord, le SOUS-TRAITANT en informe le RESPONSABLE DU TRAITEMENT avant le transfert.

13.2 Le Responsable du traitement peut demander au SOUS-TRAITANT de transférer des Données à caractère personnel à des prestataires de services tiers (tels que des Benefit Providers ou des partenaires de paie) avec lesquels le RESPONSABLE DU TRAITEMENT a conclu un accord distinct. Ce transfert peut avoir lieu manuellement ou via des intégrations techniques au sein de l'Outil. Ces prestataires de services tiers ne sont pas des Sous-traitants ultérieurs du SOUS-TRAITANT, mais traitent les Données à caractère personnel en tant que Responsables du traitement indépendants ou en tant que Sous-traitants du RESPONSABLE DU TRAITEMENT. Le RESPONSABLE DU TRAITEMENT garantit au SOUS-TRAITANT qu'il a conclu avec ces prestataires de services tiers des accords contractuels appropriés concernant la protection des données et reste responsable de la relation avec ces parties. Le rôle du SOUS-TRAITANT se limite à faciliter techniquement le transfert de données sur instruction du RESPONSABLE DU TRAITEMENT.

Article 14 : transfert international

14.1. Le SOUS-TRAITANT ne peut transférer ou stocker des Données à caractère personnel dans un pays tiers en dehors de l'Espace économique européen (« EEE ») ou auprès d'une organisation internationale que dans la mesure où cela est nécessaire à l'exécution de l'Accord et à condition que cela se fasse conformément à la Législation sur la vie privée applicable et aux dispositions du présent Accord de traitement.

14.2. Un tel transfert ne peut avoir lieu que si l'une des conditions suivantes est remplie :

- a) le pays tiers ou l'organisation internationale est reconnu par la Commission européenne comme un pays ayant un niveau de protection adéquat (décision d'adéquation) ; ou
- b) le transfert est soumis à des garanties appropriées au sens de l'Article 46 du RGPD, à condition que les personnes concernées disposent de droits opposables et de voies de recours effectives. Ces garanties peuvent notamment consister en :
 - i. des règles d'entreprise contraignantes ;
 - ii. les clauses contractuelles types relatives à la protection des données telles qu'établies par la Commission européenne dans la Décision 2021/914/UE du 4 juin 2021 ou tout successeur de celle-ci ;
 - iii. un code de conduite approuvé ou un mécanisme de certification approuvé.

14.3. Le SOUS-TRAITANT informe préalablement le RESPONSABLE DU TRAITEMENT lorsqu'une modification de la liste des Sous-traitants ultérieurs substantiels (voir Article 9.2) entraîne un transfert de Données à caractère personnel en dehors de l'EEE. Le RESPONSABLE DU TRAITEMENT accepte la liste actuelle des Sous-traitants ultérieurs substantiels et les transferts associés (voir Annexe 3).

14.4 Si le SOUS-TRAITANT est obligé de transférer des Données à caractère personnel en vertu du droit de l'Union ou du droit d'un État membre applicable, le SOUS-TRAITANT en informera le RESPONSABLE DU TRAITEMENT avant le transfert, sauf si cette législation interdit la notification pour des raisons importantes d'intérêt général.

Article 15 : conduite à l'égard des organes et autorités gouvernementaux nationaux

15.1 Le SOUS-TRAITANT informe immédiatement le RESPONSABLE DU TRAITEMENT de toute demande, ordre, enquête ou citation à comparaître adressé au SOUS-TRAITANT ou à son Sous-traitant ultérieur substantiel par une autorité nationale compétente ou une instance judiciaire et qui implique la communication des Données à caractère personnel traitées par le SOUS-TRAITANT ou un Sous-traitant ultérieur substantiel ou de toutes données et/ou informations liées à un tel Traitement par le SOUS-TRAITANT pour et au nom du RESPONSABLE DU TRAITEMENT.

15.2 Sans préjudice de l'Article 15.1 du présent Accord, le SOUS-TRAITANT garantit qu'il n'existe aucune obligation de droit législatif applicable qui rendrait impossible pour le SOUS-TRAITANT de respecter ses obligations en vertu du présent Accord.

Article 16 : responsabilité

16.1 Le RESPONSABLE DU TRAITEMENT impliqué dans le traitement est responsable des dommages causés par un Traitement contraire à la Législation sur la vie privée et au présent Accord. Sans préjudice des Conditions Générales, le SOUS-TRAITANT n'est responsable des dommages causés par le Traitement que s'il n'a pas respecté les obligations de la Législation sur la vie privée qui sont spécifiquement destinées aux Sous-traitants ou lorsqu'il a agi en dehors ou contrairement au présent Accord de traitement ou aux instructions légitimes du RESPONSABLE DU TRAITEMENT.

16.2 Le RESPONSABLE DU TRAITEMENT ou le SOUS-TRAITANT est exempté de responsabilité en vertu du point 16.1 s'il prouve qu'il n'est en aucune façon responsable de l'événement qui a causé le dommage.

16.3 Chaque Partie n'est responsable que des amendes administratives ou autres sanctions qui lui sont imposées par une Autorité de contrôle, dans la mesure où elles sont la conséquence directe d'une violation de la Législation sur la vie privée ou du présent Accord imputable à cette Partie. Aucune des Parties ne peut répercuter sur l'autre Partie le paiement d'une amende administrative ou d'une sanction résultant de sa propre violation de la Législation sur la vie privée ou du présent Accord de traitement.

16.4 Lorsqu'il s'avère que le SOUS-TRAITANT et le RESPONSABLE DU TRAITEMENT sont tous deux responsables des dommages causés par le traitement de Données à caractère personnel, les deux Parties sont responsables et paient toutes deux une indemnisation proportionnellement à leur part individuelle de responsabilité pour les dommages causés par le traitement.

16.5 Lorsque le RESPONSABLE DU TRAITEMENT et le SOUS-TRAITANT sont tous deux impliqués dans le même traitement et qu'ils sont responsables en vertu des points 16.1 et 16.4 des dommages causés par le Traitement, le RESPONSABLE DU TRAITEMENT et le SOUS-TRAITANT sont tous deux tenus responsables de l'intégralité du dommage, afin de garantir une indemnisation effective de la Personne concernée.

16.6 Lorsque le RESPONSABLE DU TRAITEMENT ou le SOUS-TRAITANT a payé l'indemnisation complète pour les dommages subis conformément au point 16.5, ce RESPONSABLE DU TRAITEMENT ou ce SOUS-TRAITANT a le droit de réclamer à l'autre la partie de l'indemnisation correspondant à leur part de responsabilité pour les dommages, conformément aux conditions du point 16.1 et/ou conformément à la limitation de responsabilité déterminée dans cet Article 16.

16.7 La limitation de responsabilité incluse dans les Conditions Générales s'applique intégralement au présent Accord de traitement. La responsabilité du SOUS-TRAITANT en vertu du présent Accord de traitement ne dépassera en aucun cas les limites convenues dans les Conditions Générales.

Article 17 : médiation et juridiction

17.1 Le SOUS-TRAITANT accepte que si la Personne concernée intente une action en dommages-intérêts contre lui en vertu du présent Accord, le SOUS-TRAITANT acceptera la décision de la Personne concernée :

- De soumettre le litige à une personne indépendante pour médiation ;
- De soumettre le litige aux tribunaux en Belgique.

17.2 Les Parties conviennent que le choix de la Personne concernée ne porte pas atteinte à ses droits matériels ou procéduraux de recours conformément à d'autres dispositions de la législation nationale ou internationale applicable.

17.3 Tout litige entre les Parties concernant les conditions du présent Accord sera porté devant les tribunaux compétents comme déterminé dans les Conditions Générales.

Annexe 1 : Traitement de Données à caractère personnel par Payflip

Cette annexe contient un aperçu des Données à caractère personnel que Payflip s'attend à Traiter pour le compte du Client dans le cadre de l'Accord, ainsi que les catégories concernées de Personnes concernées, le(s) mode(s) de Traitement de Données à caractère personnel et les moyens et finalités du Traitement.

1. Catégories de Données à caractère personnel

Données personnelles

- Nom complet
- Adresse e-mail (professionnelle ou privée)
- Signature
- Adresse
- Numéro de téléphone

Données de travail

- Date d'entrée en service dans l'entreprise (le Client)
- Commission paritaire
- Identifiant externe du fournisseur de paie de l'entreprise (le Client)
- Contrat salarial

Données salariales

- Salaire mensuel brut
- Prime de fin d'année
- Coefficient ONSS (employeur et employé)

Données bancaires (pour le remboursement des avantages)

- IBAN
- Nom de l'institution bancaire

Données automobiles (pour le budget mobilité)

- Prix de leasing / TCO
- Période de leasing
- Plaque d'immatriculation
- Données de localisation (stations de recharge/ravitaillement)

Données modifiables par les Employés

Les Employés peuvent gérer ou mettre à jour eux-mêmes les données suivantes via l'Outil :

- Adresse
- Langue préférée (NL, FR ou EN)
- Documents pouvant être téléchargés à nouveau

Les Données à caractère personnel mentionnées dans cet aperçu ne sont pas qualifiées de catégories particulières de Données à caractère personnel au sens de l'Article 9 du RGPD. Payflip, dans sa qualité de Sous-traitant, traite exclusivement des données d'identification et liées au travail nécessaires à l'exécution des Services pour le compte du Client.

Cela n'empêche pas que certaines Données à caractère personnel, notamment les données financières et de paie (telles que les données salariales, les numéros de compte bancaire et les composantes salariales contractuelles), sont considérées en pratique comme sensibles et confidentielles. Payflip accorde à ces données un niveau de protection approprié et renforcé.

Tout traitement de catégories particulières de Données à caractère personnel par le Client (par exemple via des documents téléchargés par les Employés) est en dehors de l'intention et de la responsabilité de Payflip et reste entièrement sous la responsabilité exclusive du Client en tant que Responsable du traitement.

2. Catégories de Personnes concernées

Employés du Client ayant accès à l'Outil

3. Finalités du traitement

Payflip traite ces Données à caractère personnel exclusivement pour l'exécution des Services dans le cadre de l'Accord, y compris notamment :

- La gestion et l'exécution des avantages ou options de rémunération offerts par le Client aux Employés ;
- Le soutien au Client dans l'utilisation de la plateforme et des fonctionnalités techniques nécessaires à l'exécution des Services ;
- La facilitation de l'échange de données avec des prestataires de services tiers sélectionnés par le Client, tels que des partenaires de paie ou des Benefit Providers, sur instruction du Client ;
- L'accomplissement d'opérations administratives, techniques et liées à la sécurité nécessaires à l'exécution de l'Accord.

Indépendamment de son rôle de Sous-traitant, Payflip peut traiter des Données à caractère personnel limitées des Employés pour générer des données d'utilisation anonymisées et agrégées. Ces données d'utilisation sont traitées par Payflip en tant que Responsable du traitement indépendant à des fins commerciales légitimes, telles que l'analyse statistique, la recherche, la formation, l'amélioration des produits et la sécurité de la plateforme. De plus, Payflip, en tant que Responsable du traitement, est autorisé à anonymiser et agréger les données du Client saisies par le Client ou ses Employés dans l'Outil. Ces données anonymisées du Client sont utilisées exclusivement à des fins internes, en particulier pour améliorer les Services. Ces deux activités de traitement sont en dehors de la portée du présent Accord de traitement et sont régies par la Politique de confidentialité de Payflip et la Législation sur la vie privée applicable.

4. Mode et moyens de traitement

- Mode de traitement : électronique via l'Outil, y compris les synchronisations automatiques avec des prestataires de services tiers sélectionnés par le Client (par ex. partenaires de paie, Benefit Providers).
- Moyens de traitement : l'Outil, serveurs sécurisés, sauvegardes et stockage de documents au sein de l'Outil.
- Sécurité : le traitement s'effectue avec des mesures techniques et organisationnelles appropriées telles que décrites à l'Annexe 2.

Annexe 2 : Mesures techniques et organisationnelles

Cette annexe décrit les mesures techniques et organisationnelles que Payflip, en tant que Sous-traitant, applique pour le traitement des Données à caractère personnel du Responsable du traitement. Les mesures visent à garantir la confidentialité, l'intégrité et la disponibilité des Données à caractère personnel, conformément à l'Article 32 du RGPD.

1. Infrastructure de sécurité

- Les Données à caractère personnel sont stockées dans une infrastructure cloud Microsoft Azure sécurisée au sein de l'Union européenne.
- Les bases de données disposent de répliques pour la redondance et la disponibilité, afin d'éviter la perte de données et de garantir la continuité.
- L'accès aux serveurs et bases de données est géré via les contrôles d'accès basés sur les rôles et l'authentification d'Azure.

2. Sécurité des données au repos et en transit

- Les Données à caractère personnel sont chiffrées au repos (chiffrement de base de données) et chiffrées en transit (TLS/HTTPS).
- Les données sensibles telles que l'IBAN, les informations salariales et autres données confidentielles sont sécurisées de manière supplémentaire au sein de la base de données.

3. Gestion des accès et autorisation

- Les employés de Payflip ont accès aux Données à caractère personnel via un contrôle d'accès basé sur les rôles au sein de la plateforme, les droits étant attribués en fonction de la nécessité opérationnelle (least privilege).
- Les Employés du Responsable du traitement n'ont accès qu'à leurs propres données via les droits et invitations que le Client configure.
- L'accès aux données de production à des fins de développement ou de test est exclu. Les environnements de développement utilisent uniquement des données synthétisées ou anonymisées.

4. Authentification et identification

- La connexion à la plateforme Payflip s'effectue via SSL/TLS 256 bits et est authentifiée via Auth0.
- Les employés de Payflip se connectent à leur matériel (ordinateur portable, téléphone) avec un mot de passe fort ; une authentification supplémentaire optionnelle (Touch/Face ID) peut être configurée individuellement.
- Tous les comptes de la plateforme ont des identifiants uniques ; l'accès à la plateforme est régi par des processus internes et la gestion des rôles.

5. Développement logiciel et gestion du code

- Les données de production ne sont pas disponibles dans les environnements de développement ou de test.
- L'accès aux données de production est strictement limité aux processus opérationnels et au support nécessaire.
- Le code est testé dans des environnements de développement séparés sans accès aux données clients en direct.

6. Sécurité du cloud et de l'infrastructure

- L'utilisation de solutions basées sur le cloud (Microsoft Azure) réduit le risque de vol physique ou d'accès non autorisé.
- Des sauvegardes sont effectuées périodiquement.
- Les sauvegardes et répliques se trouvent exclusivement au sein de l'UE, garantissant ainsi la continuité et la conformité au RGPD.

7. Surveillance, journalisation et audit

- Payflip utilise la journalisation et la surveillance de l'infrastructure utilisée et des outils du fournisseur pour enregistrer les activités système, les accès et les incidents.
- Les journaux contiennent des informations sur les modifications de l'infrastructure et l'authentification, permettant de détecter les accès non autorisés.
- Bien que la journalisation au niveau de la plateforme de toutes les actions des employés soit limitée, les activités opérationnelles et d'infrastructure sont surveillées avec précision.

8. Politique de notification des incidents

- Payflip dispose d'une politique interne documentée pour la notification des Violations de Données à caractère personnel et des incidents de sécurité, conforme au RGPD.
- Les employés sont formés à cette politique et tenus de suivre ces procédures.
- Les incidents pertinents sont examinés en temps opportun et, le cas échéant, signalés au Responsable du traitement.

9. Conservation et suppression des données

- Après l'expiration de l'Accord, le Sous-traitant supprime toutes les Données à caractère personnel du RESPONSABLE DU TRAITEMENT dans un délai de trente (30) jours calendaires.
- Les sauvegardes sont conservées pendant un maximum d'un (1) an après l'expiration de l'Accord.
- Les Données à caractère personnel sont également restituées à la demande du RESPONSABLE DU TRAITEMENT via une exportation, conformément à la procédure établie dans les Conditions Générales.

Annexe 3 : Sous-traitants ultérieurs substantiels

Le SOUS-TRAITANT est autorisé à utiliser le(s) Sous-traitant(s) ultérieur(s) substantiel(s) suivant(s) :

Nom du Sous-traitant	Activité de traitement	Catégorie	Lieu de stockage des données	Siège social
Microsoft Azure	Infrastructure cloud : fournit l'environnement cloud dans lequel notre Outil fonctionne.	Infrastructure & hébergement	UE	États-Unis
MongoDB	Fournisseur de base de données : gère et stocke les données dans nos bases de données.	Infrastructure & hébergement	UE	États-Unis
Datadog	Monitoring & loganalyse: houdt de prestaties, logs en operationele Surveillance & analyse des logs : surveille les performances, les logs et le statut opérationnel de l'Outil.	Infrastructure & hébergement	UE	États-Unis
Netlify	Content Delivery Network (CDN) : assure la distribution de contenu et la livraison rapide des actifs web aux utilisateurs finaux.	Infrastructure & hébergement	UE	États-Unis
Amazon Web Services (AWS)	Génération de documents PDF Adobe : génère des documents PDF au sein de la plateforme.	Fonctionnalité	UE	États-Unis
Postmark	Fournisseur de services de messagerie : envoie des e-mails aux utilisateurs finaux, tels que des notifications ou communications.	Fonctionnalité	UE	États-Unis
Auth0 (Okta)	Gestion des identités : gère l'authentification des utilisateurs et le single sign-on (SSO) pour l'Outil.	Fonctionnalité	UE	États-Unis
Dropbox Sign	Fournisseur de signature électronique : fournit une API pour faire signer numériquement des contrats par les employés.	Fonctionnalité	UE	États-Unis
Make	Service iPaaS & automation : automatise les workflows dans le cadre du support client.	Support client	UE	États-Unis
Intercom	Système de messagerie de support front-office : facilite la communication entre les utilisateurs finaux et le service d'assistance.	Support client	UE	États-Unis
Anthropic, PBC	Services d'assistance à la clientèle et rapports	AI services	États-Unis	États-Unis