

Conditions particulières – SpamNo

Conditions Particulières – version 2.0 – en vigueur depuis le 17/09/2026

Les présentes conditions particulières complètent les **conditions générales de vente et d'utilisation – Services de GROUPE SOCIATEX**, dont elles font partie intégrante. Elles ne régissent que ce qui est propre au Service SpamNo.

Tout ce qui est commun à l'ensemble des Services – durée, reconduction, préavis, résiliation, défaut de paiement, révision des prix, ajout et retrait d'unités facturées, responsabilité, protection des données à caractère personnel – relève des conditions générales et n'est pas repris ici.

Les termes employés avec une majuscule ont le sens que leur donne l'article 1 des conditions générales, sauf définition contraire à l'article 1 ci-après.

Article 1 – Définitions propres au Service

SpamNo : le service de filtrage des messages électroniques entrants édité et exploité par le Prestataire, interposé entre les serveurs émetteurs et le serveur de messagerie du CLIENT.

Domaine Protégé : tout nom de domaine dont les enregistrements MX pointent vers SpamNo et pour lequel un traitement a été configuré.

Boîte Protégée : toute adresse de destinataire distincte ayant reçu au moins un message relayé par SpamNo au cours de la période de facturation. La Boîte Protégée constitue l'**Unité Facturée** du Service au sens de l'article 1 des conditions générales. Les modalités de décompte figurent à l'article 14.

Tenant : l'espace de configuration propre au CLIENT au sein de SpamNo, regroupant ses Domaines Protégés, ses règles et sa Quarantaine.

Quarantaine : l'espace de stockage chiffré dans lequel sont conservés les messages classés comme douteux, accessible au CLIENT depuis l'interface d'administration.

Message de défi : le message adressé automatiquement à un expéditeur inconnu par la fonction Challenge-Response décrite à l'article 7.

Plan : le niveau de service souscrit par le CLIENT parmi les trois niveaux suivants : ESSENTIEL, PRO et ENTREPRISE.

Les engagements propres à chaque Plan figurent à l'Annexe 1.

Prise en charge : l'opération définie à l'article 9.1. Elle ne se confond pas avec la résolution.

Les **Heures Ouvrées**, le **Ticket** et l'**Espace Client** ont le sens que leur donne l'article 1 des conditions générales. Tout délai exprimé en heures s'entend en Heures Ouvrées, soit du lundi au vendredi de 9h00 à 18h00, hors jours fériés.

Article 2 – Description du Service

2.1 Socle commun à tous les Plans

Quel que soit le Plan souscrit, le Service comprend :

- la réception des messages adressés aux Domaines Protégés et leur analyse avant relais ;
- le contrôle des mécanismes d'authentification de l'expéditeur (SPF, DKIM, DMARC), la consultation de listes de réputation et l'application de règles de scoring ;
- l'analyse antivirus des pièces jointes dans les conditions de l'article 4.4 ;
- le relais vers le serveur de destination des messages classés comme légitimes ;
- la mise en Quarantaine des messages classés comme douteux, dans les conditions de l'article 5 ;
- un rapport de Quarantaine adressé périodiquement aux utilisateurs ;
- la vérification automatique des enregistrements DNS des Domaines Protégés, dans les conditions de l'article 3.4 ;
- l'accès à l'interface d'administration et au support dans les conditions de l'article 9.

2.2 Engagements propres à chaque Plan

Ce qui varie d'un Plan à l'autre — nombre de Domaines Protégés, fonctions disponibles, délais de prise en charge et engagement de disponibilité — est défini par le **tableau des engagements** figurant à l'Annexe 1, qui fait partie intégrante des présentes et prévaut sur toute description commerciale.

2.3 Ce que le Service n'est pas

SpamNo est un service de filtrage et de relais. Il ne constitue ni un **service d'hébergement de messagerie**, ni un **service de sauvegarde**, ni un **service d'archivage légal**, sous réserve de l'option d'archivage visée à l'article 16.3. Il ne se substitue pas au serveur de messagerie du CLIENT, qui demeure seul dépositaire des messages délivrés.

Article 3 – Mise en service et migration

3.1 Création du Tenant

À réception de l'ordre de service, le Prestataire crée le Tenant du CLIENT et configure les serveurs de destination vers lesquels les messages seront relayés.

3.2 Bascule des enregistrements MX

La modification des enregistrements MX relève du CLIENT, qui en conserve la maîtrise. Le Prestataire l'accompagne dans cette opération et lui communique les valeurs à renseigner. La bascule ne produit effet qu'après propagation dans le système de noms de domaine, dont le délai dépend de la configuration du CLIENT et de son bureau d'enregistrement, et échappe au Prestataire.

3.3 Délai de mise en service

Le délai de mise en service est indicatif. Il est usuellement compris entre quinze et trente minutes à compter de la réception de l'ordre de service, hors propagation DNS. Aucun engagement ferme de délai n'est souscrit, sauf stipulation expresse du Devis.

3.4 Vérification automatique des enregistrements

SpamNo contrôle quotidiennement les enregistrements MX et SPF des Domaines Protégés et alerte le CLIENT en cas d'anomalie ou de chute inhabituelle du volume reçu.

Ce dispositif est automatisé. Il n'emporte aucune obligation de veille humaine ni d'intervention du Prestataire : l'alerte est une information adressée au CLIENT, à qui il appartient d'en tirer les conséquences. Une intervention du Prestataire peut être demandée par Ticket et relève, selon son objet, du support ou d'une prestation hors forfait.

3.5 Réversibilité de la bascule

Le CLIENT peut à tout moment rétablir ses enregistrements MX d'origine. Cette opération suffit à interrompre l'acheminement par SpamNo ; elle ne vaut pas résiliation du Contrat, laquelle obéit à l'article 14 des conditions générales.

Article 4 – Acheminement et traitement des messages

4.1 Traitement appliqué

Chaque message reçu fait l'objet d'une analyse à l'issue de laquelle il est relayé, placé en Quarantaine ou rejeté. Le rejet intervient au niveau du protocole : le serveur émetteur en est informé et il lui appartient d'en aviser son expéditeur.

4.2 Indisponibilité du Service et sort des messages

En cas d'indisponibilité temporaire du Service, les serveurs émetteurs conformes à la norme SMTP conservent le message et le retransmettent automatiquement, selon leur propre politique de réessai.

Ce mécanisme relève du protocole de messagerie et non du Service. Il réduit fortement le risque de perte sans l'éliminer : le Prestataire ne maîtrise ni la configuration ni le comportement des serveurs émetteurs tiers, et ne garantit pas l'acheminement d'un message émis par un serveur non conforme à la norme ou dont la politique de réessai est insuffisante.

4.3 Absence de garantie de performance du filtrage

Aucun filtrage n'est exempt d'erreur. Un message légitime peut être classé comme indésirable, et un message indésirable peut être délivré. Le Prestataire ne garantit aucun taux de filtrage, aucun taux de faux positifs et aucun taux de faux négatifs.

Le CLIENT dispose, pour corriger ces erreurs, de la consultation de la Quarantaine (article 5), des listes personnelles d'autorisation et de blocage, et de la fonction de signalement décrite à l'article 4.5.

4.4 Analyse antivirale

Les pièces jointes sont analysées avant toute autre opération. Un message porteur d'une pièce jointe identifiée comme dangereuse est rejeté.

Cette analyse repose sur des signatures et des méthodes de détection qui évoluent en permanence. Elle ne garantit pas la détection de toute menace, notamment lorsqu'elle est antérieure à la connaissance de sa signature, et peut conduire au rejet d'un fichier légitime. Le rejet d'un message pour ce motif n'ouvre droit à aucune indemnité.

4.5 Signalement et apprentissage

Le CLIENT peut signaler au Prestataire un message indésirable qui lui aurait été délivré, selon les modalités indiquées dans l'interface d'administration. Ce signalement alimente l'apprentissage du moteur de filtrage. Il n'emporte aucun engagement de résultat sur le classement des messages ultérieurs.

Article 5 – Quarantaine

5.1 Nature et accès

Les messages classés comme douteux sont conservés dans la Quarantaine, sous forme chiffrée. Le CLIENT et ses utilisateurs y accèdent depuis l'interface d'administration et peuvent consulter, délivrer ou supprimer les messages qui les concernent.

5.2 Durée de conservation

Les messages sont conservés en Quarantaine pendant trente (30) jours glissants à compter de leur réception. À l'expiration de ce délai, ils sont supprimés automatiquement et définitivement.

Il appartient au CLIENT de consulter sa Quarantaine dans ce délai. Un message légitime classé à tort et non délivré avant l'expiration du délai est définitivement perdu, le Prestataire n'en conservant aucune autre copie.

5.3 Sort de la Quarantaine à la fin du Service

La Quarantaine suit le régime de l'article 15 des conditions générales : les messages qu'elle contient sont conservés trente (30) jours à compter de la suspension ou de la date d'effet de la résiliation, puis supprimés définitivement.

Le CLIENT qui souhaite conserver des messages en Quarantaine les délivre vers son serveur de messagerie avant l'expiration de cette fenêtre.

Article 6 – Analyse par intelligence artificielle

6.1 Objet

Lorsque les autres signaux d'analyse n'ont pas permis de trancher, SpamNo peut soumettre le message à un modèle de langage afin d'en apprécier le sens et d'affiner le classement. Cette analyse complète le scoring multi-critères et ne s'y substitue pas.

6.2 Activation par le CLIENT

L'analyse par intelligence artificielle n'est pas activée par défaut. Elle est activée ou désactivée par le CLIENT, domaine par domaine, depuis l'interface d'administration, lors de la création d'un Domaine Protégé ou à tout moment

ensuite.

L'activation intervient après affichage, dans l'interface, des données transmises et de l'identité du sous-traitant qui les traite. Le choix du CLIENT est horodaté et conservé.

6.3 Données transmises

Seuls sont transmis l'adresse de l'expéditeur, l'objet du message et un extrait de son corps limité à environ six cents (600) mots. Les pièces jointes ne sont jamais transmises.

6.4 Sous-traitant ultérieur

L'analyse est opérée par Mistral AI, société anonyme de droit français immatriculée au registre du commerce et des sociétés de Paris sous le numéro 952 418 325. Elle figure comme sous-traitant ultérieur à l'annexe « Protection des données à caractère personnel ».

La localisation des traitements réalisés par ce sous-traitant est celle indiquée par lui, en Union Européenne.

6.5 Conditions d'exploitation de la fonction

Le contrat-cadre de ce sous-traitant prévoit, à défaut d'option contraire exercée par son client, qu'il peut traiter les contenus transmis en qualité de responsable de traitement, aux fins d'entraînement de ses modèles. Un tel traitement excéderait les instructions du CLIENT et sortirait du cadre de l'article 28 du règlement (UE) 2016/679.

Le Prestataire a exercé les options contraires. À la date d'entrée en vigueur des présentes, les trois paramètres suivants sont actifs sur son compte auprès de ce sous-traitant :

- l'utilisation des appels d'interface de programmation pour l'entraînement des modèles est désactivée ;
- la rétention zéro est activée : les données de dépannage et d'analyse ne sont pas conservées ;
- les modèles dits « Labs » ne sont pas activés, leur activation emportant par elle-même acceptation de l'entraînement sur les données transmises, quels que soient les autres paramètres.

Le Prestataire s'oblige à maintenir ces trois paramètres pendant toute la durée du Contrat et en justifie sur simple demande du CLIENT. En cas de modification de l'un d'eux, il en informe le CLIENT sans délai et suspend la fonction jusqu'à son rétablissement.

Article 7 – Challenge-Response

7.1 Objet et activation

La fonction Challenge-Response adresse automatiquement un Message de défi à tout expéditeur inconnu. L'expéditeur qui y répond est ajouté à la liste d'autorisation du destinataire.

Cette fonction est désactivée par défaut. Elle est activable par le CLIENT depuis l'interface d'administration, pour les Plans le prévoyant à l'Annexe 1.

7.2 Garde-fous appliqués par le Prestataire

Lorsque la fonction est activée, le Prestataire applique les limitations suivantes, que le CLIENT ne peut désactiver :

- un seul Message de défi est adressé par expéditeur, sans relance ;
- aucun Message de défi n'est adressé à une liste de diffusion, à une adresse de service, à une adresse de non-réponse ni à un message automatique identifié comme tel ;
- le nombre de Messages de défi émis est limité par période, afin de préserver la réputation d'émission de l'infrastructure ;
- les demandes restées sans réponse sont purgées automatiquement.

7.3 Responsabilité du CLIENT

Le CLIENT qui active la fonction en assume l'usage. Il lui appartient d'apprécier l'opportunité d'adresser des messages automatiques à ses correspondants et d'en informer ceux-ci s'il l'estime nécessaire.

Le Prestataire peut suspendre la fonction sur un Domaine Protégé, après information du CLIENT, lorsque son usage compromet la réputation d'émission de l'infrastructure ou la délivrabilité des autres clients.

Article 8 – Simulation de phishing

Fonction réservée au Plan ENTREPRISE.

8.1 Nature de la fonction

La fonction permet au CLIENT de créer et de diffuser lui-même, depuis l'interface d'administration, des campagnes de messages simulant une tentative d'hameçonnage à destination de ses propres utilisateurs, et d'en suivre les résultats.

Le Prestataire fournit l'outil ; le CLIENT en est l'opérateur. Le Prestataire ne crée, ne déclenche ni ne paramètre aucune campagne de sa propre initiative.

8.2 Validation préalable par le CLIENT

Aucune campagne ne peut être diffusée sans que le CLIENT ait coché, dans l'interface, la case de validation prévue à cet effet. Cette validation est horodatée et conservée.

En cochant cette case, le CLIENT déclare :

- avoir informé les personnes concernées de l'existence du dispositif, selon les modalités qu'il a retenues ;
- avoir procédé, lorsqu'il y est tenu, à l'information et à la consultation de ses instances représentatives du personnel ;
- avoir déterminé la base légale du traitement et l'avoir inscrit à son registre ;
- avoir défini la durée de conservation des résultats et les personnes habilitées à y accéder.

8.3 Résultats

Les résultats des campagnes sont accessibles au CLIENT dans son Tenant. **Le CLIENT est responsable de traitement de ces données**, qui portent sur le comportement de ses utilisateurs.

Il lui appartient d'en définir l'usage et d'en restreindre l'accès. Le Prestataire recommande une exploitation agrégée, à des fins de mesure collective et de formation, et appelle l'attention du CLIENT sur les conséquences, au regard du droit du travail, d'une exploitation individuelle des résultats.

Point à faire préciser par l'avocat : l'articulation entre la mesure de la vigilance individuelle et les règles encadrant le contrôle de l'activité des salariés.

8.4 Limites

Le Prestataire n'exerce aucun contrôle sur le contenu des campagnes créées par le CLIENT. Il peut suspendre la fonction, après information du CLIENT, lorsque son usage compromet la réputation d'émission de l'infrastructure.

Article 9 – Support

9.1 Définition de la prise en charge

La prise en charge consiste à qualifier la demande, à en apprécier la nature et à informer le CLIENT de la suite qui lui est donnée, dans le délai indiqué à l'Annexe 1. Elle n'emporte aucun engagement de résolution dans ce délai.

9.2 Condition de déclenchement des délais

Les délais de prise en charge ne s'appliquent qu'aux demandes enregistrées sous forme de Ticket au moyen de la plateforme de ticketing accessible depuis l'Espace Client. Les sollicitations reçues par un autre canal ne déclenchent aucun délai tant qu'elles n'ont pas été enregistrées sous forme de Ticket.

9.3 Suspension des délais

Conformément à l'article 10 des conditions générales, les délais sont suspendus tant que le CLIENT n'a pas fourni les informations ou les accès nécessaires au traitement.

Article 10 – Engagement de disponibilité

Engagement réservé au Plan ENTREPRISE.

10.1 Objet de l'engagement

Le Prestataire s'engage sur un taux de disponibilité mensuel du service de relais de 99,9 %, mesuré par mois calendaire.

La disponibilité s'entend de la capacité du Service à accepter les messages entrants adressés aux Domaines Protégés. La mesure est effectuée par les outils de supervision du Prestataire, dont les relevés font foi jusqu'à preuve contraire conformément à l'article 23.1 des conditions générales.

10.2 Exclusions

Ne sont pas décomptées comme indisponibilité :

- les opérations de maintenance planifiée, annoncées au CLIENT au moins 48 heures à l'avance et réalisées en dehors des Heures Ouvrées ;
- les interruptions imputables aux enregistrements DNS du CLIENT, à son serveur de messagerie de destination ou à son infrastructure ;
- les interruptions résultant d'une configuration erronée effectuée par le CLIENT ou par l'un de ses administrateurs

délégués ;

- les cas de force majeure au sens de l'article 13 des conditions générales ;
- les interruptions consécutives à une suspension prononcée en application de l'article 7.3 ou de l'article 8.4.

10.3 Conséquence d'un manquement

Lorsque le taux constaté sur un mois est inférieur à l'engagement, le CLIENT peut demander un avoir, calculé proportionnellement à la durée de l'indisponibilité et plafonné à dix pour cent (10 %) du montant mensuel de l'abonnement du Domaine Protégé concerné.

La demande est adressée par Ticket dans les trente (30) jours suivant le mois considéré. L'avoir est imputé sur la facture suivante. Il constitue la seule indemnisation due au titre du manquement à l'engagement de disponibilité, sans préjudice des articles 11.3 et 11.4 des conditions générales.

Article 11 – Période d'essai

11.1 Durée et conditions

Le Service peut être souscrit à titre d'essai gratuit pour une durée de trente (30) jours à compter de la création du Tenant. Aucun moyen de paiement n'est demandé et aucun engagement n'est pris au titre de la période d'essai.

Pendant cette période, le Service est fourni dans les conditions du Plan choisi, à l'exception de l'engagement de disponibilité de l'article 10, qui ne s'applique pas.

11.2 Information du CLIENT avant le terme

Le Prestataire informe le CLIENT du terme prochain de la période d'essai quinze (15) jours puis trois (3) jours avant son expiration, par courrier électronique adressé à l'adresse renseignée à l'inscription.

11.3 Absence de reconduction automatique

La période d'essai ne se transforme pas en abonnement payant. À son terme, et à défaut de souscription expresse, le Service prend fin.

11.4 Relais de grâce

Afin d'éviter toute interruption du courrier du CLIENT qui n'aurait pas rétabli ses enregistrements MX à temps, le Prestataire maintient, pendant {{7}} jours suivant le terme de la période d'essai, l'acheminement des messages vers le serveur de destination du CLIENT, sans filtrage ni mise en Quarantaine.

Ce relais de grâce est une tolérance et non un service : il ne comporte aucun engagement de disponibilité, de performance ni de sécurité. À son terme, l'acheminement cesse définitivement.

11.5 Sort des données

Les données du Tenant d'essai, Quarantaine comprise, sont conservées **trente (30) jours** à compter du terme de la période d'essai, puis supprimées définitivement. Le CLIENT qui souscrit dans ce délai conserve son Tenant et sa configuration.

Article 12 – Exclusions

Sont expressément exclus du Service, quel que soit le Plan souscrit :

- tout engagement sur un taux de filtrage, de faux positifs ou de faux négatifs (article 4.3) ;
- toute garantie d'acheminement d'un message émis par un serveur non conforme à la norme SMTP (article 4.2) ;
- l'hébergement, la sauvegarde et l'archivage des messages délivrés, qui relèvent du serveur de messagerie du CLIENT, sous réserve de l'option d'archivage ;
- la restauration de messages supprimés de la Quarantaine à l'expiration du délai de conservation ;
- la modification des enregistrements DNS du CLIENT, qui en conserve la maîtrise (article 3.2) ;
- l'intervention humaine consécutive à une alerte de vérification DNS (article 3.4) ;
- le filtrage des messages sortants émis par le CLIENT ;
- la création et le paramétrage des campagnes de simulation de phishing, qui relèvent du CLIENT (article 8.1) ;
- les interventions sur l'infrastructure de messagerie du CLIENT, qui font l'objet d'un devis préalable.

Article 13 – Avertissement et obligations du CLIENT

13.1 Limites des solutions de filtrage

Aucune solution de filtrage ne garantit une protection absolue. Les techniques d'hameçonnage et d'usurpation évoluent en permanence et certaines échappent à la détection. Un message frauduleux peut être délivré ; un message légitime peut être retenu.

Le Prestataire attire expressément l'attention du CLIENT sur ce point, avant la souscription et indépendamment de tout incident. La souscription du Service ne dispense pas le CLIENT de sensibiliser ses utilisateurs, ni des mesures d'hygiène informatique relevant de sa responsabilité.

13.2 Obligations du CLIENT

Outre les obligations de l'article 10 des conditions générales, le CLIENT s'engage à :

- maintenir ses enregistrements DNS cohérents avec la configuration du Service et signaler toute modification envisagée ;
- n'accepter sur son serveur de destination que les connexions provenant de l'infrastructure du Prestataire, afin que le filtrage ne puisse être contourné ;
- consulter sa Quarantaine dans le délai de conservation de l'article 5.2 ;
- tenir à jour la liste de ses administrateurs et de ses administrateurs délégués par domaine, et répondre de leurs actes de configuration ;
- ne pas utiliser le Service pour recevoir des messages destinés à des tiers sans y être habilité ;
- informer ses utilisateurs de l'existence du filtrage et, le cas échéant, de l'analyse prévue à l'article 6.

Les actes de configuration accomplis par un administrateur délégué du CLIENT engagent celui-ci, y compris lorsqu'ils conduisent à autoriser un expéditeur ou à désactiver une protection.

Article 14 – Unité Facturée et variations

14.1 Décompte des Boîtes Protégées

Est comptabilisée comme Boîte Protégée toute adresse de destinataire distincte ayant reçu au moins un message relayé par SpamNo au cours de la période de facturation, quel que soit le nombre de messages reçus.

Le décompte porte sur les adresses telles qu'elles apparaissent au destinataire, sans distinction selon qu'il s'agit d'une boîte nominative, d'un alias, d'une adresse de service ou d'une liste de diffusion.

Vérifiabilité du décompte. Le CLIENT accède à tout moment, depuis l'interface d'administration, à la liste des adresses comptabilisées sur la période en cours et sur les périodes écoulées. Cette liste est jointe à la facture.

Le CLIENT qui souhaite réduire son décompte peut supprimer les alias et adresses de service inutilisés, ou en restreindre la réception, avant le terme de la période.

14.2 Ajout et retrait

Les variations du nombre de Boîtes Protégées obéissent à l'article 9 des conditions générales : facturation au prorata temporis à l'ajout, avoir imputé au renouvellement au retrait, seuil de déclenchement de dix euros hors taxes cumulés sur la période, et fait générateur constitué par la cessation effective du Service telle que constatée par les outils de supervision.

14.3 Domaines Protégés

Le nombre de Domaines Protégés autorisés dépend du Plan souscrit, dans les conditions de l'Annexe 1. L'ajout d'un Domaine Protégé au-delà du nombre autorisé emporte changement de Plan.

Article 15 – Sort des données

Les données traitées dans le cadre du Service – messages en Quarantaine, journaux de transport, configuration du Tenant, statistiques – sont conservées **rente (30) jours** à compter de la suspension ou de la date d'effet de la résiliation, conformément à l'article 15 des conditions générales. À l'expiration de ce délai, leur suppression est définitive.

Effet de la fin du Service sur l'acheminement. À la date d'effet, le Service cesse d'accepter les messages adressés aux Domaines Protégés. Il appartient au CLIENT d'avoir rétabli ses enregistrements MX avant cette date. À défaut, les messages qui lui sont adressés ne lui parviendront pas, sans que le Prestataire puisse en être tenu responsable.

Le Prestataire rappelle cette obligation au CLIENT lors de la confirmation de la résiliation prévue à l'article 14.1 des conditions générales.

Article 16 – Facturation, prix et options

16.1 Unité de facturation et détermination du prix

Le Service est facturé par Boîte Protégée, selon la périodicité choisie au Devis. Le prix applicable est celui figurant au Devis accepté par le CLIENT, lequel prévaut conformément à l'article 2.3 des conditions générales. Toute souscription fait l'objet d'un Devis préalable.

16.2 Grille tarifaire

Les prix unitaires en vigueur, la dégressivité applicable au Plan PRO et les frais de mise en service figurent à la grille tarifaire SpamNo, document daté et versionné communiqué au CLIENT avant la souscription et annexé au Devis. Conformément à l'article L441-1 du code de commerce, cette grille est communiquée sur support durable à tout acheteur professionnel qui en fait la demande.

La mise à jour de la grille est sans effet sur les prix des contrats en cours, lesquels ne varient que dans les conditions de l'article 8 des conditions générales.

16.3 Options du Plan ENTREPRISE

Instance dédiée. Le Service est alors exploité sur une infrastructure réservée au CLIENT. Le périmètre, les conséquences sur l'engagement de disponibilité et le prix sont définis au Devis.

Archivage. Les messages relayés sont conservés pendant une durée définie au Devis, à des fins de recherche et de restitution.

16.4 Prestations hors forfait

Les prestations exclues à l'article 12 et les interventions réalisées à la demande du CLIENT sont facturées au temps passé ou sur devis préalable.

Article 17 – Articulation avec les conditions générales

Les présentes conditions particulières ne traitent que de ce qui est propre au Service SpamNo. Relèvent des conditions générales, auxquelles il convient de se reporter :

Objet	Article des conditions générales
Durée, reconduction, préavis et information de non-reconduction	Article 6

Prix, facturation, paiement, mise en demeure et suspension	Article 7
Révision des prix	Article 8
Ajout et retrait d'Unités Facturées	Article 9
Obligations générales du CLIENT	Article 10
Responsabilité et limites des solutions de sécurité	Article 11
Résiliation	Article 14
Sort des données et réversibilité	Article 15
Protection des données à caractère personnel	Article 16 et annexe RGPD
Convention de preuve	Article 23.1
Réclamations et médiation de la consommation	Article 22

En cas de contradiction, l'ordre de priorité de l'article 2.3 des conditions générales s'applique, sous les trois réserves qu'il énonce.

Annexe 1 – Tableau des engagements par Plan

La présente annexe fait partie intégrante des conditions particulières SpamNo et prévaut sur toute description commerciale. Toutes les durées s'entendent en Heures Ouvrées, du lundi au vendredi de 9h00 à 18h00, hors jours fériés.

Engagement	ESSENTIEL	PRO	ENTREPRISE
Domaines Protégés	1	Illimités	Illimités
Boîtes Protégées	Jusqu'à 10	Illimitées	Illimitées
Filtrage antispam et contrôle SPF, DKIM, DMARC	Identique sur les trois Plans		
Analyse antivirus des pièces jointes	Identique sur les trois Plans		
Quarantaine chiffrée – conservation 30 jours glissants	Identique sur les trois Plans		
Listes personnelles d'autorisation et de blocage	Identique sur les trois Plans		
Rapport de Quarantaine aux utilisateurs	Quotidien – identique sur les trois Plans		
Vérification automatique des enregistrements DNS	Identique sur les trois Plans – sans veille humaine		
Authentification à deux facteurs	Identique sur les trois Plans		
Analyse par intelligence artificielle	Disponible sur les trois Plans – activée par le CLIENT, domaine par domaine		
Rapports d'administration mensuels	Non inclus	Inclus	Inclus

Délégation par domaine (administrateur local)	Non inclus	Inclus	Inclus
Challenge-Response	Non disponible	Activable par le CLIENT	Activable par le CLIENT
API REST	Non inclus	Non inclus	Inclus
Règles de filtrage sur mesure	Non inclus	Non inclus	Inclus
Simulation de phishing	Non inclus	Non inclus	Inclus — opérée par le CLIENT
Prise en charge d'un Ticket	1 jour ouvré	4 h	4 h
Engagement de disponibilité	Aucun	Aucun	99,9 % — avoir plafonné à 10 % du mois
Instance dédiée	Non disponible	Non disponible	En option
Archivage	Non disponible	Non disponible	En option
Période d'essai	30 jours, sans engagement et sans moyen de paiement — hors engagement de disponibilité		

Rappel : la prise en charge consiste à qualifier la demande et à informer le CLIENT de la suite donnée. Elle n'emporte aucun engagement de résolution dans le délai indiqué (article 9.1).

Rappel : aucun taux de filtrage, de faux positifs ou de faux négatifs n'est garanti (article 4.3).