Charte déontologique des membres de l'association Signal Spam

Les membres de Signal-Spam couvrent une variété de métiers contribuant à la création, à l'acheminement ou à la sécurité de messages électroniques. Sauf lorsque cela est précisé spécifiquement, la présente charte s'applique à toutes les formes de communication par ce biais, qu'il s'agisse de prospection à caractère commercial ou pour toute autre raison. Cette charte s'applique aussi à toutes les personnes qui souhaitent y adhérer volontairement, en particulier les personnes destinataires de boucles de rétroaction via des contrats-cadres mis en place avec les organisations membres de Signal Spam.

Les membres de l'association s'engagent à mettre en œuvre les termes de la présente charte dans un délai de 6 mois à compter de leur adoption.

La finalisation de l'adhésion de nouveaux membres est soumise à l'application de la présente charte.

Toute nouvelle mise en place de boucle de rétroaction ou signature volontaire de la charte suppose la mise en œuvre préalable des termes de la charte.

Chapitre 1 – Principes communs

Les membres de Signal-Spam s'engagent:

Article 1.1 – Lutte contre les courriers électroniques non-sollicités

à contribuer à la lutte contre les courriers électroniques non-sollicités et plus généralement aux objectifs de l'association, par une participation active aux activités de l'association, et en particulier aux assemblées générales et aux échanges électroniques.

Article 1.2 – Relations entre les membres

à recevoir toute sollicitation d'un membre de l'association avec bienveillance et à s'efforcer de lui apporter une réponse rapide et efficace.

Article 1.3 – Neutralité de l'association Signal-Spam

à préserver en toutes circonstances la neutralité de l'association. En particulier, les conflits entre les membres à l'extérieur de l'association ne doivent jamais nuire à son fonctionnement.

Article 1.4 – Obligation de conseil

à se conduire en professionnel responsable et notamment à fournir à chacun de ses clients toutes les informations et les conseils utiles pour garantir un traitement des courriers électroniques efficace, conforme à la législation et aux règles déontologiques de l'association.

Article 1.5 – Respecter un haut niveau de protection des données

à respecter un haut niveau de protection des données personnelles issu des dispositions de la loi du 6 janvier 1978 modifiée, de son décret d'application du 20 octobre 2005 modifié en 2007 et des délibérations de la Commission nationale informatique et libertés ;

Article 1.6 – Diffusion et mise en œuvre de la charte

Tout membre de l'association jouant un rôle dans l'émission ou l'acheminement des courriers électroniques fait connaître la présente charte auprès de ses salariés et prestataires. Il tient aussi à disposition du public un document mettant en lumière les engagements contenus dans la charte et la façon dont il les applique.

Les membres de l'association, les signataires de la présente charte ou les destinataires d'une boucle de rétroaction peuvent cumuler différents métiers parmi ceux qui sont couverts dans les chapitres ci-après. Dans ce cas-là, ils s'engagent à respecter l'ensemble des engagements qui les concernent.

Article 1.7 – Applicabilité de la charte aux membres des organisations

La charte de Signal Spam doit constituer un horizon de convergence pour les textes, engagements, et recommandations des organisations membres.

La charte déontologique de Signal Spam ne s'impose pas directement aux membres individuels des organisations qui composent l'association Signal Spam. Tout membre d'une organisation faisant partie de Signal-Spam peut choisir de signer individuellement la présente charte.

Et, en tout état de cause, tout membre d'une organisation qui bénéficie d'un service Signal Spam sans en être directement membre via un accord-cadre avec son organisation, plus particulièrement une boucle de rétroaction, doit souscrire à la charte de déontologie de Signal Spam.

Chapitre 2 – Applications techniques

Article 2.1 – Format des courriers électroniques

Les dispositions du présent article s'appliquent à tout envoi de mail automatisé.

Ces dispositions concernent donc de façon non exhaustive aussi bien les courriers électroniques à caractère commercial ou émis par des associations caritatives, politiques ou tout autre envoi réalisé de façon automatisée.

Les règles suivantes sont appliquées par les membres de l'association aux courriers électroniques qu'ils traitent, chacun en fonction de son rôle dans la construction des messages :

- Aucun élément de l'en-tête technique ou du corps du message ne doivent tromper son destinataire sur l'origine ou l'objet du message;
- Le corps du message est dans un format respectueux des standards en vigueur et d'une taille totale (texte, pièces jointes et contenus distants éventuels) raisonnable;
- Le corps du message ne contient pas de logiciels malveillants ou susceptibles de réaliser des opérations à l'insu des systèmes destinés à recevoir le message;
- L'objet du message informe son destinataire de façon claire et transparente du contenu et de l'objectif du message;
- Le champ technique réservé à l'émetteur du message contient une adresse de courrier électronique dont le nom de domaine correspond soit à l'émetteur réel, soit à un prestataire intervenant dans le routage du message, et un nom d'affichage informant clairement le destinataire sur l'émetteur du message;

- Le corps du message contient, dans un format garantissant son affichage clair en toutes circonstances, la raison sociale (ou bien la marque ou la dénomination sociale susceptible d'être connue de la personne destinataire des courriels) de l'émetteur du message et un lien vers une procédure d'information et de désinscription;
- En outre, l'en-tête d'un message de prospection commerciale contient un champ normalisé de type "List-unsubscribe" (conformément à la RFC 2369).

Article 2.2 – Procédures de désinscription

Les procédures de désinscription accessibles depuis chaque courrier électronique reçu doivent permettre aux personnes qui y aboutissent:

- de les utiliser pendant au moins 30 jours après l'émission du message;
- d'être informées sur l'annonceur ou le prestataire technique concerné;
- de voir immédiatement quelle est l'adresse de courrier électronique sur laquelle elles ont été contactées;
- d'être désinscrites de façon sélective de toute future campagne de l'annonceur ou du prestataire concerné;
- lorsque c'est une option gérée par le prestataire de pouvoir éventuellement accéder facilement à la sélection des sujets sur lesquels elles souhaitent être contactées à l'avenir;
- dans la mesure du possible, d'être informées par tout moyen approprié si la procédure de désinscription n'a pas pu aboutir pour une raison légitime.

Article 2.3 – Détection des adresses invalides

Les membres de l'association mettent en place des procédures permettant de détecter les adresses invalides, à la fois pour améliorer la qualité des données à caractère personnel qu'ils traitent et diminuer l'impact de courriers mal adressés sur les réseaux destinataires.

Article 2.4 – Procédures de gestion des abus

Les membres de l'association qui gèrent un domaine (un domaine de deuxième niveau du système de gestion de noms de domaine) ou un réseau (ensemble d'adresses IP) jouant un rôle dans l'acheminement d'un courrier électronique, ou pouvant jouer un tel rôle, administrent effectivement les interfaces de traitement des abus prévus par les standards en vigueur (en particulier l'adresse "abuse" de la spécification RFC 2142 pour le domaine de deuxième niveau).

Les services suivants doivent être offerts sur l'interface de traitement des abus:

- La réception et le traitement des messages au format "Abuse reporting format" (RFC 5965);
- Une prise en compte au moins quotidienne, les jours ouvrables;

Des processus complémentaires peuvent être mis en œuvre – notamment pour garantir des échanges avec des partenaires privilégiés – mais ils ne remplacent pas les dispositions minimales décrites ci-dessus.

Les membres de l'association concernés par cet engagement informent les autres membres de l'association sur l'ensemble des procédures de traitement des abus qu'ils ont mises en place.

Pour signaler un incident relevant de ces procédures d'abus à un autre membre de l'association, ils privilégient toujours les procédures évoquées ci-dessus, pour garantir un traitement efficace et fluide de ces informations.

Des procédures d'urgence peuvent être proposées entre membres de l'association. Les membres s'engagent à les utiliser dans les conditions fixées par le membre qui met en place une telle procédure d'urgence.

Des procédures d'information des usagers sur les mesures prises par les cellule de gestion des abus sont mises en place qui consistent au minimum à diffuser dans un format accessible au public l'information sur le moyen de contacter cette cellule et le type d'actions qu'elle entreprend. Cela peut aussi consister, selon les cas et en fonction des spécificités du prestataire concerné, à :

- Accuser réception des signalements d'abus reçus ;
- Mettre en place une interface de suivi des signalements ;
- Ou encore, à diffuser des statistiques d'activité de la cellule d'abus.

Article 2.5 – Configuration des serveurs de noms de domaine

Pour faciliter l'acheminement des courriers électroniques, les professionnels membres de Signal-Spam mettent en œuvre les technologies correspondant à l'état de l'art qui permettent de s'assurer de la légitimité des infrastructures qui émettent du courrier électronique et prennent en compte l'évolution des standards développés dans ce domaine.

Ainsi, l'implémentation des spécifications du "Sender policy framework" (SPF, RFC 4408) ainsi que la spécification "Domain Keys Identified Mail" (DKIM, RFC 4871) sont considérées, au moment de la rédaction de la présente charte, comme faisant partie de l'état de l'art et la recommandation DMARC "Domain-based Message Authentication, Reporting & Conformance" peut être considérée comme une piste intéressante pour leur application.

Article 2.6 – Cookies

Les membres de Signal-Spam échangent sur leurs bonnes pratiques en matière d'utilisation des cookies et, notamment, sur l'information des internautes sur les cookies.

Sur ce sujet, la loi informatique et libertés dispose dans son article 32 que :
« Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :

- *de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;*
- *des moyens dont il dispose pour s'y opposer.*

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle. Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

- *soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;*
- *soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.»*

Chapitre 3 – Personnes recevant des boucles de rétroaction

Article 3.1 – Sécurisation des traitements de données à caractère personnel

Les personnes recevant des boucles de rétroaction s'engagent à mettre en œuvre toutes les mesures conformes à l'état de l'art pour garantir la sécurité – et notamment la confidentialité – des données à caractère personnel qu'elles contiennent.

Article 3.2 – Traitement des signalements provenant de Signal-Spam

Le destinataire d'une boucle de rétroaction mise à sa disposition par l'association s'engage:

- A traiter promptement et efficacement les signalements ;
- A informer Signal-Spam de tout écart significatif par rapport à la typologie de signalement qu'il devrait recevoir, comme, par exemple, de signalements qui ne lui seraient manifestement pas destinés ;
- A échanger régulièrement avec Signal-Spam sur les actions entreprises avec les signalements qu'elle reçoit ;
- A respecter ses obligations découlant de la loi « informatique et libertés » (déclarer son traitement auprès de la CNIL ou l'inscrire sur son registre en cas de désignation d'un correspondant informatique et libertés, informer les personnes de leurs droits et de la finalité du traitement et définir des durées de conservation en fonction des finalités du traitement).

Chapitre 4 – Gestionnaires de listes

On entend par listes tous les traitements de données à caractère personnel contenant les coordonnées électroniques de personnes physiques.

Article 4.1 – Formalités préalables à la mise en œuvre des traitements

Le membre de Signal Spam qui souhaite utiliser une liste s'engage à effectuer des formalités préalables à la mise en œuvre de son traitement (déclaration du traitement auprès de la CNIL, inscription sur le registre en cas de désignation d'un correspondant informatique et libertés, demande d'autorisation pour les transferts de données hors Union-Européenne lorsque la loi l'exige).

Article 4.2 – L'information, le consentement et l'exercice du droit d'opposition

Au moment de la collecte de ses données, l'internaute concerné est informé:

- de l'identité du responsable du traitement ;
- des finalités poursuivies ;
- du caractère obligatoire ou facultatif des réponses à apporter ;
- des conséquences éventuelles, à leur égard, d'un défaut de réponse ;
- des destinataires des données ;
- et de ses droits d'accès, de rectification et d'opposition, pour des motifs légitimes, au traitement des données, sauf dans les cas où le traitement répond à une obligation légale, et, le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non membre de l'Union européenne.

En cas de transferts de données à caractère personnel envisagés à destination d'un État non membre de l'Union Européenne, les dispositions de l'article 91 du décret d'application du 20 octobre 2005 modifié s'appliquent : les personnes devront notamment être informées du ou des pays d'établissement du destinataire des données, de la nature des données transférées, de la finalité du transfert envisagé, de la ou des catégories de destinataires des données, du niveau de protection offert par le ou les pays tiers.

Au moment de la collecte des données, devra également être prévu :

- soit le recueil du consentement exprès et spécifique de la personne concernée, notamment dans les cas suivants :
  - la prospection au moyen d'un courrier électronique (adresse électronique, SMS ou MMS) hors produits ou services analogues ;
  - la cession à des partenaires d'adresses électroniques ; il est recommandé que lors de la sollicitation du consentement d'un consommateur pour l'envoi d'offres commerciales par voie électronique, tel que prévu par la loi, il soit dissocié le consentement à recevoir des offres de l'entreprise elle-même et le consentement à recevoir des offres émanant de partenaires de cette entreprise afin d'éviter toute confusion dans l'esprit du consommateur sur la portée de son consentement ;
  - la collecte ou la cession des données susceptibles de faire apparaître directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ou qui sont relatives à la vie sexuelle de celle-ci.
- soit une possibilité offerte de lui permettre de s'opposer de manière simple et dénuée d'ambiguïté, notamment dans les cas suivants :
  - la prospection au moyen d'un courrier électronique pour un produit ou service analogue dans les cas d'une relation client-entreprise préexistante ;
  - la prospection entre professionnels lorsque l'objet du message est en rapport avec l'activité du professionnel ;
  - la cession à des partenaires d'informations relatives à la situation familiale, économique et financière dès lors que les organismes destinataires s'engagent à ne les exploiter que pour s'adresser directement aux intéressés, pour des finalités exclusivement commerciales et que ces données.

Le consentement est une manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. Ainsi, l'acceptation des conditions générales d'utilisation n'est pas une modalité suffisante du recueil du consentement des personnes.

Dans le cas d'une collecte via un formulaire, le droit d'opposition ou le recueil du consentement préalable doit s'exprimer par un moyen simple et spécifique, présent sur le formulaire.

Par exemple, le formulaire pourra contenir une case à cocher ou un sélecteur, ou tout autre outil d'interface qui soit clair, lisible et accessible.

Lorsque la collecte des données intervient par voie orale, l'intéressé est mis en mesure d'exercer son droit d'opposition ou de donner son consentement avant la fin de la collecte de ses données.

Après la collecte des données :

- la personne concernée a le droit de s'opposer, sans frais, à ce que ses données soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur ;
- les messages adressés à des fins de prospection directe doivent mentionner des coordonnées valables permettant de demander à ne plus recevoir de telles sollicitations.

Article 4.3 Durées de conservation

Les gestionnaires de liste respectent les durées de conservation, nécessaires aux finalités pour lesquelles elles sont collectées et traitées, fixées par la déclaration de leurs traitements à la CNIL ou par l'inscription dans le registre en cas de désignation d'un correspondant informatique et libertés.

Article 4.4 – Qualité des données collectées

Les personnes gérant des listes s'assurent, conformément à la législation en vigueur, de la qualité des données collectées. En particulier, à chaque fois que c'est pertinent et possible, les professionnels concernés identifient de façon précise:

- la source des informations collectées (en particulier s'il s'agit de clients directs, de clients d'un partenaire ou de personnes qui ont accepté d'être prospectées par des tiers) ;
- à chaque fois que c'est pertinent, il est recommandé une catégorisation suffisamment précise des personnes inscrites.

Article 4.5 – Mises à jour en cascade

Les personnes gérant des listes mettent en place des procédures permettant une mise à jour en cascade des informations concernant une personne physique, c'est-à-dire:

- de retransmettre systématiquement, conformément à l'exercice du droit d'opposition prévu par les règlements, les demandes de désinscription vers les personnes à qui des listes de prospection ont été retransmises ;
- et de prendre en compte dans les plus brefs délais toute demande de mise à jour transmise par un gestionnaire de liste placé en amont.

Par ailleurs, les membres de Signal-Spam reconnaissent la nécessité de travailler sur les procédures permettant de faciliter l'exercice par les personnes physiques de leur droit d'opposition en amont auprès des personnes qui fournissent des listes.

Ces procédures de mise à jour en cascade sont facilitées par une plus grande qualité des données collectées, telle que décrite à l'article précédent.

Article 4.6 – Sécurité

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité des données à caractère personnel et, notamment, empêcher qu'elles soient déformées ou endommagées ou que des tiers non autorisés y aient accès.

En particulier, les accès aux traitements de données s'effectuent par un code d'accès et un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d'authentification.

Il faut noter que les moyens d'authentification biométriques sont soumis en France à l'autorisation préalable de la CNIL.

Dans le cas de l'utilisation d'un service de communication au public en ligne, le responsable de traitement prend les mesures nécessaires pour se prémunir contre tout accès non autorisé au système de traitement automatisé de données.

Chapitre 5 – Annonceurs

Article 5.1 – Gestion des listes

Lorsque les annonceurs membres de l'association gèrent eux-mêmes des listes, les prescriptions décrites plus haut s'appliquent.

Article 5.2 – Procédures de désinscription

Les annonceurs membres de l'association gèrent eux-mêmes ou requièrent que leurs prestataires mettent en place des procédures de désinscription conformes aux engagements de la présente charte.

Chapitre 6 – Routeurs

Article 6.1 – Rôle premier des routeurs

Les routeurs membres de l'association sont conscients du rôle central qu'ils jouent dans les procédures d'envoi en nombre de courriers électroniques. A ce titre, ils s'engagent à mettre en place les outils permettant à leurs clients de remplir les obligations prévues par la présente charte ou à les conseiller sur les bonnes pratiques à respecter.

Article 6.2 – Respect des normes techniques

Lorsque les outils mis en place par un routeur membre de l'association sont utilisés pour construire les courriers électroniques envoyés en nombre, ceux-ci incluent l'ensemble des fonctionnalités permettant de respecter les bonnes pratiques décrites dans la présente charte. Si des outils externes sont utilisés par ses clients, le routeur vérifie de façon régulière ou selon les alertes qu'il reçoit l'application des bonnes pratiques par ceux-ci et les conseille dans l'amélioration des procédures.

Article 6.3 – Gestion des abus

Les routeurs membres de l'association apportent une attention toute particulière à la gestion des informations qui leur parviennent par les procédures de gestion des abus ou issues des boucles de rétroaction.

Chapitre 7 – Fournisseurs d'accès à Internet et hébergeurs

Article 7.1 – Traitement des signalements d'adresses IP émettant des courriers électroniques non sollicités

Les fournisseurs d'accès à Internet et les hébergeurs membres de l'association mettent en œuvre des procédures de sécurisation correspondant aux conditions ci-après:

- Les mesures prises sont proportionnelles au risque lié à chaque situation ;
- Les types de mesures envisagées comportent plusieurs niveaux de réaction, appliquées dans la mesure du possible de façon progressive, sauf dans les situations ou la sécurité ou la qualité de fonctionnement du réseau sont sévèrement mis en cause ;
- Quelles que soient les mesures prises, le client ou l'usager doivent toujours pouvoir disposer d'un moyen d'accéder à leurs données personnelles (en particulier pour les services d'hébergement) ;
- En particulier pour les clients grand public, les titulaires de l'adresse IP (ou autre service) concernée sont informés des raisons des mesures prises et reçoivent par tout moyen adéquat des conseils adaptés à leur situation pour leur permettre de rétablir rapidement l'ensemble des fonctionnalités permises par la prestation dont ils sont titulaires.

Chapitre 8 – Hébergeurs

Les engagements de ce chapitre s'ajoutent à ceux évoqués dans le chapitre 7.

Article 8.1 – Cas particulier du hameçonnage et autres diffusions de contenus malveillants

Les hébergeurs membres de l'association mettent en œuvre des procédures permettant de supprimer ou de rendre inaccessible, dans les délais les plus brefs possibles, tout contenu, programme ou données contribuant à une opération de hameçonnage ou à la diffusion de logiciels malveillants.

Article 8.2 – Cas particulier des hébergeurs offrant des services d'émission et de réception de courriers électroniques

Les hébergeurs qui offrent des services d'émission et de réception de courriers électroniques:

- Informent leurs clients émettant des courriers électroniques et gérant un nom de domaine de bonnes pratiques, dont celles préconisées par la présente charte, et mettent à leur disposition des outils leur permettant de les respecter ;
- Respectent les dispositions de la présente charte en la matière pour les noms de domaine relevant de leur compétence directe.

Chapitre 9 – Autorités

Article 9.1 – Indépendance

Signal-Spam comporte parmi ses membres associés des autorités en charge de la protection des données à caractère personnel, de la sécurité des réseaux ou de missions de police judiciaire. A ce

titre, elles conservent toute leur indépendance par rapport aux membres de l'association, conformément aux législations et aux règlements qui encadrent leurs missions. Cette indépendance couvre notamment le secret de l'enquête.

Lorsque des informations issues des traitements opérés par l'association ou ses membres sont nécessaires aux missions des autorités, elles les obtiennent uniquement grâce aux procédures prévues par les lois et règlements.

Article 9.2 – Appui technique et juridique

Dans le contexte précisé précédemment, les autorités apportent un appui technique ou juridique permettant à l'association et à ses membres de remplir les objectifs de l'association.