Annexe - Politique de protection des données personnelles dans le cadre du Service SaaS

Les dispositions de la présente annexe s'appliquent au(x) traitement(s) de données personnelles réalisé(s) dans le cadre du service SaaS réalisé en application du Contrat (ci-après « **Service** »).

Il est entendu que la présente annexe complète les dispositions du Contrat.

Définitions

Dans la présente annexe, les termes et expressions identifiés par une majuscule ont la signification indiquée ci-après, qu'ils soient employés au singulier ou au pluriel.

Documentation : Désigne les informations fournies par Expensya sous la forme d'une documentation utilisateur accompagnant le Service et/ou pouvant revêtir la forme d'une aide en ligne.

Données Personnelles : Désigne les données à caractère personnel que le Client traite dans le cadre de l'exécution du Contrat, au sens du 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 et la loi n°78-17 du 6 janvier 1978 (dit « RGPD »), cet ensemble règlementaire désigné ci-après «**Règlementation Applicable** ».

Livret Service : Désigne le document décrivant les dispositions particulières en matière de contenu, de limitations, de durée, de Support, de conditions d'exécution et de facturation applicables au Service. En tout état de cause les dispositions du Livret Service prévalent sur les dispositions des présentes, sauf dérogation expresse prévue au présent Contrat.

Portail : Désigne le portail de services web que Expensya met à disposition de sa clientèle. Le Portail est accessible à l'adresse https://www.expensya.com ou à toute autre adresse de site communiquée par Expensya.

1. Principes généraux

1.1. Il est rappelé qu'au sens de la Règlementation Applicable et dans le cadre de l'exécution du Contrat :

-le Client agit en qualité de responsable du traitement de Données Personnelles ou, le cas échéant, sous-traitant de ses clients ;

-Expensya agit en qualité de sous-traitant uniquement pour le compte et sur les instructions documentées et licites du Client.

1.2. Les Parties reconnaissent que la réalisation de l'objet du Contrat ainsi que l'utilisation du Service et de ses fonctionnalités conformément à sa Documentation constituent les instructions documentées du Client.

Toute instruction supplémentaire du Client devra être faite par écrit, préciser la finalité concernée et l'opération à effectuer, étant entendu que la mise en œuvre de toute instruction

supplémentaire sera conditionnée à l'acceptation par le Client du devis correspondant émis par Expensya.

Expensya s'engage à informer le Client par tout moyen dans un délai de cinq (5) jours à compter de la prise de connaissance par Expensya de l'instruction si, selon elle, cette instruction constitue une violation de la Règlementation Applicable.

1.3. Il est entendu que le Client est le seul à disposer de la maitrise et de la connaissance, notamment de l'origine, des Données Personnelles traitées lors de l'exécution du Contrat. Le Client garantit ainsi respecter l'ensemble des obligations qui lui incombent en qualité de responsable du traitement.

1.4. Expensya supprimera les Données Personnelles et leurs éventuelles copies en application de l'article « Restitution des Données Clients » du Contrat à moins que le droit applicable n'exige la conservation de ces Données Personnelles.

1.5. Le Client s'engage à indiquer à Expensya au moment de la signature du Contrat la personne à contacter pour toutes informations, communications, notifications ou demandes en application de la présente annexe. À défaut d'indication par le Client, le signataire du Contrat sera considéré comme la personne à contacter.

1.6. Expensya pourra être amenée à transférer les Données Personnelles pour les stricts besoins de l'exécution du Contrat sous réserve d'en informer préalablement le Client. Dans tous les cas, Expensya s'interdit de transférer les Données Personnelles, sans mettre en place les outils adéquats d'encadrement de ces transferts en application de l'article 46 du RGPD, en dehors :

- de l'Union Européenne, ou
- de l'Espace Economique Européen, ou
- des pays reconnus comme disposant d'un niveau de sécurité adéquat par la Commission Européenne (convention 108), comprenant la filiale Tunisienne de Expensya : « Expensya Tunisie »

En tout état de cause, les Données Personnelles demeurent localisées dans un ou plusieurs sites situées en Union Européenne, sauf dispositions contraires stipulées dans un Livret Service.

2. Sécurité des Données Personnelles

2.1. En application de l'article 32.1 du RGPD, le Client et Expensya reconnaissent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques. Les moyens mis en œuvre par Expensya sont listés dans un document dédié dont la dernière version à jour est mise à disposition du Client sur demande.

2.2. Il est entendu que Expensya est responsable de la sécurité du Service uniquement pour les aspects relevant de son contrôle. Ainsi, le Client demeure responsable de la sécurité et de la confidentialité de ses systèmes et de sa politique d'accès au Service. Il lui appartient de s'assurer que les usages et les choix de configuration du Service à sa disposition répondent aux exigences de la Règlementation Applicable. Il est entendu que Expensya n'a aucune obligation de protéger des données personnelles qui sont stockées ou transférées hors du Service par le Client ou par Expensya sur instruction du Client.

2.3. Expensya veille à ce que son personnel autorisé à traiter des Données Personnelles s'engage à en respecter la confidentialité.

3. Coopération avec le Client

3.1. Expensya s'engage à communiquer au Client dans les meilleurs délais après réception, toute demande, requête ou plainte qui lui serait adressée par toute personne physique concernée par le traitement de ses Données Personnelles réalisé dans le cadre du Contrat.

En qualité de responsable du traitement, le Client reste responsable de la réponse à apporter aux personnes physiques concernées et Expensya s'engage à ne pas répondre à de telles demandes. Cependant, compte tenu de la nature du traitement de Données Personnelles, Expensya s'engage, par des mesures techniques et organisationnelles appropriées et dans toute la mesure du possible, à aider le Client à s'acquitter de son obligation de donner suite à de telles sollicitations.

3.2. Sur demande écrite du Client, Expensya fournit au Client, aux frais de ce dernier, toute information utile en sa possession afin de l'aider à satisfaire aux exigences de la Règlementation Applicable qui incombent au Client en qualité de responsable du traitement concernant les analyses d'impact relatives à la protection des Données Personnelles menées par et sous la seule responsabilité du Client ainsi que les consultations préalables auprès de la CNIL qui pourraient en découler.

4. Notification des violations de Données Personnelles

4.1. Expensya notifie au Client dans les meilleurs délais après en avoir pris connaissance toute violation de la sécurité des Données Personnelles entrainant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données Personnelles.

4.2. Expensya fournit au Client dans les meilleurs délais à compter de la notification de la violation de la sécurité des Données Personnelles et dans la mesure du possible les informations suivantes :

- les catégories et le nombre approximatif de personnes concernées par la violation ;
- les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que Expensya propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

5. Sous-traitance

5.1. Le Client autorise Expensya à faire appel à des sous-traitants pour mener les activités de traitement de Données Personnelles pour le compte du Client strictement nécessaires à l'exécution du Contrat.

5.2. Expensya s'engage à faire appel à des sous-traitants présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à répondre aux exigences de la Règlementation Applicable.

5.3. Expensya s'engage à imposer contractuellement à ses sous-traitants un niveau d'obligation au moins aussi équivalent en matière de protection des Données Personnelles à celui fixé dans le présent Contrat et par la Règlementation Applicable. Expensya demeure responsable devant le Client de l'exécution par ledit sous-traitant de ses obligations.

5.4. Expensya s'engage à faire appel uniquement à un sous-traitant :

- établi dans un pays de l'Union Européenne ou de l'Espace Economique Européen, ou
- établi dans un pays disposant d'un niveau de protection suffisant par décision de la Commission Européenne au regard de la Règlementation Applicable, ou
- certifié Privacy Shield si celui-ci est établi aux Etats-Unis, ou
- disposant des garanties appropriées en application de l'article 46 du RGPD.

5.5. La liste des sous-traitants de Expensya est fournie sur demande écrite du Client. Expensya s'engage à informer le Client de tout ajout ou remplacement de sous-traitants dans les plus brefs délais. Le cas échéant, cette information constitue l'information préalable visée à l'article 1.6.

Le Client pourra formuler ses objections par écrit dans un délai de trente (30) jours ouvrés à compter de la réception de l'information. Le Client reconnaît et accepte que l'absence d'objection dans ce délai équivaut à une acceptation de sa part du sous-traitant.

En cas d'objection, Expensya dispose de la possibilité de répondre au Client pour apporter des éléments de nature à lever ces objections. Si le Client maintient ses objections, les Parties s'engagent à se rencontrer et à échanger de bonne foi concernant la poursuite de leur relation.

6. Conformité et audit

Expensya met à la disposition du Client, par courriel et à la demande de celui-ci, tout document nécessaire permettant de démontrer le respect des obligations de Expensya en qualité de sous-traitant au titre du Contrat. Tout autre mode de transmission de ces documents s'effectuera aux frais du Client.
Le Client pourra réclamer auprès de Expensya des explications complémentaires si les documents fournis ne lui permettent pas de vérifier le respect des obligations de Expensya en qualité de sous-traitant au titre du Contrat. Le Client formule alors une demande écrite auprès de Expensya, par lettre recommandée avec accusé de réception, dans laquelle il justifie et documente sa demande d'explication complémentaire. Expensya s'engage à apporter une réponse au Client dans les meilleurs délais.

Si malgré la réponse de Expensya, le Client remet en cause la véracité ou la complétude des informations transmises ou en cas de risques imminents à la sécurité des Données Personnelles, le Client pourra procéder à un audit sur site sous réserve du respect des conditions suivantes :

(i) le Client formule une demande écrite d'audit sur site auprès de Expensya, par lettre recommandée avec accusé de réception, en justifiant et en documentant sa demande ;

(ii) Expensya s'engage à apporter une réponse au Client en précisant le périmètre et les conditions de réalisation de l'audit sur site. La sécurité du système d'information de Expensya et des data center reposant sur leur accès restreint, le périmètre d'un audit sur

site sera limité aux processus de Expensya permettant d'opérer le Service en qualité de sous-traitant du ou des traitements de Données Personnelles confié(s) par le Client à Expensya. La durée de l'audit ne devra pas dépasser deux (2) jours ouvrés qui seront facturés par Expensya au Client selon le tarif des prestations en vigueur au moment du déroulement de l'audit ;

(iii) Cette mission d'audit peut être réalisée par les auditeurs internes du Client ou peut être confiée à tout prestataire au choix du Client, non concurrent de Expensya ;

(iv) Les auditeurs devront prendre un engagement formel de non divulgation des informations recueillies chez Expensya quel qu'en soit le mode d'acquisition. La signature de l'accord de confidentialité par les auditeurs devra être préalable à l'audit et communiquée à Expensya.

Dans le cadre de l'audit, Expensya donnera accès à ses locaux, et d'une manière générale aux documents et aux personnes nécessaires afin que les auditeurs puissent conduire l'audit dans des conditions satisfaisantes. Il est entendu que cet audit ne doit pas avoir pour conséquence de perturber l'exploitation du Service.

Le rapport d'audit sera mis à la disposition de Expensya par les auditeurs avant d'être finalisé, de telle sorte que Expensya puisse formuler toutes ses observations, le rapport final devant tenir compte et répondre à ces observations. Le rapport d'audit sera ensuite adressé à Expensya et fera l'objet d'un examen dans le cadre d'une réunion entre les Parties.

Au cas où le rapport d'audit final révèlerait des manquements aux engagements pris au titre de l'exécution du Service, Expensya devra proposer un plan d'actions correctives dans un délai de vingt (20) jours ouvrés maximum à compter de la réunion entre les Parties.

Il est entendu qu'au sens de la présente clause, jour ouvré désigne un jour compris entre le lundi et le vendredi et qui n'est pas un jour férié en France métropolitaine.

Sauf changement de circonstance et événement légitimant la mise en œuvre d'un audit dans un délai plus court, les audits ne pourront être réalisés par le Client sur site de Expensya, qu'une fois pendant la période initiale du Contrat, puis une fois par période de renouvellement.

7. Description du traitement

La nature des opérations réalisées sur les Données Personnelles, la ou les finalité(s) du traitement, les Données Personnelles traitées, les catégories de personnes concernées et la durée du traitement sont décrits dans un document dédié dans le Portail (tel que ce terme est défini dans le Contrat).

POUR EXPENSYA	POUR LE CLIENT