

Annexes du contrat de sous-traitance

Annexes I à IV de l'accord conclu au titre de l'article 28 du RGPD, sur la base des Clauses Contractuelles Types de la Décision d'exécution (UE) 2021/915. À joindre au contrat signé entre chaque conseiller et la plateforme.

28

article du RGPD

7

sous-traitants ultérieurs

0

transfert hors UE

15 j

effacement chez
l'imprimeur

Établi le 25 août 2026 · Version 3

Responsable du traitement : le conseiller immobilier · Sous-traitant : la plateforme

Toutes les mesures décrites ont été vérifiées dans le code avant rédaction

Avertissement de rédaction

Ces annexes ont été établies à partir du **fonctionnement réel du système**, et non d'une description commerciale. Chaque mesure de l'annexe III a été relue dans le code source avant d'être écrite ici.

Ce qui n'est pas encore en place est signalé **en rouge** plutôt que passé sous silence. Une annexe qui promet une garantie inexistante expose le signataire bien plus qu'un blanc assumé.

Annexe I – Les parties

A. Responsable du traitement

Identité	Nom, prénom ou raison sociale du conseiller — renseigné à la création du compte
Habilitation	Carte professionnelle « Transactions sur immeubles et fonds de commerce » et CCI de délivrance, <i>ou</i> numéro RSAC et greffe (loi n° 70-9 du 2 janvier 1970)
Coordonnées	Adresse professionnelle, téléphone, adresse électronique
Signature	Par acceptation en ligne, horodatée, avec conservation du libellé exact accepté et de l'adresse IP

B. Sous-traitant

Identité	Gildo Pandi — Entreprise individuelle (EI) , SIREN 830 339 057, Metz (Moselle). Régime de la micro-entreprise. Pas de capital social ni d'immatriculation au RCS : la forme est l'entreprise individuelle, dont le patrimoine professionnel est séparé depuis la loi du 14 février 2022. La mention « EI » accompagne le nom sur les documents professionnels, comme l'impose l'article L.526-22 du code de commerce.
Représentant	Gildo Pandi, Metz (Moselle)
Contact protection des données	gildopandi2010@gmail.com

Annexe II – Description du traitement

a. Catégories de personnes concernées

- Propriétaires ou occupants d'un logement ayant fait l'objet d'un diagnostic de performance énergétique dans le secteur géographique du Responsable du traitement.
- Personnes ayant scanné le code figurant sur le document reçu et ayant donné leur accord pour être recontactées.
- Destinataires des courriers d'information ayant complété le formulaire en ligne.
- Personnes ayant exercé leur droit d'opposition.

b. Catégories de données

CATÉGORIE	DONNÉES	ORIGINE
-----------	---------	---------

Logement	Adresse postale ; étiquette énergétique et climat ; surface habitable ; année de construction ; type de bâtiment ; numéro de diagnostic	Base ADEME dpe03existant, Licence Ouverte 2.0 ; Base Adresse Nationale
Accord de recontact	Numéro de téléphone ; nom et prénom si la personne les indique ; créneau souhaité ; horodatage serveur ; adresse IP ; libellé exact de chaque case et son état ; méthode de recueil	Saisie par la personne elle-même
Qualification déclarative	Données déclaratives fournies volontairement par la personne concernée : estimation subjective de la valeur par le propriétaire, horizon prévisionnel de vente, statut d'occupation du bien, historique déclaratif des travaux réalisés	Saisie par la personne elle-même, postérieurement au recueil de son accord
Opposition	Adresse du logement ; message libre éventuel ; horodatage serveur ; adresse IP	Formulaire public d'opposition

Données non traitées

Aucune donnée relevant de l'article 9 du RGPD. **Aucun nom, prénom, téléphone ou adresse électronique n'est recherché ni associé avant le premier contact** : ni par annuaire inversé, ni par fichiers fonciers, ni auprès de courtiers en données. Aucune adresse électronique de personne démarchée n'est collectée à aucun stade.

c. Nature et finalité des opérations

Collecte, hébergement et transmission sécurisée au Responsable de traitement des éléments de qualification précontractuelle du projet immobilier, **sans traitement algorithmique de valorisation**.

Ces données déclaratives ne peuvent être enregistrées qu'en présence d'un consentement en cours de validité, et sont effacées dès son retrait : le droit d'appeler disparaissant, leur conservation serait sans base légale.

- **Sélection** des logements du secteur à partir de la base publique des diagnostics, déduplication par adresse, exclusion des adresses opposées.
- **Production et expédition** des documents d'information, portant les mentions professionnelles obligatoires du Responsable du traitement.
- **Hébergement de la page de recueil** de l'accord de recontact, et enregistrement de la preuve associée.
- **Tenue de la liste d'exclusion** alimentée par le formulaire d'opposition, et application de cette liste avant chaque expédition.
- **Restitution** au Responsable du traitement des accords recueillis et des oppositions reçues, et transmission le cas échéant vers l'outil de gestion qu'il désigne.

Le Sous-traitant ne poursuit aucune finalité propre sur ces données. Il ne les cède pas, ne les revend pas, ne les mutualise pas entre Responsables du traitement — sous la seule réserve de la liste d'exclusion, dont la centralisation est expressément instruite par le Responsable du traitement au contrat.

d. Durée du traitement

Durée générale	Durée de l'abonnement du Responsable du traitement, puis restitution ou suppression selon son instruction.
Logement sans réponse	Douze mois au maximum après le dernier contact.
Accord de recontact	Un an, sans reconduction tacite (décret n° 2026-662).

Preuve de l'accord	Trois ans, à fin probatoire.
Chez le prestataire postal	Quinze jours après impression pour le contenu du pli et l'adresse du destinataire — instruction transmise à chaque envoi et conservée avec celui-ci.
Opposition	Conservée sans limitation de durée : l'effacer reviendrait à rendre possible un nouvel envoi vers une personne qui l'a refusé.

Annexe III – Mesures techniques et organisationnelles (art. 32)

Chacune de ces mesures est en place à la date du présent document et a été vérifiée dans le code source.

MESURE	MISE EN ŒUVRE
Cloisonnement entre Responsables du traitement	Isolation appliquée dans la base de données elle-même (<i>Row Level Security PostgreSQL</i>), et non dans l'interface : un conseiller ne peut pas lire les données d'un autre, même en contournant l'application.
Chiffrement des identifiants confiés	Les clés d'API du compte postal de chaque conseiller sont chiffrées en AES-256-GCM avant stockage, avec clé secrète tenue hors base. Elles ne sont jamais réaffichées : seuls les quatre derniers caractères sont restitués.
Protection des secrets	Clés et jetons en variables d'environnement, jamais inscrits dans le code, jamais journalisés, jamais exposés au navigateur. Les messages d'erreur ne restituent que le code de retour, jamais l'identifiant employé.
Chiffrement en transit	HTTPS sur l'ensemble des échanges. Authentification par jeton pour l'accès à la console.
Contrôle des destinations sortantes	La transmission vers l'outil de gestion d'un conseiller refuse les adresses non chiffrées, les adresses internes et les adresses de métadonnées d'infrastructure. Le contrôle s'applique à l'enregistrement <i>et</i> avant chaque transmission.
Refus d'agir en cas de doute	Aucun courrier n'est expédié si la liste des oppositions ne peut pas être lue, si la fiche du conseiller est incomplète, si les mentions professionnelles obligatoires manquent, ou si le test de mise en balance n'a pas été validé. Un envoi retardé se rattrape ; un pli déposé ne se rappelle pas.
Journalisation	Registre horodaté des consultations, des accords et des oppositions, avec adresse IP et libellé exact présenté à la personne au moment du recueil.
Minimisation chez le sous-traitant ultérieur	Instruction d'effacement à quinze jours transmise avec chaque courrier, et conservée avec l'envoi — l'instruction et sa date sont produites pour un pli donné, sans avoir à invoquer le code source.
Assistance au Responsable du traitement	Export du registre des consentements à tout moment ; traitement immédiat des demandes d'opposition ; restitution des données sur demande.
Notification des violations	Délai contractuel de 24 à 48 heures à compter de la connaissance d'une violation, stipulé à l'article 4 du contrat au titre de l'article 33.2 du RGPD. La notification est adressée par voie électronique au Responsable du traitement, à l'adresse figurant sur sa fiche.

Ce qui reste à établir

Le délai de notification est désormais fixé au contrat. **La procédure qui permet de le tenir, elle, n'existe pas encore.** Un délai contractuel ne crée pas la capacité de le respecter : encore faut-il savoir qu'une violation a eu lieu.

Trois points restent ouverts — par quel moyen une violation est détectée ; qui, chez le Sous-traitant, est joignable et sous quel délai ; et la tenue du registre interne des violations, que l'article 33.5 impose **indépendamment de toute notification**. À traiter avant la mise en service, faute de quoi l'engagement des 24 à 48 heures serait tenu par chance plutôt que par organisation.

Annexe IV – Sous-traitants ultérieurs

Le Responsable du traitement autorise les sous-traitants ultérieurs suivants. Toute modification de cette liste lui est notifiée préalablement, conformément à l'article 28.2.

PRESTATAIRE	RÔLE	DONNÉES CONFIIÉES
Supabase	Base de données et authentification	Ensemble des données du traitement
Netlify	Hébergement du site et des fonctions serveur	Données en transit ; journaux techniques
Merci Facteur	Impression et dépôt postal	Adresse du destinataire et contenu du pli, effacés à J+15
La Poste	Distribution, via Merci Facteur	Adresse du destinataire
Brevo	Envoi des messages électroniques	Adresse électronique et contenu — professionnels uniquement , jamais les personnes démarchées
OVH	Envoi des SMS	Numéro de téléphone et contenu du message
Make	Automatisations et journal de suivi	Données de capture et d'opposition

Aucun transfert hors Union européenne n'est prévu. Stripe intervient pour l'abonnement du conseiller à la plateforme : ce traitement ne porte pas sur les personnes démarchées et relève de la relation commerciale, non du présent accord.

Le Responsable du traitement

Nom, date et signature

Le Sous-traitant

Nom, date et signature

Références : règlement (UE) 2016/679, articles 5, 28, 32 et 33 · Décision d'exécution (UE) 2021/915 du 4 juin 2021 · loi n° 78-17 du 6 janvier 1978 modifiée · loi n° 70-9 du 2 janvier 1970 · décret n° 2026-662 · Licence Ouverte 2.0 (Etalab).