Accord de sous-traitance RGPD

Article 28 du RGPD — Client professionnel

Référence : PTC-ANNEXE-DPA-B2B

Version 1.0.0 — 2026-08-25

Phénix Tech

SASU au capital de 100 € · SIRET 102 975 372 00016
13300 Salon-de-Provence, France
contact@phenix-tech.fr · https://phenix-tech.fr

Préambule

Le présent **Accord de sous-traitance** (ci-après « l'Accord » ou « le DPA ») est conclu en application de l'**article 28 du Règlement (UE) 2016/679** (ci-après « **RGPD** ») entre :

Phénix Tech, SASU au capital de 100 €, immatriculée au Registre du Commerce et des Sociétés de Salon-de-Provence sous le numéro SIRET **102 975 372 00016**, dont le siège social est situé à **13300 Salon-de-Provence, France**, représentée par son Président **Bastien Bertorello**, joignable à `contact@phenix-tech.fr` — ci-après « **le Prestataire** », agissant en qualité de **sous-traitant** —

et

Le Client — *(à compléter au contrat)* : raison sociale, forme juridique, SIRET, siège social, représentant légal, email de l'interlocuteur — ci-après « **le Client** », agissant en qualité de **responsable de traitement**.

Ci-après désignés ensemble « **les Parties** ».

> ***Le Prestataire n'héberge pas.*** *Toutes les prestations couvertes par le présent Accord sont des prestations de* ***mise en place, de configuration, de développement et de maintenance*** *réalisées sur l'infrastructure du Client ou sur celle qu'il a souscrite en son nom propre. Le Prestataire* ***n'exploite aucun hébergement pour le compte du Client*** *et ne détient aucune base de données du Client. Son intervention consiste en des* ***accès ponctuels ou récurrents****, sur instruction, à des systèmes qui restent sous la maîtrise du Client.*
>
> *Cette qualité de sous-traitant est néanmoins retenue sans réserve : l'accès à des données personnelles au cours d'une mission d'installation, de migration, de maintenance ou de support relève de l'article 28 du RGPD, quand bien même le Prestataire ne conserve pas ces données.*

> ***Sens de la relation.*** *Le Client détermine les finalités et les moyens des traitements. Le Prestataire traite les données personnelles* ***pour le compte du Client*** *et* ***sur ses seules instructions****. Le présent Accord ne couvre* ***pas*** *les traitements pour lesquels le Prestataire agit en qualité de responsable de traitement pour son propre compte (gestion de la relation commerciale, facturation, prospection), régis par les* ***CGV B2B*** *article 12 et par la politique de confidentialité publiée à https://phenix-tech.fr/politique-de-confidentialite.html.*

Portée de ce document. La présente version est le **DPA-type** du Prestataire, publié à titre d'information. La version applicable à une prestation donnée est **individualisée** (identité du Client, traitements réellement confiés, durées) et signée électroniquement en annexe du contrat de prestation. En cas de divergence, la version signée prévaut.

Article 1 — Définitions

Les termes « données à caractère personnel », « traitement », « responsable de traitement », « sous-traitant », « personne concernée », « violation de données à caractère personnel » et « autorité de contrôle » s'entendent au sens de l'**article 4 du RGPD**.

« **Données** » désigne les données à caractère personnel auxquelles le Prestataire accède ou qu'il traite pour le compte du Client dans le cadre du Contrat.

« **Systèmes du Client** » désigne les serveurs, instances, hébergements et postes détenus par le Client ou souscrits par lui en son nom propre, sur lesquels le Prestataire intervient.

« **Copies de travail** » désigne les extractions, exports, sauvegardes préalables et fichiers temporaires que le Prestataire est amené à constituer sur son propre poste pour les besoins d'une migration, d'un diagnostic ou d'une recette.

« **Contrat** » désigne le contrat de prestation auquel le présent Accord est annexé, ainsi que les CGV B2B du Prestataire (https://phenix-tech.fr/cgv.html).

« **Sous-traitant ultérieur** » désigne tout tiers auquel le Prestataire confierait tout ou partie d'un traitement effectué pour le compte du Client.

Article 2 — Objet

Le présent Accord définit les conditions dans lesquelles le Prestataire s'engage à effectuer, pour le compte du Client, les opérations de traitement de Données décrites à l'**Annexe 1**.

Il constitue l'acte juridique exigé par l'**article 28.3 du RGPD** et lie les Parties pour toute la durée du Contrat.

Article 3 — Description des traitements

La nature, la finalité, la durée de chaque traitement, ainsi que les catégories de Données et de personnes concernées, sont décrites à l'**Annexe 1**, complétée au contrat selon les prestations effectivement souscrites.

Article 4 — Obligations du Prestataire

4.1 Instructions documentées

Le Prestataire traite les Données **uniquement sur instruction documentée du Client**, y compris en ce qui concerne les transferts vers un pays tiers, sauf obligation légale à laquelle il serait soumis. Dans ce dernier cas, il en informe le Client avant le traitement, sauf interdiction légale pour des motifs d'intérêt public.

Le Contrat, ses annexes et le présent Accord constituent les instructions initiales du Client. Toute instruction ultérieure est formulée **par écrit** (email à `contact@phenix-tech.fr` suffisant).

4.2 Devoir d'alerte

Conformément à l'**article 28.3 alinéa 2 du RGPD**, le Prestataire **informe immédiatement le Client** s'il estime qu'une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l'Union ou du droit national relative à la protection des données.

4.3 Confidentialité

Le Prestataire veille à ce que les personnes autorisées à traiter les Données s'engagent à en respecter la **confidentialité** ou soient soumises à une obligation légale appropriée de confidentialité. Cet engagement survit **trois (3) ans** à la fin du Contrat.

Compte tenu de la structure du Prestataire (société unipersonnelle), l'accès aux Données est limité à son **représentant légal**. Tout élargissement de cette liste est notifié au Client.

4.4 Minimisation de l'accès

Le Prestataire limite son accès aux Systèmes du Client à ce qui est **strictement nécessaire** à l'exécution de la mission. Il ne consulte, n'extrait ni ne copie aucune Donnée au-delà de ce que la prestation exige, et privilégie en toute circonstance le recours à des **données fictives ou anonymisées** pour les phases de conception et de recette.

4.5 Sécurité des traitements

Le Prestataire met en œuvre les mesures techniques et organisationnelles appropriées prévues à l'**article 32 du RGPD**, décrites à l'**Annexe 3**. Ces mesures portent sur son propre poste de travail, sur ses modalités d'accès aux Systèmes du Client et sur le traitement des Copies de travail. Elles peuvent évoluer, sous réserve de ne pas abaisser le niveau de sécurité initial.

La sécurité des Systèmes du Client eux-mêmes — disponibilité, sauvegardes, chiffrement au repos, contrôle d'accès des utilisateurs finaux, renouvellement des certificats — **relève du Client**, qui en conserve la maîtrise. Le Prestataire l'assiste sur ces points dans les limites de la prestation souscrite et l'alerte de toute faiblesse constatée.

4.6 Recours à des sous-traitants ultérieurs

Le Prestataire **ne recourt à aucun sous-traitant ultérieur** à ce jour (Annexe 2).

S'il devait en employer un, le Client lui donne une **autorisation générale**, assortie d'une **information écrite préalable au moins trente (30) jours** avant sa mise en œuvre. Le Client dispose de ce délai pour formuler des objections motivées ; à défaut d'accord, il peut résilier la prestation concernée sans indemnité.

Le Prestataire imposerait à tout sous-traitant ultérieur, **par contrat**, les mêmes obligations de protection des données que celles du présent Accord, et demeurerait **pleinement responsable** devant le Client de l'exécution par celui-ci de ses obligations.

4.7 Droits des personnes concernées

Le Prestataire ne répond pas directement aux demandes d'exercice de droits (accès, rectification, effacement, limitation, portabilité, opposition) émanant des personnes concernées : il les **transmet au Client sans délai**, et au plus tard sous **cinq (5) jours ouvrés**.

Il apporte au Client, **compte tenu de la nature du traitement**, toute l'aide nécessaire par des mesures techniques et organisationnelles appropriées pour lui permettre de s'acquitter de son obligation de donner suite à ces demandes (**articles 12 à 23 du RGPD**). Les Données demeurant sur les Systèmes du Client, cette aide prend principalement la forme d'une **assistance technique à l'extraction, à la rectification ou à l'effacement** effectués par le Client lui-même.

4.8 Assistance au Client

Le Prestataire aide le Client à garantir le respect des obligations prévues aux **articles 32 à 36 du RGPD**, compte tenu de la nature du traitement et des informations à sa disposition :

- sécurité des traitements (art. 32) ;
- notification des violations à l'autorité de contrôle (art. 33) et communication aux personnes concernées (art. 34) ;
- **analyse d'impact relative à la protection des données** (art. 35) et consultation préalable de l'autorité de contrôle (art. 36).

4.9 Notification des violations de données

Le Prestataire notifie au Client **toute violation de Données** dont il a connaissance et qui résulte de son intervention ou affecte ses Copies de travail, **par email et par téléphone**, dans les meilleurs délais et **au plus tard quarante-huit (48) heures** après en avoir pris connaissance — délai calibré pour préserver au Client le temps utile à sa propre notification à la CNIL sous 72 heures (**art. 33.1 RGPD**).

Il alerte également le Client, dans le même délai, de **toute violation affectant les Systèmes du Client qu'il viendrait à constater** au cours d'une intervention, quand bien même elle lui serait étrangère.

La notification comporte, dans la mesure du possible, les éléments de l'**article 33.3 du RGPD** : nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises ou proposées.

La notification à l'autorité de contrôle et, le cas échéant, aux personnes concernées incombe au Client en sa qualité de responsable de traitement.

4.10 Registre des activités de traitement

Le Prestataire tient un **registre de toutes les catégories d'activités de traitement effectuées pour le compte du Client**, conformément à l'**article 30.2 du RGPD**. Ce registre est mis à disposition du Client et de l'autorité de contrôle sur demande.

4.11 Point de contact

Le Prestataire n'est pas tenu de désigner un délégué à la protection des données au sens de l'article 37 du RGPD. Le point de contact unique pour toute question relative au présent Accord est : `contact@phenix-tech.fr`.

4.12 Mise à disposition et audit

Le Prestataire met à la disposition du Client **toutes les informations nécessaires pour démontrer le respect** des obligations de l'article 28 du RGPD (**art. 28.3.h**).

Il permet la réalisation d'**audits**, y compris des inspections, par le Client ou un auditeur mandaté par lui, dans les conditions suivantes :

- **un (1) audit par année civile** au maximum, sauf survenance d'une violation de Données ou demande d'une autorité de contrôle ;
- préavis écrit d'au moins **trente (30) jours** ;
- pendant les heures ouvrées, sans perturbation disproportionnée de l'activité ;
- l'auditeur mandaté ne doit pas être un concurrent du Prestataire et est soumis à un engagement de confidentialité ;
- **frais à la charge du Client**, sauf si l'audit révèle un manquement substantiel du Prestataire.

Le Prestataire n'exploitant aucune infrastructure d'hébergement, l'audit porte sur ses **procédures, ses modalités d'accès et la gestion de ses Copies de travail**, et non sur des installations d'hébergement.

Article 5 — Obligations du Client

Le Client garantit au Prestataire :

- qu'il dispose d'une **base légale** valable (art. 6 RGPD) pour chacun des traitements confiés, et le cas échéant d'une condition de levée d'interdiction pour les données sensibles (art. 9) ;
- qu'il a **informé les personnes concernées** conformément aux articles 12 à 14 du RGPD, y compris du recours au Prestataire ;
- que les **instructions** qu'il donne sont licites et documentées ;
- qu'il **supervise** le traitement et répond aux demandes d'exercice de droits.

Les Systèmes du Client restant sous sa maîtrise, le Client demeure en outre responsable :

- du **choix et du contrat de son hébergeur**, ainsi que de la localisation des Données qui en résulte ;
- de la **disponibilité, des sauvegardes et de leur restauration** ;
- de la **gestion des comptes et des droits** de ses propres utilisateurs ;
- de l'application des **mises à jour de sécurité** en dehors du périmètre d'un contrat de maintenance souscrit auprès du Prestataire.

Le Client s'abstient de transmettre au Prestataire des Données excédant ce qui est nécessaire à l'exécution du Contrat (**principe de minimisation**, art. 5.1.c RGPD), et notamment de lui communiquer des jeux de données réels lorsque des données de test suffisent.

Article 6 — Localisation des Données et transferts hors Union européenne

Les Données demeurent en permanence sur les Systèmes du Client. Le Prestataire n'héberge, ne stocke et ne réplique aucune Donnée du Client sur une infrastructure qu'il exploiterait pour son compte.

Deux exceptions strictement délimitées, toutes deux situées **en France** :

- les **Copies de travail** temporaires constituées sur le poste de travail du Prestataire pour les besoins d'une migration, d'un diagnostic ou d'une recette, traitées conformément à l'Annexe 3 et supprimées dans les conditions de l'article 7 ;
- les **flux de prise en main à distance**, qui transitent par le serveur relais RustDesk **auto-hébergé par le Prestataire en France**, sans conservation du contenu de la session.

Aucun transfert de Données hors de l'Union européenne n'est effectué, ni vers un prestataire soumis à une législation d'accès extraterritorial aux données de type *CLOUD Act*. Aucun fournisseur de cloud public n'intervient. Tout projet de transfert hors UE ferait l'objet d'une instruction écrite préalable du Client et de garanties appropriées au sens de l'article 46 du RGPD.

La localisation des Données hébergées relevant du contrat souscrit par le Client auprès de son propre hébergeur, il lui appartient de s'assurer que celui-ci offre des garanties équivalentes. Le Prestataire l'assiste dans ce choix au titre de son devoir de conseil.

Article 7 — Sort des Données au terme du Contrat

La restitution des Données est sans objet : elles n'ont jamais quitté les Systèmes du Client, qui en conserve la maîtrise pleine et entière au terme du Contrat.

Au terme de la prestation, le Prestataire s'engage à :

1. **supprimer l'intégralité des Copies de travail** — exports de migration, sauvegardes préalables, extractions de diagnostic, fichiers temporaires — dans un délai de **trente (30) jours**, y compris dans ses propres sauvegardes sous réserve de leurs délais de rotation techniques (**quatre-vingt-dix (90) jours** au maximum) ;
2. **restituer au Client puis effacer tout identifiant, clé, certificat ou secret** d'accès à ses Systèmes, et demander la **révocation des comptes d'administration** créés à son bénéfice pour les besoins de la mission, dans un délai de **sept (7) jours** ;
3. **cesser tout accès** aux Systèmes du Client.

Le Prestataire ne conserve au-delà que les éléments dont la conservation lui est **imposée par une obligation légale** (notamment les pièces comptables, art. L. 123-22 C. com.), pour la seule durée de cette obligation et à cette seule fin, ainsi que les livrables de la mission expurgés de toute Donnée (documentation technique, configuration type). Une **attestation de suppression** est délivrée sur demande.

Article 8 — Durée, responsabilité et divers

Le présent Accord entre en vigueur à la date de signature du Contrat et demeure applicable **tant que le Prestataire est susceptible d'accéder à des Données pour le compte du Client**, ainsi que pour les obligations qui lui survivent (confidentialité, suppression, attestation).

Chaque Partie répond des dommages causés par un traitement qui contreviendrait au RGPD dans les conditions de l'**article 82 du RGPD**. Les plafonds de responsabilité stipulés au Contrat et aux CGV B2B ne s'appliquent pas aux amendes administratives prononcées par une autorité de contrôle à l'encontre d'une Partie du fait de ses propres manquements.

En cas de contradiction entre le présent Accord et le Contrat ou les CGV B2B **sur un point relatif à la protection des données personnelles**, le présent Accord prévaut.

Droit applicable : **droit français**. Juridiction compétente : celle stipulée aux CGV B2B.

Annexe 1 — Description des traitements

Tableau à **individualiser au contrat** : ne conserver que les lignes correspondant aux prestations réellement souscrites, et compléter les catégories de personnes concernées propres au Client.

Dans tous les cas ci-dessous, **les Données résident sur les Systèmes du Client** ; le Prestataire y accède sans en devenir dépositaire.

Prestation	Nature et finalité du traitement	Catégories de Données	Catégories de personnes concernées	Durée
Mise en place Nextcloud Pro	Installation, configuration et paramétrage de l'instance sur l'infrastructure du Client ou sur l'hébergement qu'il a souscrit ; création des comptes et des droits ; recette	Comptes et identifiants des utilisateurs ; par ricochet, les contenus déjà présents lors des tests	Salariés du Client, ses contacts	Durée de la mission de mise en place
Reprise / migration de données	Extraction depuis l'ancien système et injection dans la nouvelle instance	Fichiers, contacts, agendas, messages migrés	Salariés du Client, ses clients et contacts	Durée de la migration ; Copies de travail supprimées sous 30 jours (art. 7)
Mise en place email professionnel	Configuration des boîtes, du routage et des enregistrements DNS sur l'hébergement souscrit par le Client en son nom propre	Adresses email, et le cas échéant messages repris lors d'une migration	Salariés du Client et leurs correspondants	Durée de la mission
Création de site web	Développement puis déploiement sur l'hébergement du Client ; paramétrage des formulaires	Données saisies via les formulaires du site, le cas échéant contenus existants repris	Visiteurs et prospects du Client	Durée de la mission
Maintenance web	Mises à jour, correctifs et interventions sur le site en production, hébergé par le Client	Données saisies via les formulaires du site	Visiteurs et prospects du Client	Durée du contrat de maintenance
Automatisation n8n	Conception, test et maintenance de workflows exécutés sur l'instance du Client	Selon le workflow — à préciser au contrat	Selon le workflow — à préciser au contrat	Durée du contrat ; en conception et recette, données fictives ou anonymisées par défaut
Support à distance (RustDesk)	Prise en main à distance d'un poste pour diagnostic, dépannage, configuration ou formation	Données visibles à l'écran pendant la session	Salariés du Client et tiers dont les données sont affichées	Aucune conservation du contenu — la session est fermée en fin d'intervention ; journaux de connexion du relais : 12 mois

Les conditions détaillées du support à distance figurent à l'annexe `PTC-ANNEXE-RUSTDESK`.

Annexe 2 — Sous-traitants ultérieurs

Aucun sous-traitant ultérieur n'intervient.

Le Prestataire n'exploitant aucun hébergement pour le compte du Client, aucune Donnée n'est confiée à un tiers. Précisions utiles :

- le **serveur relais RustDesk** est l'infrastructure propre du Prestataire, auto-hébergée en France : il ne s'agit pas d'un tiers, et aucun serveur relais public n'est utilisé ;
- les **logiciels libres** mis en œuvre (Nextcloud, n8n, RustDesk, Home Assistant) sont installés sur les Systèmes du Client ou du Prestataire : leurs éditeurs n'ont **aucun accès** aux Données et ne sont pas des sous-traitants ultérieurs ;
- **Infomaniak Network SA** assure la messagerie du Prestataire pour sa propre relation commerciale (devis, factures, échanges). Ce traitement relève de sa qualité de **responsable de traitement** et **non du présent Accord** : aucune Donnée traitée pour le compte du Client n'y transite ;
- l'**hébergeur du Client** et sa **solution de sauvegarde**, lorsqu'il les souscrit, sont des sous-traitants **du Client**, contractés directement par lui. Ils n'entrent pas dans la chaîne de sous-traitance du Prestataire, qui se borne à les configurer sur instruction.

Toute évolution de cette liste suivrait la procédure de l'article 4.6.

Annexe 3 — Mesures techniques et organisationnelles (art. 32 RGPD)

Périmètre et répartition des responsabilités : voir article 4.5.

Poste de travail du Prestataire

- Chiffrement intégral du disque ; verrouillage automatique de session.
- Système et outils maintenus à jour des correctifs de sécurité.
- Aucune synchronisation des Copies de travail vers un service de cloud public.

Accès aux Systèmes du Client

- Comptes **nominatifs**, jamais partagés ; authentification forte lorsque le système du Client le permet.
- Secrets, clés et certificats conservés dans un **gestionnaire de mots de passe dédié et chiffré**, jamais en clair dans un dépôt de code, un email ou un fichier de configuration.
- Accès demandés au **niveau de privilège minimal** nécessaire à la mission, et **révoqués à son terme** (art. 7).
- Traçabilité des interventions : date, périmètre et nature de l'opération consignés.

Copies de travail

- Constituées **uniquement lorsque la prestation l'exige** (migration, diagnostic, sauvegarde préalable à une intervention).

- **Chiffrées** et cloisonnées du reste du poste.
- **Supprimées dans les 30 jours** suivant la fin de la mission, sauvegardes comprises sous réserve d'une rotation technique de 90 jours maximum.

Prise en main à distance

- **Consentement explicite du Client pour chaque session**, chiffrement de bout en bout, serveur relais auto-hébergé en France : aucun accès non surveillé, aucun enregistrement de session.
- Conditions détaillées — modalités de consentement, durées de conservation des journaux, garanties techniques — à l'annexe `PTC-ANNEXE-RUSTDESK`, qui fait seule référence en cas de divergence.

Organisation

- **Procédure documentée de notification de violation** : détection, confinement, évaluation sous 4 h, notification, documentation, bilan post-incident.
- **Registre des activités de traitement** tenu au titre de l'article 30.2 du RGPD.
- **Registre des violations** tenu conformément à l'article 33.5 du RGPD.
- **Aucun sous-traitant ultérieur**, donc aucune chaîne de sous-traitance à auditer.