Avenant de traitement des données (DPA)

S2M Consulting SAS — Éditeur du service Comptao SIREN 819 859 273 · SIRET 819 859 273 00016 · TVA FR47 819859273 10 rue des Rambervilliers, 75012 Paris

Dernière mise à jour : 16 avril 2026 — Version 1.1

ARTICLE 28 RGPD · VERSION 2.0 Comptao — Avenant de traitement des données personnelles Contrat de sous-traitance conforme à l'article 28 du Règlement (UE) 2016/679 (RGPD).

Entre Le cabinet abonné au service Comptao, dénommé ci-après « le Responsable de traitement ».

Et **S2M Consulting SAS** SIREN 819 859 273 · RCS Paris Siège : 10 rue des Rambervilliers, 75012 Paris Éditrice du service Comptao, dénommée ci-après « le Sous-traitant ».

Document contractuel — partie intégrante des CGV Comptao v2.1 Édition du 16 avril 2026

Sommaire

Préambule

Le Responsable de traitement a souscrit au service Comptao, édité par S2M Consulting SAS, dans le cadre d'un contrat d'abonnement SaaS régi par les Conditions générales de vente.

Dans le cadre de l'exécution de ce contrat, le Sous-traitant est amené à traiter des données à caractère personnel pour le compte du Responsable de traitement. Les parties établissent le présent avenant (ci-après le « DPA ») conformément à l'article 28 du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (ci-après le « RGPD »).

Le présent DPA fait partie intégrante du contrat d'abonnement. En cas de contradiction entre les stipulations du DPA et celles des CGV, les stipulations du DPA prévalent pour tout ce qui concerne le traitement des données personnelles.

Définitions

- **Données personnelles** : toute information se rapportant à une personne physique identifiée ou identifiable (art. 4.1 RGPD).
- **Traitement** : toute opération effectuée sur des Données personnelles (art. 4.2 RGPD).
- **Responsable de traitement** : le cabinet d'expertise comptable abonné à Comptao.
- **Sous-traitant** : S2M Consulting SAS.
- **Sous-traitant ultérieur** : toute entité à laquelle le Sous-traitant recourt pour l'exécution d'une partie du traitement.
- **Personne concernée** : personne physique dont les Données personnelles sont traitées.
- **Violation de données** : violation de la sécurité entraînant la destruction, la perte, l'altération ou la divulgation non autorisée de Données personnelles.
- **CNIL** : Commission nationale de l'informatique et des libertés.

Article 1 — Objet

Le présent DPA a pour objet d'encadrer les conditions dans lesquelles le Sous-traitant s'engage à effectuer les opérations de traitement de Données personnelles décrites à l'article 3, pour le compte et selon les instructions documentées du Responsable de traitement.

Article 2 — Durée

Le présent DPA prend effet à la date d'acceptation des CGV et demeure en vigueur pendant toute la durée du contrat d'abonnement, y compris les renouvellements.

Les obligations de confidentialité, de sécurité et de notification de violation demeurent applicables pendant cinq (5) ans après la fin du contrat.

Article 3 — Nature et finalités du traitement

3.1 Nature des opérations Le Sous-traitant réalise : collecte, enregistrement, organisation, structuration, conservation, adaptation, extraction, consultation, utilisation, communication par transmission, effacement ou destruction des Données personnelles.

3.2 Finalités

- Gestion des dossiers clients du cabinet ;
- Envoi de relances graduées (courriel, Telegram, WhatsApp) ;
- Production de briefings quotidiens ;
- Tri et classement des pièces comptables ;
- Support et assistance aux Utilisateurs ;
- Journalisation technique et d'audit.

3.3 Absence d'entraînement IA Le Sous-traitant s'engage formellement à ne jamais utiliser les Données personnelles pour entraîner, affiner ou évaluer un modèle d'intelligence artificielle, ni à aucune autre finalité secondaire. Cet engagement est opposable à l'ensemble des Sous-traitants ultérieurs listés à l'Annexe 2.

Article 4 — Données personnelles et personnes concernées

4.1 Catégories de Données personnelles

Catégorie	Exemples
Identification des Utilisateurs	Nom, prénom, email professionnel, fonction
Authentification	Email, mot de passe chiffré (bcrypt), jetons, logs de connexion
Contact des clients du cabinet	Nom / raison sociale, email, téléphone, SIREN
Données d'activité	Échanges de relances, pièces comptables, état des dossiers
Données techniques	Adresse IP, navigateur, horodatage, actions

4.2 Personnes concernées

- Utilisateurs du Responsable de traitement ;
- Clients du Responsable de traitement ;
- Prospects enregistrés dans Comptao.

4.3 Données sensibles Le Sous-traitant ne traite aucune donnée relevant de l'article 9 du RGPD. En cas de saisie accidentelle, effacement dès signalement.

Article 5 — Obligations du Sous-traitant

5.1 Traitement sur instruction documentée Le Sous-traitant traite les Données uniquement sur instruction documentée du Responsable de traitement, formalisée par les CGV, le DPA, les paramètres applicatifs et les demandes écrites à contact@comptao.eu.

5.2 Confidentialité Les personnes autorisées sont tenues à une obligation de confidentialité contractuelle. Le Sous-traitant respecte le secret professionnel de l'expert-comptable (art. 21 ordonnance n° 45-2138).

5.3 Sécurité Mesures techniques et organisationnelles détaillées en Annexe 1 (privacy by design & by default). Registre des activités de traitement (art. 30 RGPD) disponible sur demande.

5.4 Sous-traitants ultérieurs Le Sous-traitant est autorisé à recourir aux sous-traitants listés en Annexe 2. Préavis de 30 jours pour tout ajout. Droit d'opposition du Responsable pour motif légitime. Le Sous-traitant demeure pleinement responsable de ses sous-traitants ultérieurs.

5.5 Assistance Le Sous-traitant aide le Responsable à répondre aux demandes d'exercice des droits des personnes concernées et à respecter ses obligations des articles 32 à 36 RGPD.

5.6 Notification de violation En cas de violation, notification dans les 72 heures maximum, par courriel, avec les éléments prévus à l'article 33 RGPD.

5.7 AIPD Assistance raisonnable pour les analyses d'impact et consultations préalables de la CNIL.

5.8 Droit à l'audit Le Responsable peut procéder à un audit par an (sous préavis de 30 jours, à ses frais). Le Sous-traitant peut fournir un rapport d'audit tiers en alternative.

5.9 Registre et conformité Registre des activités de traitement à jour, disponible sur demande.

Article 6 — Obligations du Responsable de traitement

Le Responsable de traitement s'engage à : documenter ses instructions par écrit ; respecter ses obligations légales (information des personnes, licéité, minimisation) ; coopérer avec le Sous-traitant ; désigner un point de contact RGPD.

Article 7 — Sort des données à la fin du contrat

1. Export pendant 30 jours calendaires (CSV, JSON) ;
2. Effacement sécurisé et irréversible des systèmes de production ;
3. Suppression des sauvegardes sous 90 jours par rotation naturelle ;
4. Conservation des données légalement requises (factures) dans des systèmes à accès restreint.

Sur demande écrite, attestation d'effacement fournie.

Article 8 — Droit applicable et juridiction

Le présent DPA est régi par le droit français. Tout différend sera soumis aux tribunaux de Paris, après tentative de résolution amiable.

Signatures

Fait en deux exemplaires originaux (ou acceptation électronique opposable via la plateforme).

	RESPONSABLE DE TRAITEMENT	**SOUS-TRAITANT**
Raison sociale	*(à compléter)*	S2M Consulting SAS
SIREN	*(à compléter)*	819 859 273
Nom et fonction	*(à compléter)*	Tom Weisz, Président
Date	*(à compléter)*	*(à compléter)*
Signature		

L'acceptation des CGV dans l'application Comptao vaut acceptation simultanée du présent DPA. Copie horodatée conservée dans l'espace « Facturation / Documents contractuels ».

Annexe 1 — Mesures techniques et organisationnelles (TOMs)

A1.1 Chiffrement

- En transit : TLS 1.3 imposé, HSTS activé
- Au repos : AES-256 sur sauvegardes et pièces comptables
- Mots de passe : bcrypt avec sel et coût ≥12

A1.2 Contrôle d'accès Principe du moindre privilège, 2FA obligatoire (plans supérieurs et personnel interne), SSH par clé uniquement, segmentation réseau.

A1.3 Journalisation et audit Logs applicatifs (90 jours), logs d'audit (1 an + 5 ans archive), traçabilité des accès administrateurs.

A1.4 Sauvegardes Quotidiennes chiffrées multi-sites, tests de restauration mensuels, rétention 30 jours / 12 mois.

A1.5 Durcissement et mises à jour Correctifs critiques ≤72h, SCA automatisé, revue de code systématique.

A1.6 Disponibilité et continuité Supervision 24/7, PRA testé semestriellement, redondance.

A1.7 Mesures organisationnelles Engagement de confidentialité signé, formation RGPD annuelle, politique de sécurité revue annuellement, procédure d'incident formalisée.

A1.8 Gestion des accès fournisseurs Revue trimestrielle, retrait immédiat, cloisonnement dev/recette/production.

A1.9 Tests et audits de sécurité Pentests et audits de sécurité réguliers par des tiers indépendants.

Annexe 2 — Sous-traitants ultérieurs autorisés

Sous-traitant	Finalité	Localisation	Garanties
S2M Consulting SAS	Hébergement, BDD, sauvegardes	France (Paris)	Infra propriétaire, AES-256
Anthropic PBC	Modèle IA (relances, résumés)	États-Unis	CCT 2021, no training, DPF
Groq Inc. (optionnel)	Modèle IA rapide	États-Unis	CCT 2021, no training
Stripe Payments Europe	Encaissement, facturation	Irlande, États-Unis	CCT 2021, DPF, PCI-DSS
Sendinblue SAS (Brevo)	Envoi de courriels	France	ISO 27001
Meta Platforms Ireland	WhatsApp Business (opt.)	Irlande, États-Unis	CCT 2021, DPF
Telegram FZ-LLC (opt.)	Telegram Bot	Émirats arabes unis	CCT 2021
Hostinger International	DNS, courriels pro	Chypre, Lituanie	UE, conforme RGPD

Chaque fournisseur d'IA est contractuellement tenu de ne pas utiliser les Données pour l'entraînement ou l'évaluation de modèles.

Annexe 3 — Transferts hors UE

Les transferts sont encadrés par :

- Clauses contractuelles types (décision 2021/914, modules 2 et 3) ;
- Adhésion au Data Privacy Framework (lorsque applicable) ;
- Analyse d'impact du transfert (TIA) formalisée, avec mesures supplémentaires le cas échéant.

Documentation disponible sur demande à contact@comptao.eu.
