Annexe – Dispositions communes au traitement des Données personnelles

1. Définitions

Aux fins de la présente annexe, toutes les définitions énoncées dans le Règlement (UE) 2016/679 (RGPD) s'appliqueront.

« **Lois sur la protection des données** » désigne toute loi ou tout règlement relatif à la protection des données et la cybersécurité qui régit le traitement de Données à caractère personnel en vertu du Contrat, y compris le Règlement (UE) 2016/679 (RGPD) et la législation nationale spécifique en matière de protection des données applicable au Client et à Expensya.

2. Objet

Le présent document fait partie des annexes aux Conditions Générales et constitue les « Dispositions communes au traitement des Données personnelles » entre le Prestataire et le Client.

3. Interprétation

Une référence à une loi ou une disposition légale inclut une référence à toute législation subordonnée et constitue également une référence à cette loi, disposition légale ou législation subordonnée dans le cadre de toute modification, unification, nouvelle promulgation, renumérotation ou remplacement (avec ou sans modification) de celle-ci après la date de l'annexe et toute loi, disposition légale ou législation subordonnée qu'elle vise à unifier, promulguer à nouveau ou remplacer (avec ou sans modification).

Les références au singulier incluent le pluriel, et vice versa.

Les termes suivant les termes/expressions « inclut », « incluent », « y compris », « notamment », « en particulier » ou termes et expressions similaires seront interprétés sans restriction et, en conséquence, ne limiteront pas la signification des termes qui les précèdent.

4. Engagement du Prestataire en qualité de sous-traitant des Données

Sauf accord contraire entre les Parties consigné par écrit, le Prestataire traitera les Données à caractère personnel à la seule fin d'exécuter ses obligations en vertu des présentes Conditions Générales ou pour toute autre finalité expressément autorisée dans le Contrat et conformément aux Lois sur la protection des Données applicables, sous la supervision du Client en sa qualité de Responsable du traitement.

Le Prestataire ne traitera pas les Données à caractère personnel d'une manière incompatible avec les Lois sur la protection des données applicables au Prestataire et/ou au Client.

En particulier, le Prestataire s'engage à :

- Traiter les Données à caractère personnel uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du Contrat ;
- Traiter les Données à caractère personnel conformément aux instructions documentées du Client ;

- Garantir la confidentialité des Données à caractère personnel traitées dans le cadre du Contrat ;
- Veiller à ce que les personnes autorisées à traiter les Données à caractère personnel en vertu du Contrat :
    - S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
    - Reçoivent la formation nécessaire en matière de protection des Données à caractère personnel.
- Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut ;
- Informer le Client avant tout traitement si le Prestataire est tenu légalement de traiter les Données à caractère personnel autrement que conformément aux instructions du Client, sauf si le droit concerné interdit une telle information pour des motifs d'intérêt public, auquel cas le Prestataire en informera le Client dès que la loi l'autorisera ;
- Aider le Client à s'acquitter de ses obligations en vertu des Lois sur la protection des données, notamment de son obligation de donner suite aux demandes d'exercice des droits des Personnes concernées. Cette aide devra être apportée de façon à permettre au Client de respecter pleinement ses obligations, en temps opportun ;
- Coopérer avec le Client dans l'élaboration et la mise à jour du registre des activités de traitement du Client, mais uniquement pour les activités de traitement réalisées par le Prestataire pour le compte du Client dans le cadre des présentes Conditions Générales.

Conformément aux engagements énoncés précédemment, si le Prestataire considère qu'une instruction du Client constitue une violation des Lois sur la protection des données applicables, elle en informe immédiatement le Client.

En outre, si le Prestataire est tenu de procéder à un transfert de Données vers un pays tiers ou à une organisation internationale, en vertu des Lois sur la protection des données, elle doit informer le Client de cette obligation légale avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

Le Prestataire garantit en outre n'avoir aucune raison de croire que la législation le concernant ou concernant ses activités l'empêche de se conformer aux instructions données par le Client ou de remplir les obligations qui lui incombent conformément à la présente. Si un changement dans la législation est susceptible d'avoir une incidence négative significative sur les garanties et les obligations prévues dans la présente annexe ou si le Prestataire considère que les instructions du Client constituent une violation des Lois sur la protection des données ou des décisions émanant d'une autorité de contrôle, le Prestataire en informera le Client dès qu'elle en aura connaissance.

Le Prestataire conservera un registre du personnel et des prestataires autorisés à traiter les Données à caractère personnel et s'assurera que ce personnel et ses sous-traitants :

- Sont liés par des obligations de confidentialité identiques à celles liant le Client et el Prestataire et énoncées dans les présentes Conditions Générales ;
- Ont reçu une formation appropriée et font l'objet d'un contrôle approprié en ce qui concerne le traitement des Données à caractère personnel ;
- Ont un accès aux Données à caractère personnel strictement limité à ce qui est nécessaire pour l'exécution des Services et/ou des obligations d'Expensya en vertu des présentes Conditions Générales.

5. Mesures de sécurité

Le Prestataire a mis en œuvre et maintiendra les mesures techniques, physiques et organisationnelles appropriées (y compris en imposant une clause de confidentialité à ses employés, agents et sous-traitants) afin de protéger les Données à caractère personnel de toute destruction accidentelle ou illicite, perte accidentelle, altération ou divulgation ou accès non autorisé.

Le Prestataire informera de façon diligente le Client dès lors qu'il a connaissance d'un incident de sécurité, accès non autorisé, appropriation frauduleuse, perte, dommage ou autre compromission réel(le) ou présumé(e) lié(e) à la sécurité, la confidentialité ou l'intégrité des Données à caractère personnel traitées par ses employés, en sa qualité de Sous-traitant des données.

Dès lors qu'il constate une faille de sécurité, le Prestataire prendra toute mesure nécessaire pour prévenir une éventuelle nouvelle violation et apportera rapidement au Client toute l'aide requise pour remplir les obligations d'information qui lui incombent en qualité de Responsable du traitement.

En outre, le Prestataire a désigné un Délégué à la protection des données (Data Protection Officer ou DPO) et veille à ce que ce DPO puisse exercer ses fonctions dans le respect des Lois sur la protection des données.

Coordonnées du DPO du Prestataire :
Virtual DPO SAS
42 rue Manin 75019 Paris
RCS 830 490 603 Paris
E-mail : contact@virtual-dpo.fr

6. Coopération

6.1. Dispositions générales

À la demande écrite du Client, le Prestataire lui communique sans délai toute information utile en sa possession afin de lui permettre de répondre aux exigences des Lois sur la protection des données.

L'audit de conformité du Prestataire réalisé par son DPO détaille la description des mesures techniques, physiques et organisationnelles mises en œuvre par le Prestataire pour protéger les Données à caractère personnel de toute destruction accidentelle ou illicite ou perte accidentelle, altération, divulgation ou accès non autorisé et inclue le registre des activités de traitement des Données pour le Client par le Prestataire.

Sur demande écrite du Client, le Prestataire fournira au plus tard sous dix (10) jours ouvrés une copie électronique de l'audit de conformité.

En ce qui concerne les caractéristiques et spécificités de sa Solution, le Prestataire a choisi de ne pas effectuer d'analyse d'impact relative à la protection des données (Privacy Impact Assessment ou PIA). Si le Client exige l'exécution d'une analyse d'impact sur les opérations de traitement réalisées par le Prestataire en qualité de Sous-traitant des données, le Prestataire devra néanmoins mettre à disposition le matériel et le support technique appropriés. Les Parties conviennent que le coût de l'analyse d'impact sera à la charge exclusive du Client, en sa qualité de Responsable du traitement. Si nécessaire, le Prestataire pourra facturer au Client le temps passé et le personnel et le matériel affectés à la réalisation de cette analyse, ce que le Client comprend et accepte.

6.2. Demandes des personnes concernées

Le Prestataire répondra aux demandes des Personnes concernées portant sur leurs Données à caractère personnel, conformément aux instructions du Client :

Si le Client a demandé à ce que toutes les demandes soient transférées à ses propres services, le Prestataire s'abstiendra de répondre directement aux Personnes concernées et redirigera ces demandes vers l'interlocuteur dédié, à l'adresse indiquée par le Client dans le Contrat ;

Si le Client a demandé à ce que le Prestataire réponde à toutes les demandes pour son compte, le Prestataire s'efforcera d'apporter des réponses précises, dans la mesure de ses connaissances et compétences. Dans le cas où il serait impossible de répondre aux questions en raison d'un manque d'informations, le Prestataire transférera les demandes à l'interlocuteur dédié, à l'adresse indiquée par le Client dans le Contrat.

Le Prestataire informera le Client sans délai des demandes des Personnes concernées d'exercer leurs droits en vertu des Lois sur la protection des données.

6.3. Violation des Données

En cas de violation des Données à caractère personnel, le Prestataire informera le Client dans les plus brefs délais, et trente-six (36) heures au plus tard après avoir eu connaissance de cette violation entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Dès que possible après la notification de la violation des Données à caractère personnel et dans la mesure du possible, le Prestataire communiquera au Client 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 ;

Une description des conséquences probables de la violation de Données à caractère personnel ;

Une description des mesures prises ou que le Prestataire propose de prendre pour remédier à la violation des Données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, au moment de la notification initiale, le Prestataire ne dispose pas de toutes les informations prévues au paragraphe qui précède, il inclura dans la notification initiale les informations en sa possession au moment de la communication, puis transmettra les informations manquantes dès que possible.

7. Accès des tiers aux Données – sous-traitants ultérieurs

Le Prestataire veille à ce que ses employés, représentants et sous-traitants respectent et préservent l'intégrité, la confidentialité et la sécurité des Données à caractère personnel.

En cas de sous-traitance, le Prestataire s'engage à imposer contractuellement à ses sous-traitants un niveau d'obligation au moins équivalent en termes de protection des Données que ceux prévus dans la présente annexe et dans les Lois sur la protection des données. Le

Prestataire demeure seul responsable vis-à-vis du Client de l'exécution par ses sous-traitants de leurs obligations.

Le Prestataire fournit au Client dans l'annexe **Registre de traitement des Données** une liste de ses sous-traitants actuels susceptibles d'effectuer, directement ou indirectement, des activités de traitement de données sur tout ou partie des Données du Client et celui-ci a autorisé le Prestataire à recourir aux services de ces sous-traitants.

Le Prestataire s'engage à recourir aux services de sous-traitant uniquement s'ils sont absolument nécessaires à l'exécution du Contrat.

Le Prestataire s'engage à recourir uniquement à des sous-traitants :

- Etablis dans un pays membre de l'Union européenne ou de l'Espace économique européen ; ou,
- Etablis dans un pays considéré par la Commission européenne comme offrant un niveau de protection adéquat en vertu des Lois sur la protection des données ; ou,
- Certifiés « Privacy Shield » (bouclier de protection des données UE-États-Unis) s'ils sont basés aux États-Unis, ou certifiés dans le cadre d'un mécanisme similaire, reconnu par la Commission européenne comme offrant un niveau de sécurité adéquat ; ou,
- Offrant les garanties appropriées en vertu de l'Article 46 du RGPD.

8. Transferts internationaux de Données à caractère personnel

Si le Prestataire transfère, directement ou indirectement, des Données à caractère personnel à l'extérieur de l'Union européenne ou si un sous-traitant envisagé par le Prestataire est susceptible de transférer les Données à caractère personnel hors de l'Union européenne ou dans un pays qui ne garantit pas un niveau de protection adéquat au sens des Lois sur la protection des données, l'accès à ces données ne sera possible qu'après avoir obtenu le consentement du Client et mis en œuvre les garanties appropriées prévues à l'Article 46 du RGPD.

La filiale du Prestataire, SARL Expensya Tunisie ((Pepinotech Tunisia), détenue à 99,92 % par SA Expensya, est située en Tunisie. La filiale, chargée du développement et du support informatique, peut accéder aux Données à caractère personnel dans le cadre des services spécifiques qu'elle fournit en lien avec la Solution. Expensya SA et Expensya Tunisia ont signé des clauses contractuelles types qui garantissent que les Données à caractère personnel peuvent être transférées conformément aux Lois sur la protection des données.

Le Client reconnait en avoir été informé et accepte que la filiale d'Expensya soit située en Tunisie et puisse avoir accès aux Données à caractère personnel.

Sur demande écrite du Client, le Prestataire fournira au plus tard sous dix (10) jours ouvrés une copie électronique des clauses contractuelles signées avec le sous-traitant SARL Expensya Tunisie (Pepinotech Tunisia).

9. Audit

Le Prestataire communiquera par voie électronique au Client, sur demande, tout document nécessaire pour démontrer le respect de ses obligations de sous-traitant en vertu des présentes Conditions Générales. Les frais de transmission de ces documents par tout autre moyen seront à la charge du Client.

Le Client pourra demander des explications supplémentaires au Prestataire si les documents communiqués ne lui permettent pas de vérifier le respect des obligations de sous-traitant en vertu des présentes Conditions Générales ou de la présente annexe.

Le Client adressera alors une demande au Prestataire, par courrier recommandé avec accusé de réception, dans laquelle il justifie et documente sa demande d'explications supplémentaires. Le Prestataire s'engage à répondre au Client dans les meilleurs délais.

Si, malgré la réponse du Prestataire, le Client conteste l'exhaustivité des informations communiquées ou s'il existe un danger imminent pour la sécurité des Données à caractère personnel, le Client peut réaliser un audit sur site à sa charge et dont les modalités sont à convenir entre le Prestataire et le Client.

Annexe – Registre des activités de traitement de Données

1. Objet

Le présent document fait partie des annexes aux Conditions Générales et constitue le « Registre des activités de traitement de Données».

2. Description du traitement des Données

Objet du traitement

☒ L'objet du traitement de Données par le Sous-traitant est défini notamment à l'Annexe **Livret de Service**

☐ Autre :

……

Qualification du risque présenté par le Traitement

Risques	Impacts sur les personnes	Principales sources de risques	Principales menaces	Mesures existantes ou prévues	Gravité	Vraisemblance
Accès illégitime à des données	Visibilité sur les notes de frais	Usurpation d'accès / mot de passe	L'utilisateur / divulgation de mot de passe	SSO	Modérée	Faible
Modification non désirée de données	Fraude sur les notes de frais	Usurpation d'accès / mot de passe	L'utilisateur / divulgation de mot de passe	SSO / Audit des changements	Modérée	Faible
Disparition de données	Perte des données sur les notes de frais, impact comptable	Destruction des données Expensya	Menaces externes au fournisseur	Redondance, archivage à valeur probante	Forte	Très Faible

Durée du traitement :

☒ La durée du traitement correspond à la durée du Contrat,

☐ Autre :

……

Nature du traitement opéré par le Sous-traitant dans le cadre du Contrat inclut :

☒ Collecte ou enregistrement des Données

☒ Organisation ou structuration des Données

☒ Hébergement ou conservation des Données

☒ Adaptation ou modification des Données

☒ Extraction ou consultation des Données

☐ Utilisation des Données

☒ Communication des Données par transmission, diffusion or toute autre forme de mise à disposition

☐ Rapprochement ou interconnexion des Données

☒ Limitation (Blocage) des Données Limitation

☒ Effacement ou destruction des Données

☐ Autre Traitement

:……...……

Finalité du traitement

☒ La finalité du traitement de Données est définie au Contrat notamment à l'Annexe Livret de Service.

☐ Autre :

……

Catégories de Données

☒ Nom, titre, fonctions	☒Numéro(s) d'identification
☐Photos ou enregistrements tel que vidéo or enregistrement téléphonique	☐Informations en lien avec le contrat (relations contractuelles, intérêts dans des produits, services ou contrats)
☐Données de contact personnelles (ex.: téléphone, e-mail)	☐Historique Bénéficiaire
☒Données de contact professionnelles (ex: société, adresse, téléphone, e-mail)	☐Données bancaires (RIB, IBAN, numéro de carte bancaire, transactions)
☐Données relatives à la vie personnelle (habitudes de vie, situation familiale, etc.)	☒Données de facturation ou de paiement
☒Données relatives à la vie professionnelle (CV, formation professionnelle, distinctions…)	☐Données d'évaluation ou de notation
☐Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)	☐Données de connexion (adresse IP, logs, etc.)

☒Données de localisation (déplacements, données GPS, GSM etc.)

☐ Autres: ……

Catégories de Données Spéciales

☐ Données révélant l'origine raciale ou ethnique

☐ Données révélant les opinions politiques

☐ Données révélant les convictions religieuses ou philosophiques

☐ Données révélant l'appartenance syndicale

☐ Données génétiques

☐ Données biométriques aux fins d'identifier une personne physique de manière unique

☐ Données concernant la santé

☐ Données concernant la vie sexuelle ou l'orientation sexuelle

☐ Données relatives à des condamnations pénales ou infractions

☐ Numéro d'identification national unique (NIR pour la France)

Catégories de personnes concernées :

☒ Collaborateurs et anciens collaborateurs (salariés, stagiaires)

☐Visiteurs

☐Prospects

☐Bénéficiaires

☐Autres : …….....

☐ Souscripteurs

☒ Fournisseurs, consultants

☐ Représentants commerciaux

☐Contacts

3. Liste des sous-traitants autorisés

#	Dénomination	Adresse	Pays	Traitement opéré
1.	Microsoft Azure	Amsterdam	Pays-Bas	Stockage et hébergement de la solution Expensya
2.	Expensya Tunisie	Les Berges du Lac 2, Tunis	Tunisie	Support client
3.	CDC Arkhineo	122-120 Rue Réaumur – 75002 PARIS	France	Archivage à valeur probante

4. Cartographie des flux de données hors de l'Espace Economique Européen ou vers le Royaume-Uni

Des flux de données sont engagés en dehors de l'Espace Economique Européen uniquement lorsque le Client effectue une requête au service de support du Prestataire situé en Tunisie. Le membre de l'équipe de support du Prestataire ayant pris en charge la requête accède alors à la donnée

spécifiquement mentionnée sur les serveurs Microsoft Azure hébergés à Amsterdam. Lors de cette prise en charge aucun transfert effectif de données n'est opéré ni aucune sauvegarde.

5. Mesures visant à assurer la conformité du Traitement à la Réglementation relative à la protection des Données

5.1. Sécurité

Politique de sécurité des systèmes d'information du Sous—traitant : disponible sur demande

Chiffrement :

☒ Procédure de gestion des clés et certificats

☒Chiffrement des données

☒Chiffrement des transmissions de données

☒Fonction de hachage: SHA-256, SHA-512 ou SHA-3

☒Stockage des mots de passe: HMAC utilisation SHA-256, bcrypt, scrypt ou PBKDF2

☐Autres :
……
……

☐ Chiffrement symétrique: AES ou AES-CBC avec clés de 128 bits

☐ Signatures: RSA-SSA-PSS comme spécifié dans PKCS#1 v2.1
avec modules et exposants secrets d'au moins 2048 bits ou
3072 bits avec des exposants publics, pour le chiffrement,
supérieurs à 65536

Protection du réseau informatique du Sous--traitant :

☐Limitation des accès Internet

☒Gestion des réseaux Wi-Fi

☐Imposition d'un VPN pour l'accès à distance

☒Les interfaces d'administration ne sont pas accessible directement depuis Internet.

☒Limitation des flux réseau

☐Autres :
……..

☒Application des recommandations de l'ANSSI en matière de sécurisation dessites web, TLS et le Wi-Fi

☐Identification automatique de matériels

☒Mise en place de systèmes de détection d'intrusion

☒Cloisonnement réseau

Traçabilité :

☒Mise en place d'un système de journalisation

☒Mise en place de protection spécifique des équipements de journalisation et des informations journalisées

☒Mise en place d'une procédure de surveillance de l'utilisation du Traitement

☒Examen périodique des journaux d'événement

☒Mise en place d'une procédure de notification des anomalies ou de tout incident de sécurité

☐ Autres : ……

Gestion des habilitations :

☒ Définition de profils d'habilitation

☒ Réalisation d'une revue annuelle des habilitations

☒ Suppression des permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique, ainsi qu'à la fin de leur contrat

☒ Mise en place d'une politique de contrôle d'accès

☐Autres :

……

Gestion des authentifications :

☒ Mise en place d'identifiant unique par utilisateur

☐ Utilisation des gestionnaires de mots de passe pour avoir des mots de passe différents pour chaque service

☒ Interdiction des comptes partagés

☒ Respect de la recommandation de la CNIL du 4 septembre 2017 « Authentification par mot de passe: les mesures de sécurité élémentaires

☒Stockage les mots de passe de façon sécurisée

☒ Authentification forte

☒ Se référer aux règles et recommandations concernant les mécanismes d'authentification publiées par l'ANSSI dès lors que des mécanismes d'authentification forte sont mis en œuvre, notamment ses annexes B36 et B17 s'agissant respectivement des mécanismes d'authentification et des mécanismes cryptographiques

☒ Limitation du nombre de tentatives d'accès

☒ Imposition d'un renouvellement du mot de passe

☒ Blocage du compte en cas de non renouvellement du mot de passe

☐Autres :

……

Mesures de sécurité :

☒ Utilisation d'anti-virus régulièrement mis-à-jour

☒ Mise-à-jour automatique de sécurité

☒ Rechercher la source et les traces d'intrusion en cas de compromission d'un poste

☒ Veille de sécurité

☒ Chiffrement des postes nomades et supports de stockage mobiles

☒ Mise en place de mécanismes de protection contre le vol et de limitation de ses impacts

☐ Imposition d'un VPN pour l'accès à distance

☒ Application des recommandations de l'ANSSI en matière de sécurisation des sites web, TLS et le Wi-Fi

☒ Mise en place de systèmes de détection d'intrusion

☒ Application des recommandations de l'ANSSI relatives à la sécurisation de l'administration des systèmes d'information et aux bonnes pratiques en matière de sécurisation de l'annuaire central Active Directory

☒ Mise en place d'un plan de reprise et de continuité d'activité informatique

☒ Test de la restauration des sauvegardes et de l'application du plan de continuité ou de reprise de l'activité

☒ Mise en œuvre d'une procédure de suppression sécurisée des données

☐ Utilisation de logiciels dédiés à la suppression de données certifiés par l'ANSSI

☐ Autres : ……..

5.2. Privacy by design/Privacy by default

☒ Paramétrage par défaut et a minima par les utilisateurs de la collecte des données

☒ Non-obligation de renseignement d'un champ facultatif

☒ Seules les données nécessaires à la finalité du Traitement sont collectées

☒ Purge automatique et sélective des données à la fin du Traitement

☒ Gestion des habilitations et droits d'accès informatiques « donnée par donnée» ou sur demande

☐ Autres : ……..

5.3. Gouvernance des données

☒ Application des 25 référentiels de la Délibération n°2017-219 du 13 juillet 2017 de la CNIL

☒ Désignation d'un délégué à la protection des données

☒ Mise en place d'une politique appropriée en matière de protection de données

☐ Autres : ……..

5.4. Formation

☒ Formation régulière aux principes de la RGPD des personnes participantes au Traitement

☐ Autres : ……..