ACCORD DE PROTECTION DES DONNÉES (Data Protection Agreement)

Section 1

Clause 1 – Objet

Le présent Accord de Protection des Données définit les conditions dans lesquelles le Sous-traitant s'engage à traiter, pour le compte du Responsable, les données à caractère personnel nécessaires au fonctionnement des modules Tevasoft, notamment EVA Controls, Multi TVA, Smart Extract et Connect :

- la capture, l'analyse et la vérification des justificatifs de dépenses ;
- l'exécution de contrôles automatisés de conformité, de fraude ou d'application de la politique de dépenses ;
- l'extraction de données via OCR ou grand modèle de langage lorsque nécessaire ;
- l'identification et la structuration des informations de TVA, y compris en présence de plusieurs taux de TVA ;
- la recherche, l'extraction, la consultation et l'export de données et justificatifs ;
- la transformation, le mapping et la transmission de données entre systèmes ;
- la validation d'identifiants d'entreprise tels que SIREN, SIRET, numéro de TVA ou tout autre identifiant applicable ;
- la génération de rapports, alertes, fichiers d'export ou flux d'intégration ;
- le traitement de tout autre champ nécessaire au fonctionnement des modules souscrits par le Client.

Clause 2 - Clause d'Invariabilité des Clauses

Les Parties s'engagent à ne pas modifier les clauses, à l'exception de l'ajout d'informations dans les annexes ou de la mise à jour des informations qui y sont contenues.

Les Parties ne sont toutefois pas empêchées d'inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d'y ajouter d'autres clauses ou garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ni ne portent atteinte aux droits et libertés fondamentaux des personnes concernées.

Clause 3 – Interprétations

Lorsque des termes définis respectivement dans le Règlement (UE) 2016/679 ou le Règlement (UE) 2018/1725 apparaissent dans les présentes Clauses, ils doivent être interprétés conformément au Règlement en question.

Les présentes Clauses doivent être lues et interprétées à la lumière des dispositions des Règlements (UE) 2016/679 et 2018/1725 respectivement.

Les présentes Clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations découlant du Règlement (UE) 2016/679 ou du Règlement (UE) 2018/1725, ni d'une manière qui porterait atteinte aux droits et libertés fondamentaux des personnes concernées.

Clause 4 – Hiérarchie

En cas d'incohérence entre les présentes Clauses et les dispositions d'accords connexes existants entre les Parties au moment de la signature des présentes Clauses ou conclus ultérieurement, les présentes Clauses prévaudront.

Clause 5 – Durée

Le présent Accord entre en vigueur à sa date de signature et demeure valable pendant toute la durée contractuelle de fourniture des modules Tevasoft souscrits par le Client, augmentée de la période nécessaire à l'exécution des obligations de purge ou de restitution des données prévues à l'Article 16.

Section 2 – Obligation des parties

Clause 6 – Description des traitements

Les détails des opérations de traitement, et en particulier les catégories de données à caractère personnel et les finalités pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable du traitement, figurent à l'annexe 1.

Clause 7 – Obligations du sous-traitant

- Ne traiter les données personnelles que sur instruction documentée du Responsable ;
- Garantir la confidentialité des données et former le personnel habilité ;
- Mettre en œuvre les mesures techniques et organisationnelles appropriées détaillées en Annexe 2 ;
- Aider le Responsable à satisfaire ses obligations en matière de droits des personnes (articles 12 à 22 RGPD) et d'analyse d'impact (article 35 RGPD) ;
- Notifier toute violation de données au Responsable dans les 24 heures suivant sa découverte, selon les modalités de l'Article 8 ;
- Tenir un registre des catégories d'activités de traitement (article 30 §2 RGPD ;
- Permettre et contribuer aux audits, y compris les inspections, réalisés par le Responsable ou tout auditeur mandaté (Article 12) ;
- Informer le Responsable de tout changement envisagé concernant l'ajout ou le remplacement de Sous-traitants ultérieurs (Article 10).

Clause 8 – Obligations du Responsable

- S'assurer de la base légale du traitement et fournir une information appropriée aux personnes concernées :
- Transmettre au Sous-traitant des instructions licites et documentées ;
- Coopérer avec le Sous-traitant pour la réalisation d'analyses d'impact ou la réponse aux autorités de contrôle ;
- Superviser l'activité du Sous-traitant et des Sous-traitants ultérieurs.

Clause 9 – Mesures de sécurité techniques et organisationnelles

Le Sous-traitant s'engage à mettre en œuvre, au minimum, les mesures décrites en Annexe 2.

Clause 10 – Notification des violations de données

En cas de violation de données, le Sous-traitant :

- Informe le Responsable sans délai et, en tout état de cause, dans les 24 heures suivant la découverte ;
- Fournit toute information utile permettant au Responsable d'évaluer la portée, l'incidence et les actions correctives nécessaires ;
- Collabore avec le Responsable pour toute notification aux autorités et aux personnes concernées.

Clause 11 – Sous-traitance ultérieure

Le Sous-traitant ne peut engager un Sous-traitant qu'après autorisation écrite du Responsable. Les Sous-traitants actuels autorisés sont listés en Annexe 3. Le Sous-traitant impose à tout Sous-traitant ultérieur des obligations au moins équivalentes aux siennes.

Clause 12 – Transferts de données hors UE/EEE

Tout transfert vers un pays tiers est soumis :

- à une décision d'adéquation de la Commission européenne ;
- ou à des Clauses Contractuelles Types approuvées ;
- ou à un autre mécanisme conforme aux articles 46 à 49 RGPD.

Le Sous-traitant s'engage à fournir les documents justificatifs sur demande.

Clause 13 – Droit d'audit

Le Responsable peut, une (1) fois par an et moyennant un préavis raisonnable de trente (30) jours, réaliser ou faire réaliser un audit des traitements couverts par le présent Accord. Les frais d'audit sont à la charge du Responsable, sauf manquement grave avéré du Sous-traitant.

Clause 14 – Confidentialité

Les Parties reconnaissent que les données personnelles et l'information relative aux mesures de sécurité constituent des informations confidentielles.

Clause 15 – Assistance et coopération

En cas de violation de données à caractère personnel concernant les données traitées par le sous-traitant, ce dernier en informe le responsable du traitement dans les meilleurs délais après en avoir eu connaissance. Cette notification comprend au minimum :

- une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées et d'enregistrements de données à caractère personnel affectés) ;
- les coordonnées d'un point de contact auprès duquel des informations complémentaires peuvent être obtenues à propos de la violation ;
- ses conséquences probables ainsi que les mesures prises ou envisagées pour remédier à la violation, y compris les mesures visant à atténuer les conséquences négatives éventuelles.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en une seule fois, la notification initiale contient les informations disponibles à ce moment-là, et des informations complémentaires sont communiquées ultérieurement dès qu'elles deviennent disponibles.

Clause 16 – Durée et sort des données

À l'expiration ou la résiliation du contrat de service, le Sous-traitant doit, au choix du responsable de traitement ;

1. Supprimer ou restituer toutes les données à caractère personnel traitées pour le compte du responsable.
2. Restituer toutes les données à caractère personnel et détruire toutes les copies existantes, sauf si une disposition du droit de l'Union ou du droit national exige leur conservation pendant une période plus longue.

Le sous-traitant continue d'assurer le respect des présentes clauses jusqu'à la suppression ou la restitution complète des données.

La confirmation de suppression est remise par écrit au Responsable.

Clause 17 – Loi applicable et juridiction

Le présent Accord est régi par le droit français. Tout litige sera soumis à la compétence exclusive des tribunaux du siège du Responsable, sauf disposition impérative contraire.

Section 3 – Dispositions finales

Clause 18 – Non-respect des clauses et résiliation

Sans préjudice des dispositions du Règlement (UE) 2016/679 et/ou du Règlement (UE) 2018/1725, en cas de manquement par le sous-traitant à ses obligations au titre des présentes clauses, le responsable du traitement peut ordonner au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que le sous-traitant se conforme aux présentes clauses ou que le contrat soit résilié. Le sous-traitant informe rapidement le responsable s'il n'est pas en mesure de se conformer aux présentes clauses, quelle qu'en soit la raison.

Le responsable du traitement est en droit de résilier le contrat, dans la mesure où celui-ci concerne le traitement de données à caractère personnel conformément aux présentes clauses, si :

1. le traitement des données personnelles par le sous-traitant a été suspendu par le responsable, et que le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;
2. le sous-traitant commet une violation grave ou répétée des présentes clauses ou de ses obligations en vertu du Règlement (UE) 2016/679 et/ou du Règlement (UE) 2018/1725 ;
3. le sous-traitant ne respecte pas une décision contraignante d'un tribunal compétent ou d'une ou plusieurs autorités de contrôle compétentes relative à ses obligations en vertu des présentes clauses ou du Règlement (UE) 2016/679 et/ou du Règlement (UE) 2018/1725.

Le sous-traitant est en droit de résilier le contrat, dans la mesure où celui-ci concerne le traitement de données à caractère personnel au titre des présentes clauses, dans le cas où, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences légales applicables, le responsable insiste pour que ses instructions soient exécutées.

Après la résiliation du contrat, les conditions de restitution ou suppression prévues à la Clause 16 s'appliquent.

Signature :

Nom du Client	
Nom du signataire	
Position	
Date	
Signature	

Annexe 1 - Description détaillée des traitements

Module	Finalité principale	Opérations réalisées
EVA Controls	Contrôle, validation et conformité des frais professionnels	Collecte des justificatifs, extraction OCR/LLM, contrôle de conformité, détection de fraudes, vérification SIREN/SIRET, contrôle d'adresse, contrôle des montants, détection de mots-clés, contrôle du format des justificatifs, application de la politique de dépenses, génération d'alertes et rapports
Multi TVA	Identification et structuration des informations de TVA liées aux dépenses professionnelles	Analyse des justificatifs, identification des taux de TVA, extraction des montants HT/TTC/TVA, structuration des données fiscales, mise à jour ou transmission des champs TVA vers le système source
Smart Extract	Recherche, extraction et export de données et justificatifs	Recherche de données, extraction de justificatifs, génération d'exports PDF/Excel/CSV/JSON/XML, planification d'exports, mise à disposition sécurisée des fichiers
Connect	Intégration, transformation et transmission de données entre systèmes	Réception de données, mapping, transformation, contrôle de cohérence, transmission vers SAP Concur, systèmes clients ou plateformes externes, suivi des statuts, gestion des erreurs d'intégration

Catégories des données à caractère personnel traitées :

Catégorie des données	Traitées dans le cadre du contrat ?	Détails
État civil, identité, données d'identification	Oui	Nom, prénom, identifiant, adresse e-mail, pays de résidence, identifiant utilisateur dans le système source, identifiant collaborateur, identifiant fournisseur ou tiers lorsque applicable.
Identification d'un véhicule personnel	Oui	Immatriculation du véhicule

ou professionnel		et puissance fiscale
Vie personnelle (mode de vie, situation familiale, à l'exclusion des données sensibles)	Non	
Vie professionnelle (CV, formation, diplômes, distinctions…)	Oui	Affectation dans l'entreprise (emploi, rattachement à une société, un département, un centre de coûts ou tout autre niveau organisationnel) Nom, prénom, position et société des externes invités dans le cadre professionnel (repas d'affaire, évènement, cadeaux)
Informations économiques et financières (revenus, situation fiscale, etc.)	Non	
Données de connexion (adresses IP, journaux d'événements, etc.)	Oui	Journaux de connexion
Données de localisation (déplacements, GPS, données GSM, etc.)	Non	
Coordonnées bancaires	Non	Non, sauf activation spécifique d'un flux Connect contenant de telles informations, auquel cas le traitement sera documenté contractuellement.
Autres types de données	Oui	Reçus de frais professionnels, justificatifs de dépenses, données de facturation, données de TVA, numéros de facture, identifiants fiscaux ou commerciaux, données issues des exports ou flux d'intégration.

Données sensibles (catégories particulières)

Catégorie des données	Traitées dans le cadre du contrat ?	Détails
Données biométriques	Non	

Opinions philosophiques	Non	
Opinions politiques	Non	
Croyances religieuses	Non	
Opinions syndicales	Non	
Vie sexuelle ou orientation sexuelle	Non	
Données de santé	Non	
Données génétiques	Non	
Numéro de sécurité sociale	Non	
Données relatives à des condamnations ou infractions	Non	

Durée de conservation : 10 ans à compter de la clôture de l'exercice fiscal concerné pour les données ayant une valeur comptable ou fiscale, sauf législation contraire ou instruction documentée du Client. Les logs techniques et journaux d'événements sont conservés selon la durée indiquée en Annexe 2.

Annexe 2 - Mesures techniques et organisationnelles

Chiffrement	● Données au repos : AES-256. ● Données en transit : TLS 1.3.
Contrôle d'accès	● Connexion SSO ● Contrôle d'accès basé sur les rôles (RBAC) avec principe du moindre privilège.
Journalisation et supervision	● Logs horodatés, conservés 1 mois, immuables.
Tests de sécurité	● Scan de vulnérabilités annuel. ● Test d'intrusion annuel par un tiers qualifié.
Continuité d'activité	● Sauvegardes quotidiennes, conservation 30 jours, stockage hors site.
Gouvernance Intelligence Artificielle	● Lorsque les modules Tevasoft utilisent des traitements OCR, LLM ou d'analyse automatisée, ceux-ci font l'objet d'une revue régulière, incluant l'évaluation de la performance, des risques d'erreur, des biais potentiels et des mesures de contrôle associées.

Annexe 3 – Sous-traitants autorisés

Société	Services fournis	Localisation des données	Mécanisme de transfert	Notes
CleverCloud	Hébergement applicatif, base de données, infrastructure cloud et sauvegardes des modules Tevasoft	France, Paris	Aucun (UE)	ISO 9001 ISO 27001 : 2022 SecNumCloud
Mistral AI	Service de grand modèle de langage utilisé pour certains traitements d'analyse documentaire ou d'extraction, selon les modules activés.	UE	Aucun (UE)	ISO 27001:2022 ISO 27701 SOC 2
Sightengine	Service de détection de reçus ou justificatifs potentiellement générés par intelligence artificielle, principalement dans le cadre des contrôles automatisés.	Données non stockées	Clauses Contractuelles Types	ISO 27001:2022 SOC 2 PCI DSS