

# Contrat de sous-traitance RGPD

EcoSuivi — DPA

Version 0.2 — 21 avril 2026

Ecosuivi SASU — RCS Paris 103 668 943  
47 rue Vivienne, 75002 Paris — [contact@ecosuivi.com](mailto:contact@ecosuivi.com)

# Contrat de sous-traitance RGPD (Data Processing Agreement — DPA)

---

Entre d'une part :

**Ecosuivi**, Société par Actions Simplifiée à associé unique, au capital de 1 000 euros, immatriculée au Registre du Commerce et des Sociétés de Paris sous le numéro 103 668 943, dont le siège social est situé 47 rue Vivienne, 75002 Paris, représentée par son Président, Monsieur Ronan Seveno, ci-après désignée « **Ecosuivi** » ou « **le Sous-traitant** ».

Et d'autre part :

**L'Organisation** telle qu'identifiée lors de l'inscription sur l'Application EcoSuivi, représentée par son Utilisateur dûment habilité, ci-après désignée « **le Client** » ou « **le Responsable de traitement** ».

Ecosuivi et le Client sont ci-après individuellement désignés « **la Partie** » et collectivement « **les Parties** ».

---

## Préambule

---

Dans le cadre de l'utilisation de l'Application EcoSuivi, le Client est amené à saisir, téléverser ou générer des données à caractère personnel dont il est Responsable de traitement au sens de l'article 4.7 du Règlement général sur la protection des données (RGPD — règlement UE 2016/679), notamment :

- les coordonnées du porteur de projet lorsqu'il s'agit d'une personne physique (nom, adresse, téléphone, e-mail) ;
- les noms et qualifications des opérateurs terrain figurant sur les photographies ou dans les métadonnées EXIF ;
- les coordonnées de riverains, agriculteurs exploitants, ou autres tiers mentionnés dans les études.

Ecosuivi, en qualité d'hébergeur et d'exploitant du Service, traite ces données pour le compte du Client et agit par conséquent en qualité de **Sous-traitant** au sens de l'article 4.8 du RGPD.

Le présent Contrat de sous-traitance a pour objet d'encadrer ce traitement, conformément à l'article 28 du RGPD.

**Acceptation et opposabilité.** Le présent Contrat constitue une **Annexe indissociable des CGU**. Il est réputé **accepté par le Client dès l'acceptation des CGU par l'Utilisateur habilité à engager l'Organisation** au moment de l'inscription (Utilisateur disposant d'un mandat, d'une délégation de signature ou de la qualité de représentant légal de l'Organisation). Il s'applique automatiquement et sans formalité supplémentaire dès lors que le Client saisit, téléverse ou génère dans l'Application des données à caractère personnel relatives à des tiers.

Le Client garantit à l'Éditeur que l'Utilisateur procédant à l'inscription dispose du pouvoir d'engager l'Organisation pour les besoins du présent Contrat. En cas de contestation ultérieure par l'Organisation, l'Utilisateur reste tenu solidairement des obligations nées avant la résolution du différend.

**Version et mise à jour.** La version en vigueur du présent Contrat est consultable à tout moment depuis l'Application et depuis le site ecosuivi.com. Toute modification substantielle fait l'objet d'une **notification au Client au moins trente (30) jours avant son entrée en vigueur**, par courrier électronique à l'administrateur de l'Organisation et par bannière dans l'Application. Passé ce délai, la poursuite de l'utilisation du Service vaut acceptation de la nouvelle version. Le Client qui refuse les modifications peut résilier son Compte sans préavis ni pénalité.

## Article 1 — Objet et description du traitement

### 1.1 Nature des traitements réalisés par le Sous-traitant

Pour le compte du Client, le Sous-traitant réalise les opérations de traitement suivantes au sens de l'article 4.2 du RGPD :

- **hébergement** et **stockage** des données sur des infrastructures situées en France (cf. article 2.11) ;
- **sauvegarde** quotidienne avec rotation sur sept (7) jours glissants ;
- **consultation** et **mise à disposition pour affichage** des données dans l'interface de l'Application, au profit de l'Utilisateur concerné et des autres membres de l'Organisation disposant des droits d'accès appropriés ;
- **export** des données vers des formats structurés (Excel, CSV, JSON, GeoJSON, SHP) à la demande du Client ;
- **pré-remplissage automatisé** de certains champs de Projet à partir de données publiques ouvertes (IGN, INPN, SANDRE, BRGM, Eaufrance, etc.) — ce pré-remplissage **ne crée pas** de données personnelles supplémentaires et reste sous la maîtrise du Client qui peut à tout moment les modifier ou les supprimer ;
- **journalisation des accès et des actions** dans un journal technique permettant la traçabilité, la détection d'intrusions et la réponse aux demandes d'exercice de droits (art. 2.5 et art. 2.6 ci-après) ;
- **suppression** ou **anonymisation** des données conformément à l'article 2.10.

Le Sous-traitant **n'utilise en aucune manière les données du Client à d'autres fins** que l'exécution du Service. Il ne procède à **aucune exploitation secondaire** (entraînement de modèles d'intelligence artificielle, revente à des tiers, analyses statistiques publiées, enrichissement de bases de données tierces).

### 1.2 Finalités du traitement

Le traitement est réalisé exclusivement aux finalités suivantes :

- permettre au Client de **conduire une évaluation MNEFZH v2** (application de la méthode sur un ou plusieurs Couples site impacté / site de compensation) ;
- permettre au Client de **produire les livrables** attendus par la méthode (tableur des sites, photos référencées, fichiers SIG) ;
- assurer l'**exécution des CGU** et du présent Contrat (authentification, facturation le cas échéant, gestion du support) ;
- garantir la **sécurité du Service** au profit du Client et des autres Utilisateurs (détection d'incidents, investigation, réponse à une violation de données).

Aucune autre finalité ne peut être poursuivie sans instruction documentée préalable du Client.

### 1.3 Durée

Le présent Contrat prend effet à la date d'acceptation des CGU par le Client et court jusqu'à la résiliation du Compte ou de l'abonnement. Les données sont ensuite conservées pendant 30 jours (période d'export), puis supprimées ou anonymisées dans un délai maximal de 90 jours.

### 1.4 Catégories de données à caractère personnel traitées

- **données d'identification** : nom, prénom, fonction ou qualification professionnelle ;
- **coordonnées de contact** : adresse postale, adresse électronique, numéro de téléphone ;
- **images et photographies** : clichés de sondages pédologiques, d'habitats, de parcelles, de dispositifs d'ouvrage — pouvant contenir des personnes identifiables (opérateurs terrain, riverains de passage) ;
- **métadonnées EXIF des photographies** : coordonnées GPS de la prise de vue, horodatage, cap (boussole), altitude, modèle et numéro de série de l'appareil utilisé — ces métadonnées peuvent constituer, prises isolément ou recoupées, des données à caractère personnel ;
- **données de localisation précise** : coordonnées GPS associées aux sondages pédologiques, aux limites de Sites, aux points de mesure ;
- **annotations libres** : commentaires, observations et notes saisis dans les champs ouverts de l'Application — le Client demeure responsable de s'assurer que ces champs ne contiennent pas de données personnelles de tiers qu'il n'aurait pas le droit de traiter.

Aucune **donnée sensible** au sens de l'article 9 du RGPD (santé, origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques ou biométriques, orientation sexuelle) ne doit être saisie dans l'Application. Aucune **donnée relative à des condamnations pénales** au sens de l'article 10 du RGPD ne doit non plus y figurer. Le Client s'engage à ne pas téléverser de telles données et assume l'entière responsabilité d'un manquement à cette obligation.

### 1.5 Catégories de personnes concernées

- **porteurs de projet** lorsqu'il s'agit de personnes physiques (particuliers, exploitants individuels, professions libérales) ;
- **exploitants agricoles et riverains** mentionnés dans le cadre de l'étude, notamment dans les analyses de pressions anthropiques ou d'usages du sol ;
- **opérateurs terrain** du Client ou de ses propres sous-traitants, susceptibles d'apparaître sur les photographies ou dans leurs métadonnées ;
- **employés du Client** (chargés d'études, écologues, pédologues) dont le nom figure en tant qu'auteur ou contributeur d'une saisie, d'une photographie ou d'un livrable — le traitement des données des salariés du Client obéit aux obligations d'information renforcée prévues par le Code du travail, dont le respect incombe au Client ;
- **tiers quelconques** dont l'identité apparaîtrait incidemment dans une photographie ou une annotation libre, sans que leur identification ait été recherchée par le Client.

## Article 2 — Obligations du Sous-traitant

---

Conformément à l'article 28.3 du RGPD, le Sous-traitant s'engage à :

## 2.1 Agir sur instructions documentées

Ne traiter les données que sur instructions documentées du Client, y compris en ce qui concerne les transferts vers un pays tiers ou à une organisation internationale, sauf obligation légale contraire. Les CGU et les fonctionnalités mises à disposition dans l'Application constituent l'essentiel de ces instructions.

## 2.2 Confidentialité

Garantir que les personnes autorisées à traiter les données sont soumises à une obligation de confidentialité contractuelle (clause de confidentialité dans les contrats de travail et contrats de prestation) ou à une obligation légale appropriée. **Cette obligation de confidentialité survit à la cessation de la relation contractuelle entre la personne concernée et le Sous-traitant, pendant une durée minimale de cinq (5) ans.**

## 2.3 Sécurité

Mettre en œuvre les mesures techniques et organisationnelles appropriées au sens de l'article 32 du RGPD, notamment :

- chiffrement en transit (HTTPS / **TLS 1.3**, TLS 1.2 accepté en repli pour les clients legacy) ;
- chiffrement au repos des stockages objets contenant les photos ;
- **hachage des mots de passe avec l'algorithme Argon2id** (ou équivalent à l'état de l'art), **jamais en clair** ;
- contrôle d'accès par authentification forte et cloisonnement par Organisation ;
- journalisation des accès sensibles ;
- sauvegardes quotidiennes avec rotation de 7 jours ;
- mises à jour régulières des composants logiciels ;
- environnement de production isolé des environnements de développement et de recette ;
- revues de code et tests de sécurité réguliers.

## 2.4 Recours à des sous-traitants ultérieurs

Le Sous-traitant peut recourir à des sous-traitants ultérieurs, à condition :

- d'informer préalablement le Client par tout moyen (notification dans l'Application, e-mail) ;
- d'imposer à ces sous-traitants des obligations de protection des données au moins équivalentes à celles du présent Contrat.

**Liste des sous-traitants ultérieurs à date** (à maintenir à jour) :

Sous-traitant ultérieur	Rôle	Localisation
<b>OVH SAS</b> (RCS Lille 424 761 419)	Hébergement des serveurs applicatifs, de la base de données PostgreSQL et du stockage objet (photos de	France (régions OVH : Roubaix, Gravelines, Strasbourg, Limoges)

Sous-traitant ultérieur	Rôle	Localisation
	sondages, exports SIG)	
<b>Brevo</b> ( <i>choix à confirmer — alternative OVH Email Pro</i> )	Envoi des e-mails transactionnels (confirmation d'inscription, ré-initialisation de mot de passe, notifications)	France (Paris)
<b>LegalPlace Pro</b>	Outil comptable mobilisé pour la facturation et les déclarations fiscales — traite incidemment les noms et coordonnées de facturation des clients professionnels	France

Le Client dispose d'un délai de **trente (30) jours** à compter de la notification pour s'opposer à l'ajout d'un nouveau sous-traitant ultérieur. À défaut d'opposition dans ce délai, l'ajout est réputé accepté. En cas d'opposition maintenue, chaque Partie peut résilier le contrat sans pénalité, avec restitution ou suppression des données selon l'article 2.10.

## 2.5 Droits des personnes concernées

Le Sous-traitant aide le Client à répondre aux demandes d'exercice des droits des personnes concernées (accès, rectification, effacement, opposition, limitation, portabilité) par la mise à disposition des fonctionnalités idoines dans l'Application (export, suppression de Projet, suppression de Compte).

Lorsqu'une personne s'adresse directement au Sous-traitant pour exercer ses droits, le Sous-traitant **transfère la demande au Client dans un délai maximal de cinq (5) jours ouvrés**, accompagnée des éléments techniques utiles à son traitement.

## 2.6 Notification de violation de données

Le Sous-traitant notifie au Client toute violation de données à caractère personnel au sens de l'article 4.12 du RGPD dans un délai **maximal de vingt-quatre (24) heures** après en avoir pris connaissance, par courrier électronique à l'adresse du Compte administrateur de l'Organisation et, le cas échéant, par appel téléphonique de courtoisie.

Ce délai est calculé pour laisser au Client, en sa qualité de Responsable de traitement, une marge de quarante-huit (48) heures avant l'expiration du délai de soixante-douze (72) heures qui lui est imparti pour notifier la violation à la CNIL (article 33 RGPD).

La notification du Sous-traitant contient au minimum :

- la description de la nature de la violation ;
- les catégories et le nombre approximatif de personnes et d'enregistrements concernés ;
- les conséquences probables de la violation ;
- les mesures prises ou proposées pour y remédier, y compris les mesures d'atténuation des effets négatifs.

Si tous ces éléments ne sont pas immédiatement disponibles, le Sous-traitant procède à une notification initiale contenant les éléments disponibles, puis à des notifications complémentaires au fur et à mesure.

Il appartient au Client, en sa qualité de Responsable de traitement, de procéder à la notification auprès de la CNIL (article 33 RGPD) et, le cas échéant, auprès des personnes concernées (article 34 RGPD), dans les délais qui lui sont imposés.

## 2.7 Analyse d'impact relative à la protection des données (AIPD / DPIA)

Le Sous-traitant aide le Client à réaliser, lorsque celle-ci est requise au sens de l'article 35 du RGPD, une analyse d'impact relative à la protection des données.

À cet effet, le Sous-traitant met à disposition du Client, sur demande et dans un délai maximal de **dix (10) jours ouvrés**, les informations suivantes :

- description détaillée des mesures techniques et organisationnelles de sécurité mises en œuvre ;
- cartographie des flux de données (flux entrants, flux sortants, flux internes) ;
- liste exhaustive et à jour des sous-traitants ultérieurs (cf. art. 2.4) ;
- durées de conservation effectives par catégorie de données (cf. Politique de confidentialité) ;
- attestations et certifications disponibles (notamment certifications hébergeur OVH).

## 2.8 Registre des activités de traitement

Le Sous-traitant tient un registre des catégories d'activités de traitement effectuées pour le compte du Client, conformément à l'article 30.2 du RGPD.

## 2.9 Audit

Sous réserve d'un préavis raisonnable de 30 jours, et sans perturber le Service, le Client peut demander à auditer le respect par le Sous-traitant des obligations prévues à l'article 28 du RGPD. Un audit sur pièces (questionnaire, certifications, attestations de conformité) est privilégié. Les audits sur site ne peuvent avoir lieu qu'en cas de motif légitime et font l'objet d'un accord préalable sur leurs modalités et coûts.

## 2.10 Sort des données au terme du Contrat

À la résiliation du Contrat, le Sous-traitant :

- met à disposition du Client un export complet des données pendant 30 jours ;
- procède à la suppression ou à l'anonymisation des données dans un délai maximal de 90 jours ;
- supprime les copies existantes (sauvegardes comprises, selon la rotation naturelle de la politique de sauvegarde) ;
- transmet une attestation de suppression au Client sur demande.

## 2.11 Localisation des données

Les données sont hébergées **exclusivement sur des infrastructures situées en France** (régions OVH de Roubaix, Gravelines, Strasbourg ou Limoges). Tout changement de localisation, même au sein de l'Union européenne, est notifié au Client selon la procédure de changement de sous-traitant ultérieure prévue à l'article 2.4.

## 2.12 Interdiction des transferts hors Union européenne

Aucun transfert de données à caractère personnel hors de l'Union européenne ou de l'Espace économique européen n'est autorisé dans le cadre de l'exécution du présent Contrat.

Toute dérogation à cette interdiction suppose **l'accord écrit préalable et exprès du Client**, ainsi que la mise en place effective d'un mécanisme de transfert conforme à l'article 46 du RGPD (clauses contractuelles types de la Commission européenne, règles d'entreprise contraignantes, décision d'adéquation ou dérogations de l'article 49).

Le Sous-traitant s'engage à ne recourir à aucun sous-traitant ultérieur qui procéderait à des transferts hors UE sans respecter ces conditions.

## Article 3 — Obligations du Client

---

Le Client, en qualité de Responsable de traitement, s'engage à :

- disposer d'une base légale pour le traitement de chaque donnée personnelle saisie dans l'Application ;
- informer les personnes concernées de la collecte et du traitement de leurs données ;
- respecter les droits des personnes concernées ;
- ne pas saisir de données sensibles au sens de l'article 9 du RGPD ;
- veiller à la confidentialité des identifiants de connexion et à la gestion appropriée des habilitations au sein de son Organisation ;
- documenter le recours à Ecosuivi comme sous-traitant dans son propre registre des traitements.

## Article 4 — Coopération

---

Les Parties coopèrent de bonne foi pour remplir leurs obligations respectives au titre du RGPD. Chaque Partie désigne un point de contact :

- **Côté Sous-traitant** : [contact@ecosuivi.com](mailto:contact@ecosuivi.com)

- **Côté Client** : l'Utilisateur disposant des droits d'administration dans l'Organisation

## Article 5 — Responsabilité

---

Chaque Partie est responsable des dommages causés par le traitement lorsqu'elle n'a pas respecté les obligations du RGPD qui lui incombent (article 82 RGPD). La responsabilité du Sous-traitant est engagée uniquement si le Sous-traitant n'a pas respecté les obligations du RGPD qui lui incombent spécifiquement ou s'il a agi en dehors ou contrairement aux instructions licites du Responsable de traitement.

La responsabilité du Sous-traitant est en tout état de cause limitée dans les conditions prévues aux CGU.

## Article 6 — Documentation

---

Le Sous-traitant met à disposition du Client, sur demande, toute documentation nécessaire pour démontrer le respect des obligations prévues au présent Contrat (politique de sécurité, description des mesures techniques, liste des sous-traitants ultérieurs, attestations de sauvegarde, etc.).

## Article 7 — Droit applicable et juridiction

---

Le présent Contrat est soumis au droit français. Tout litige relève de la compétence exclusive des tribunaux de Paris.

### Version : v0.2 — 2026-04-21 **Évolutions v0.1 → v0.2** :

- Préambule : ajout du mécanisme d'acceptation (inscription de l'Utilisateur habilité), opposabilité au Client, versioning et mise à jour à 30 jours de préavis ;
- art. 1.1 : enrichissement des opérations de traitement (consultation, journalisation, pré-remplissage à partir de données publiques) + interdiction explicite d'exploitation secondaire (IA, revente, enrichissement de bases tierces) ;
- art. 1.2 : reformulation des finalités, ajout « exécution des CGU et du présent Contrat » ;
- art. 1.4 : ajout des métadonnées EXIF, des annotations libres, et extension de l'interdiction aux données pénales (art. 10 RGPD) ;
- art. 1.5 : ajout des employés du Client et des tiers incidemment identifiés ;
- art. 2.2 : obligation de confidentialité **survit 5 ans** après la fin de la relation ;
- art. 2.3 : TLS 1.3, Argon2id, précision environnements dev/recette/prod ;
- art. 2.4 : sous-traitants ultérieurs **complétés** (OVH SAS, Brevo, LegalPlace Pro), délai d'opposition **30 jours** (au lieu de 15) ;
- art. 2.5 : transfert des demandes de droits au Client sous **5 jours ouvrés** (au lieu de « délai raisonnable ») ;
- art. 2.6 : notification de violation **24 h** (au lieu de 48 h) pour laisser 48 h de marge au Client avant son obligation de notification CNIL ;
- art. 2.7 : AIPD renforcée, documentation fournie sous **10 jours ouvrés** avec contenu détaillé ;
- art. 2.11 : hébergement **exclusivement en France** (au lieu de France ou UE), cohérence CGU v0.3 art. 6 ;

- **art. 2.12 (nouveau)** : interdiction explicite des transferts hors UE sauf accord écrit du Client + mécanisme art. 46 RGPD.

**À traiter ensemble ultérieurement (articles 3 à 7)** : obligations du Client, coopération, responsabilité, documentation, droit applicable — prochaine passe de relecture.

**Document à soumettre à la relecture d'un avocat ou d'un DPO externe avant publication**, notamment pour :

- valider la restriction « hébergement France uniquement » au regard de la libre prestation de services UE (Schrems II a durci les contraintes côté hors-UE mais pas intra-UE) ;
- vérifier la compatibilité avec les éventuelles exigences spécifiques des bureaux d'études intervenant pour des donneurs d'ordre publics (collectivités, État, établissements publics) — certains cahiers des charges imposent la certification HDS ou SecNumCloud qui sortiraient d'OVH Public Cloud ;
- confirmer qu'une cyber-assurance n'est pas nécessaire en phase V1 (reportée à v2 lorsque le CA permettra de financer la prime de ~300-800 €/an).