Return Path

Prérequis de la Certification

L'email : notre cœur de métier

returnpath.com/fr

Toutes les exigences valables à partir de 2019

Sommaire

Sommaire
Présentation du programme de Certification
Obtention de la Certification
Conservation de la Certification
Présentation des normes de Certification
Détail des normes de Certification
1. Business model
2. Mesurabilité
3. Infrastructure
4. Contenu des emails
5. Points de collecte
6. Consentement
Exemples de pratiques interdites en matière de consentement
7. Politique de confidentialité
8. Légitimité
9. Sécurité
10. Boucles de rétroaction
11. Communication
12. Performances et conformité
Besoin d'aide ?

Présentation du programme de Certification

Le programme de Certification de Return Path offre la liste blanche la plus sélective et performante du secteur. Mais ce n'est là qu'un de ses atouts. Ce programme vous donne accès aux avantages exclusifs réservés aux opérateurs de messagerie et fournisseurs de données, vous permettant ainsi d'améliorer votre taux de remise en boîte de réception, d'atteindre davantage d'abonnés et de doper votre chiffre d'affaires.

Obtention de la Certification

Notre programme de Certification est destiné à l'élite des annonceurs, qui répondent aux attentes des abonnés et des principaux opérateurs de messagerie et respectent les bonnes pratiques du secteur. Tout au long du processus de Certification, nous travaillons de concert avec vous afin que vos campagnes respectent les normes du programme.

Voici les principales étapes à suivre pour obtenir la Certification :

1. Envoyez ce formulaire si vous souhaitez obtenir la Certification et n'avez jamais été en contact avec Return Path. Si vous êtes déjà un client de Return Path, contactez votre chargé de compte ou envoyez une demande d'assistance.
2. Au début du processus de Certification, nous réalisons un audit complet de vos campagnes email afin de nous assurer qu'elles répondent à toutes les normes de Certification détaillées ci-dessous.
3. Au cours de cet audit, nous vous prévenons si des aspects de vos campagnes email ne répondent pas à nos exigences. Pour que nous puissions poursuivre l'audit, vous devez apporter les modifications requises dans les 30 jours suivant notre demande. (Ne vous inquiétez pas, nous vous fournirons des informations supplémentaires sur les modifications nécessaires et la procédure à suivre.)
4. Dès lors que les modifications appropriées ont été apportées, nous finalisons votre audit et vous envoyons un email d'activation de compte.
5. Une fois la Certification obtenue, vos adresses IP commenceront à bénéficier d'avantages auprès d'AOL, de Microsoft, de Yahoo! et d'autres opérateurs de messagerie et fournisseurs de solutions de sécurité internationaux.

Conservation de la Certification

En tant qu'expéditeur certifié, vous êtes tenu de respecter en permanence les normes de Certification utilisées pour évaluer vos campagnes durant l'audit. En respectant constamment les normes de Certification, vous vous assurez de bénéficier de tous les avantages du programme en matière de délivrabilité. Nous procédons à des vérifications régulières de la conformité afin de nous assurer que vos campagnes email continuent de répondre à nos exigences et de protéger le programme de Certification.

La Certification offre de nombreux avantages, notamment :

- Amélioration tangible du placement en boîte de réception auprès des opérateurs de messagerie tels que Microsoft, Yahoo!, AOL et d'autres, y compris lors des périodes cruciales de fêtes et de soldes, durant lesquelles les opérateurs de messagerie appliquent souvent des filtrages et des limites en termes de volume d'envoi horaire aux expéditeurs
- Flux de données exclusifs des opérateurs de messagerie, qui fournissent des informations détaillées sur vos performances et votre placement en boîte de réception
- Equipe de surveillance dédiée, opérationnelle 24 heures sur 24, 7 jours sur 7, qui vous envoie des alertes de sécurité et vous aide à résoudre les éventuelles compromissions

Nous comprenons que des problèmes puissent déclencher une situation de non-conformité, ce qui peut entraîner une suspension temporaire du programme pendant que vous rectifiez la situation. Cependant, si vous enfreignez les normes de Certification de manière flagrante, répétée ou excessive, nous vous en aviserons et vous aiderons à mettre en œuvre les modifications nécessaires. Nous nous réservons également le droit de vous exclure du programme, le cas échéant.

Présentation des normes de Certification

A présent que vous en savez plus sur le programme de Certification ainsi que sur l'obtention et la conservation de la Certification, il est temps de découvrir les normes de Certification. Les informations ci-dessous décrivent les normes auxquelles vos campagnes email doivent répondre pour vous permettre de réussir l'audit initial et de rester certifié après avoir obtenu la Certification.

Détail des normes de Certification

Les normes de Certification concernent 12 aspects différents de vos campagnes email, tels que votre infrastructure de routage ou votre politique de confidentialité. Ensemble, elles offrent une vue complète de vos campagnes email et déterminent si vous êtes admissible à notre programme de Certification.

Vous trouverez ci-dessous les différents aspects que nous vérifions et leur signification :

- Le **business model** explique qui vous êtes et ce que vous faites.
- La **mesurabilité** indique le nombre et la fréquence des emails envoyés.
- L'**infrastructure** précise le mode d'envoi, d'authentification et de gestion des emails.
- Le **contenu des emails** détermine la façon dont vous vous présentez à vos abonnés.
- Les **points de collecte** indiquent les méthodes que vous utilisez pour collecter des adresses email.
- Le **consentement** définit la façon dont les abonnés acceptent de recevoir vos emails.

- La **politique de confidentialité** documente tous les détails de vos campagnes email.
- La **légalité** est importante pour votre entreprise et détermine si vous respectez les lois applicables en matière de spam et de confidentialité des données qui concernent votre entreprise et vos abonnés.
- La **sécurité** illustre la manière dont vous protégez vos systèmes et les données de vos abonnés.
- La **communication** atteste de votre volonté et de votre capacité à communiquer avec Return Path.
- L'utilisation de **boucles de rétroaction** démontre que vous tenez à conserver une liste d'abonnés « propre ».
- Les **performances et la conformité** déterminent si vos campagnes email sont en mesure de respecter les limites établies par les opérateurs de messagerie et les abonnés.

Poursuivez la lecture pour en savoir plus sur chacune des sections énumérées ci-dessus.

1. Business model

Pour commencer votre audit de Certification, nous examinons votre **business model**. Celui-ci fournit des informations importantes sur l'ensemble de vos campagnes email et nous aide à déterminer si vous êtes un bon candidat à la Certification.

Voici les normes auxquelles votre business model doit répondre pour vous permettre d'obtenir et de conserver la Certification :

1. **Immatriculation de l'entreprise**

    a. L'identité de votre entreprise peut être vérifiée par une source tierce via un site web légitime, tel qu'un registre national, ou une application telle que Dun & Bradstreet.
    b. L'immatriculation de votre entreprise inclut l'adresse postale actuelle de votre entreprise.
    c. Votre entreprise exerce ses activités depuis au moins un an.
    d. Votre entreprise n'a pas recours à un agent enregistré pour masquer des informations la concernant.

2. **Présence sur le Web**

    a. Votre entreprise gère un site web et des pages de destination valides pour toutes les marques dont des emails marketing seront envoyés via les adresses IP certifiées depuis au moins six mois.

3. **Adresses IP et contenu**

a. Nous ne certifions actuellement que les adresses IP dédiées. Les adresses IP partagées ne sont pas admissibles.
b. Les adresses IP certifiées peuvent uniquement envoyer des emails spécifiques à l'annonceur. Cela signifie que les adresses IP certifiées ne peuvent pas envoyer d'emails tiers, c'est-à-dire de messages diffusés au nom d'entités autres que votre marque.
c. Les adresses IP certifiées peuvent uniquement envoyer des emails transactionnels et à visée commerciale. Cela signifie que vous ne pouvez pas utiliser les adresses IP certifiées pour envoyer des emails d'entreprise, qui incluent souvent des communications internes entre collègues ou des messages de support à la clientèle.
d. Les adresses IP certifiées doivent diffuser des emails basés sur des modèles dans lesquels la marque est clairement identifiée. Elles ne peuvent pas envoyer de contenu libre comme des formulaires web ou des zones de texte libre.

IMPORTANT : Nous ne certifions pas les adresses IP des entreprises appartenant à l'une des catégories suivantes :

- Agences
- Expéditeurs pour le compte de tiers
- Génération de prospects
- Sites web d'enchères
- Activités illégales
- Trafic d'êtres humains

2. Mesurabilité

Si votre business model répond à nos exigences, nous examinons la **mesurabilité** de vos campagnes email. Ce critère nous aide à comprendre vos tendances générales en matière d'envoi, y compris la fréquence d'envoi d'emails à vos abonnés.

Voici les normes de mesurabilité auxquelles vous devez répondre pour obtenir et conserver la Certification :

1. **Volume mesurable et régulier**

a. Votre adresse IP envoie au moins 100 emails à Microsoft et 100 à Yahoo! au cours de la période de 30 jours la plus récente, comme en attestent les sources de données de Return Path.
b. Votre adresse IP maintient un volume mesurable et régulier pour rester certifiée. La régularité est déterminée sur la base de vos campagnes email et de votre comportement en matière d'envois. S'il apparaît que le volume d'une adresse IP n'est ni mesurable ni régulier, celle-ci est suspendue après 30 jours et supprimée du processus de candidature ou du programme de Certification après 90 jours.

2. **Ciblage des opérateurs de messagerie**

    a. Votre entreprise ne peut pas utiliser une adresse IP unique pour envoyer des emails à un opérateur de messagerie spécifique du réseau d'usagers ou du réseau d'opérateurs de Return Path.
    *Les envois occasionnels et temporaires à un destinataire unique peuvent être tolérés dans certains cas, pour autant que Return Path ait donné son accord écrit préalable.

3. Infrastructure

Dès lors que votre mesurabilité répond à nos exigences, nous examinons l'**infrastructure** de routage de vos emails, autrement dit le matériel et les processus utilisés pour le déploiement des campagnes email. Vous devez impérativement envoyer vos emails à partir de systèmes d'infrastructure correctement gérés et qui respectent les bonnes pratiques.

Gardez à l'esprit que vous devrez peut-être collaborer avec votre routeur ou votre équipe informatique interne pour répondre aux normes détaillées ci-dessous afin d'obtenir et de conserver votre Certification :

1. **Adresses IP dédiées**

    a. Votre entreprise est la seule entité à envoyer des emails sur les adresses IP dédiées depuis au moins 60 jours.

2. **Relais ouverts**

    a. Votre infrastructure ne contient pas de serveurs à relais ouverts.

3. **FCrDNS**

    a. Les entrées de résolution DNS inverse (rDNS) de vos adresses IP correspondent aux entrées de résolution DNS vers l'avant, également appelées FCrDNS (Forward-Confirmed reverse DNS).

4. **Listes noires**

    a. Vos adresses ou domaines IP ne figurent pas sur une liste noire surveillée par Return Path. Des placements répétés ou excessifs sur liste noire peuvent entraîner la suspension ou la révocation des avantages liés à la Certification. Découvrez les seuils de placement sur liste noire ci-dessous
    .

5. **SPF**

    a. Tous vos domaines Return-Path et expéditeurs disposent d'enregistrements SPF (Sender Policy Framework) publiés. Découvrez comment configurer le protocole SPF ici.
    b. Vos enregistrements SPF passent les contrôles d'authentification des opérateurs avec succès, dans les limites de tolérance opérationnelle raisonnable définies par Return Path.
    c. Aucun domaine d'envoi ou Return-Path n'utilise une directive `+all` ou `?all`.
    d. Aucun domaine d'envoi ou Return-Path n'inclut d'enregistrement PTR (pointeur).

6. **DKIM**

    a. L'authentification DomainKeys Identified Mail (DKIM) est configurée sur tous les emails que vous envoyez sur des adresses IP certifiées. Découvrez comment configurer l'authentification DKIM ici.
    b. Votre authentification DKIM passe les contrôles d'authentification des opérateurs de messagerie avec succès, dans les limites de tolérance opérationnelle raisonnable définies par Return Path.

7. **DMARC** (recommandation uniquement)

    a. Nous vous *recommandons fortement* d'implémenter le protocole Domain-based Message Authentication, Reporting & Conformance (DMARC). Cette implémentation ne constitue cependant pas une norme de Certification à l'heure actuelle. Découvrez comment configurer un enregistrement DMARC ici.

8. **Comptes de rôle**

    a. Vous configurez et maintenez des comptes de rôle abuse@ et postmaster@ pour tous les domaines Return-Path et d'envoi afin de traiter les plaintes et autres problèmes.
    b. Nous vous recommandons également de prendre en charge et de gérer d'autres comptes de rôle standard tels que les comptes support@ ou help@.

9. **Enregistrements WHOIS**

    Vos enregistrements WHOIS doivent répondre aux critères suivants pour tous les domaines d'envoi, les domaines Return-Path et les domaines de site web associés à l'email envoyé à partir de vos adresses IP.

    a. Votre entreprise tient les enregistrements WHOIS à jour.
    b. Vos enregistrements WHOIS contiennent la dénomination sociale de votre entreprise. Pour les enregistrements WHOIS de votre domaine Return-Path, le nom légal peut être celui de votre routeur, le cas échéant.

c. Vos enregistrements WHOIS recensent au moins une méthode de contact, telle que le numéro de téléphone ou l'adresse email.
d. Vos enregistrements WHOIS contiennent l'adresse postale actuelle de votre entreprise, qui n'est pas une boîte postale.
e. Vos enregistrements WHOIS ne dissimulent pas les informations de votre entreprise à l'aide de services de proxy ou de confidentialité.
f. Découvrez un exemple et des informations supplémentaires sur les enregistrements WHOIS ici.

10. **Maintenance des listes**

a. Votre entreprise utilise des systèmes de maintenance des listes d'adresses email pour recevoir et traiter de manière fiable les erreurs de remise en boîte de réception, les messages de retour à l'expéditeur (bounce) et les autres réponses des réseaux de réception.
b. Vous traitez les notifications de rejet permanent reçues en réponse à des emails envoyés sur vos adresses IP en supprimant l'adresse email à l'origine de la notification de non-remise de tous les futurs envois.

4. Contenu des emails

Si votre infrastructure répond à nos exigences, nous examinons le **contenu de vos emails**. Nous nous assurons principalement que vos messages respectent les bonnes pratiques décrites par les opérateurs de messagerie, notamment la transparence de votre identité aux yeux de vos abonnés.

Voici les normes en matière de contenu des emails que vous devez respecter pour obtenir et conserver la Certification :

1. **Marque**

a. Vous envoyez des emails qui présentent clairement la marque de votre entreprise pour vous identifier précisément auprès de vos abonnés.

2. **Ligne d'objet**

a. Toutes les lignes d'objet sont exactes.
b. Les lignes d'objet sont clairement liées au contenu du corps de l'email et ne sont ni trompeuses ni mensongères.
c. Aucune ligne d'objet ne comprend « RE : » ou « TR :». L'utilisation de ces abréviations est généralement perçue comme une tactique trompeuse qui incite les abonnés à ouvrir l'email comme s'il avait été envoyé par une personne plutôt que par un expéditeur

commercial.

3. **Contenu du corps du message**

   a. Le contenu du corps du message est exact et précis.
   b. Vous devez inclure l'adresse postale de votre entreprise dans tout email commercial, promotionnel ou transactionnel.
   c. Vous n'utilisez pas de raccourcisseurs d'URL dans le corps de vos messages, notamment Bitly, TinyURL et Google URL Shortener.
   d. Vous ne pouvez pas utiliser de lien Signaler comme courrier indésirable dans le corps de vos messages. Ce type de lien est généralement utilisé par les expéditeurs qui tentent d'éviter le dépôt de plaintes auprès des opérateurs de messagerie.

4. **En-têtes des messages**

   a. Les en-têtes des messages ne sont pas falsifiés, masqués, mensongers ou trompeurs, et vous utilisez notamment des en-têtes Return-Path, From et de nom et d'adresse d'expéditeur conviviaux.

5. **Contenu tiers**

   Comme indiqué ci-dessus à la section 1, les emails spécifiques à l'annonceur qui contiennent du contenu tiers (publicité sponsorisée, par exemple) sont admissibles pour la Certification, mais doivent répondre aux exigences suivantes :

   a. La ligne d'objet fait référence au contenu propre à l'annonceur.
   b. Tous les emails affichent votre marque de façon visible afin d'indiquer clairement qu'ils émanent de vous, l'expéditeur certifié.
   c. L'essentiel du contenu de l'email relève du marketing de votre entreprise, y compris les liens et les logos.
   d. L'adresse From et l'adresse d'expéditeur conviviale (Friendly From) identifient l'expéditeur certifié et n'incluent pas le nom du tiers.

6. **Procédure de désinscription**

   a. Chaque email commercial, promotionnel ou sur invitation d'un « pair » envoyé sur votre adresse IP comprend un en-tête List-Unsubscribe et un lien de désinscription.
   b. Les instructions de désinscription sont claires, visibles et faciles à comprendre.
   c. Les mécanismes de désinscription sont faciles à utiliser pour le destinataire qui souhaite se désinscrire de vos campagnes email. Un mécanisme de désinscription convivial consiste par exemple à répondre à l'email à caractère commercial ou promotionnel pour faire la demande de désinscription ou à sélectionner un lien pour se désinscrire par le biais d'un processus en ligne.

d. Le processus de désinscription n'oblige pas le destinataire à fournir des informations autres que son adresse email. Nous recommandons l'utilisation d'un processus en un seul clic, tel que l'activation d'un lien.
e. Lorsqu'un destinataire se désinscrit de vos campagnes email, vous cessez de lui envoyer tout email à caractère commercial ou promotionnel. Par ailleurs, vous ne vendez, louez ou partagez l'adresse email ou les informations personnelles du destinataire avec aucun tiers.
f. Vous traitez et honorez toutes les demandes de désinscription dans les trois jours suivant la réception de la demande.
g. Vous honorez la demande de désinscription de vos campagnes email de n'importe quel destinataire pour une durée illimitée, même en cas d'invitation d'un « pair », ou jusqu'à ce qu'il choisisse de participer à nouveau à vos campagnes email. Découvrez les exigences en matière de consentement explicite (opt-in) de la Certification ici.
h. Les liens de désinscription qui sont envoyés par email restent actifs et fonctionnels pendant au moins 60 jours après la date d'envoi.
i. Si un destinataire demande à se désinscrire de vos campagnes email par le biais d'un mécanisme de désinscription non standard, vous traitez également la demande dans un délai raisonnable. Ces mécanismes de désinscription non standard peuvent notamment prendre la forme d'un courrier postal, d'adresses email alias, d'adresses postmaster ou abuse et d'appels téléphoniques.
j. Vous devez inclure un lien de désinscription valide dans tout sondage par email visant à recueillir les commentaires des destinataires. Toutefois, vous n'êtes pas obligé d'inclure un mécanisme de désinscription si vous envoyez à un destinataire un sondage lié à une transaction antérieure avec votre entreprise.

5. Points de collecte

Après avoir établi que le contenu de vos emails et les processus de désinscription répondent à nos exigences, nous examinons la manière dont vous collectez les adresses email, autrement dit vos **points de collecte**. Il est essentiel que vous informiez directement les abonnés du type d'emails auxquels ils s'abonnent, du contenu auquel ils doivent s'attendre, etc.

Vos points de collecte doivent répondre aux exigences suivantes :

1. **Clarté et simplicité**

a. Des informations claires et simples sont disponibles à tous les points de collecte des adresses email. Il ne suffit pas d'inclure un lien vers votre politique de confidentialité pour remplir cette exigence : les informations doivent figurer en toutes lettres au point de collecte.
b. Vous fournissez au futur abonné des informations précises sur les emails qu'il recevra s'il soumet son adresse email. Il peut par exemple s'agir d'informations sur la nature exacte du contenu ou la fréquence des emails.

c. Vous devez indiquer clairement au niveau de tous les points de collecte si vous partagez ou louez les adresses email ou des informations personnelles de vos abonnés.

2. **Politique de confidentialité**

   a. Votre politique de confidentialité est directement référencée de façon claire et visible au niveau de tous les points de collecte, y compris sur les applications mobiles. Découvrez nos exigences en matière de politique de confidentialité ici.

6. Consentement

Si vos points de collecte sont conformes à nos standards, nous allons analyser vos pratiques en terme de recueil de consentement. Nous voulons nous assurer que vous demandez/recevez le consentement de vos abonnées conformément à nos attentes.

Voici les exigences que vous devez satisfaire concernant le consentement afin de devenir certifié et rester certifié.

1. **Méthodes d'opt in autorisées**

   Vous devez utiliser une des méthodes suivantes d'opt in quand vous obtenez le consentement de vos abonnées.

   a. **Le double opt-in (avec confirmation)**: Le double opt'in ne devient effectif qu'après avoir cliqué sur un lien dans un e-mail de confirmation d'enregistrement de la demande. L'objectif est de disposer de la validation des destinataires avant de leur envoyer des e-mails.
   b. **L'opt in avec une notification**: Dès qu'un abonné s'inscrit à votre programme email, vous devez lui envoyer une notification pour confirmer son abonnement et inclure aussi des instructions claire et explicite de désabonnement avant de lui envoyer des e-mail.

   Pour le double opt in et l'opt in avec notification, vous pouvez avoir une case à précochée que les utilisateurs pourront désélectionner pendant la création de leur compte s'ils décident de ne pas recevoir les emails promotionnels.

   c. **Autres méthodes de consentement**: Si votre programme d'email se réfère à une méthode de consentement alternative comme base légale de collecte de données personnelles, vous devrez nous fournir la base de documentation de cette méthode, telle qu'une évaluation d'intérêt légitime ou n'importe autre évaluation.

   Rappelez-vous qu'il est important de vous conformer aux lois et aux règlements qui vous impactent et qui peuvent être potentiellement plus restrictives que les exigences de notre programme.

2. **Co-enregistrement**

   Lorsque vous offrez aux utilisateurs la possibilité supplémentaire de s'inscrire aux campagnes email d'entités tierces ou affiliées sur votre site web, vous devez répondre aux exigences suivantes. Celles-ci s'appliquent également à toutes les marques qui opèrent sous la même société mère.

   a. Au point de collecte, vous désignez de façon claire et visible l'entreprise dont le destinataire recevra également des emails en cas d'inscription.
   b. Vous définissez clairement chaque marque dont le destinataire recevra également des emails en cas d'inscription. Vous proposez également des options d'inscription distinctes, telles que des cases à cocher désélectionnées par défaut. Cette exigence s'applique également aux marques qui opèrent sous la même société mère.
   c. Vous êtes en mesure de produire une preuve de consentement pour chaque adresse collectée. Cette preuve doit inclure la date, l'heure, l'adresse IP d'origine et l'emplacement (URL) du point de collecte.

3. **Emails de transfert à un ami et envoyés sur invitation d'un « pair »**

   a. Le formulaire d'inscription comprend un test CAPTCHA ou reCAPTCHA pour vérifier la légitimité de l'ami à l'origine de l'email. Les tests CAPTCHA et reCAPTCHA permettent de bloquer les robots ou les utilisateurs abusifs.
   b. Vous n'envoyez qu'un seul email de transfert à un ami à caractère publicitaire ou promotionnel à l'adresse soumise.
   c. Si le destinataire d'un email de transfert à un ami ne répond pas, vous ne pouvez lui envoyer qu'un seul message de suivi.
   d. Les domaines Return-Path et Mail-From (MFrom) sont vos propres domaines qui figurent dans l'en-tête de l'email.
   e. Vous fournissez aux destinataires un moyen de se désinscrire de tous les emails à venir, autrement dit un mécanisme de désinscription globale.
   f. Les emails ne contiennent pas de liens ou d'URL vers des adresses web externes.
   g. Les emails peuvent inclure des commentaires personnalisés comptant jusqu'à 140 caractères.
   h. Un utilisateur individuel peut uniquement utiliser cette fonction pour envoyer 100 messages au maximum sur une période de 24 heures.
   i. Pour envoyer des emails à caractère commercial ou promotionnel supplémentaires au destinataire d'un email de transfert à un ami, vous devez obtenir son consentement explicite à l'aide d'une des méthodes de consentement explicite acceptables décrites ci-dessus.

Exemples de pratiques de consentement interdites

- Les cases pré-cochées par défaut (sans notification)
- L'opt-in (sans notifications)
- La collecte d'adresses de courriel sans consentement
- Location ou achat de base e-mail. Enrichissement de bases email.
- L'envoi des e-mails de prospection

7. Politique de confidentialité

Si vos pratiques de consentement répondent à nos exigences, nous examinons votre **politique de confidentialité**. Il est important de noter que vos politiques de confidentialité doivent impérativement respecter les lois applicables. Nous nous assurons en outre que vous faites preuve d'une totale transparence auprès des abonnés potentiels en ce qui concerne vos campagnes email, les moyens dont ils disposent pour vous joindre et les données que vous collectez.

Voici les normes relatives à la politique de confidentialité que vous devez respecter pour obtenir et conserver la Certification :

1. **Accès aisé**

    a. Votre politique de confidentialité est facilement accessible sur la page d'accueil de votre site web.

2. **Instructions de désinscription**

    a. Votre politique de confidentialité contient des instructions claires et directes indiquant aux abonnés comment se désinscrire de vos campagnes email.

3. **Adresse postale**

    a. Votre politique de confidentialité inclut l'adresse postale de votre société et des sociétés partenaires. Les boîtes postales sont acceptables mais les abonnés préfèrent les adresses réelles.

4. **Point de collecte**

    a. Votre politique de confidentialité reflète fidèlement les pratiques de votre entreprise lorsqu'elle est référencée au niveau des points de collecte. Par exemple, vous devez expliquer l'usage fait des adresses email une fois collectées.

5. **Divulgation des données**

a. Votre politique de confidentialité doit informer les destinataires de toutes les informations personnelles collectées par votre entreprise et de la façon dont elles peuvent être partagées.

6. **Propriété des marques**

a. Si vous êtes une société mère détentrice de plusieurs marques, vous devez inclure une liste de toutes les autres marques que vous possédez dans chaque politique de confidentialité.
b. Si vous êtes une marque appartenant à une société mère, vous devez inclure le nom de la société mère dans votre politique de confidentialité.

8. Légitimité

En tant qu'entreprise, vous êtes tenu de respecter toutes les **lois et réglementations** en vigueur qui vous sont applicables. Chaque pays et territoire dispose d'une législation relative aux pratiques en matière d'email et de données. Vous devez impérativement respecter pleinement ces lois et réglementations partout où vous exercez vos activités.

Exemples (non exhaustifs) :

- États-Unis : Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)
- Canada : Loi canadienne anti-pourriel (LCAP)
- Union européenne : RGPD (Règlement général sur la protection des données)
- Australie : Loi sur le spam de 2003

9. Sécurité

Dans le cadre de votre audit, nous examinons ensuite vos pratiques en matière de **sécurité**. Il est important que votre entreprise prenne les mesures qui s'imposent, conformes aux normes du secteur, pour protéger votre base de données et vos systèmes et, partant, votre infrastructure et vos abonnés.

Voici les normes de sécurité que vous devez respecter pour obtenir et conserver la Certification :

1. **Infrastructure**

a. Votre infrastructure de messagerie est gérée et exploitée de manière responsable.

2. **Protection des abonnés**

    a. Votre entreprise met en œuvre des stratégies et procédures appropriées, conformes aux normes du secteur, pour sécuriser et protéger les adresses email et autres informations personnelles identifiables de vos abonnés.

3. **Systèmes sécurisés**

    a. Votre entreprise a recours à des outils standard du secteur pour bloquer les proxys et relais ouverts, les virus, les vers, les logiciels espions, les logiciels publicitaires, les chevaux de Troie, les requêtes DNS récursives ou tout autre élément identifié comme malveillant sur votre infrastructure.

4. **Compromissions**

    a. Si vous découvrez que votre adresse IP ou votre domaine a été compromis, vous êtes tenu d'en informer Return Path par écrit dans les deux jours ouvrables.
    b. Si votre adresse IP ou votre domaine est compromis, vous acceptez que cette adresse IP ou ce domaine ne sera pas réactivé au sein du programme de Certification tant qu'un employé de Return Path n'aura pas procédé à un examen complet et établi que la cause de la compromission a été correctement neutralisée.

10. Boucles de rétroaction

A titre de bonne pratique, nous vous recommandons de souscrire à toutes les boucles de rétroaction disponibles afin de gérer et réduire efficacement les plaintes. Vous trouverez la liste complète des boucles de rétroaction ici.

Si vous n'êtes pas en mesure de souscrire à toutes les boucles de rétroaction pour une raison quelconque, voici celles auxquelles vous devez impérativement vous inscrire pour obtenir et conserver la Certification :

- Boucle de rétroaction des domaines et adresses IP Comcast
- Boucle de rétroaction Yahoo!
- Programme Microsoft Junk Mail Reporting
- Boucle de rétroaction AOL

11. Communication

Que vous soyez au début du processus de Certification ou déjà certifié, il est important de maintenir une communication claire et ouverte entre votre entreprise et Return Path.

Voici les normes de communication à respecter pour obtenir et conserver la Certification :

1. **Résolution des problèmes**

    a. Toutes les parties impliquées dans l'envoi des emails au sein de votre entreprise coopèrent avec les administrateurs de Certification pour résoudre les problèmes liés au programme de Certification.
    b. Vous répondez aux notifications du programme dans les trois jours suivant la notification et appliquez les mesures correctives requises dans les dix jours.

2. **Informations de contact**

    a. Vous tenez Return Path informé de toute modification de vos informations de contact.

12. Performances et conformité

Une part essentielle du maintien de la Certification consiste à s'assurer que vos campagnes email restent dans les limites de nos seuils de performances. Lorsque vous respectez les seuils répertoriés ci-dessous, vous bénéficiez d'avantages auprès des opérateurs de messagerie correspondants, ce qui améliore votre délivrabilité globale et vous permet d'atteindre un plus grand nombre d'abonnés.

Remarque : Nous collaborons activement avec nos partenaires pour fixer les seuils et les suspensions.

Voici les normes de performances que vous devez respecter pour obtenir et conserver la Certification :

Seuils de conformité Microsoft SRD pour les adresses IP individuelles			
Volume de votants SRD	0 à 4	5 à 10	11 ou plus
Taux de votes SRD	Non mis en œuvre	5 votes négatifs	45 %

Seuils de conformité Microsoft SRD de groupe				
Volume de votants SRD	0 à 9	10 à 30	31 à 50	51 ou plus

Taux de votes SRD	Non mis en œuvre	75 %	65 %	55 %

Remarque : Nous appliquons la norme SRD de groupe dès lors que vous possédez deux adresses IP certifiées ou plus.

Conseil : Vous rencontrez des problèmes avec vos taux de votes SRD Microsoft ? Consultez ces ressources.

Seuils de conformité pour les plaintes, les adresses pièges et les listes noires

Microsoft : Taux de plaintes (moyenne sur 30 jours)	Volume d'envoi total 0,2 %
Yahoo! : taux de plaintes pour la boîte de réception (moyenne sur 30 jours)	Volume d'envoi total 0,6 %
AOL : Taux de plaintes (moyenne sur 30 jours)	N'est plus appliqué
Comcast : Taux de plaintes (moyenne sur 30 jours)	Volume d'envoi total 0,3 %
Adresses pièges (cumul sur 30 jours)	3 envois à des adresses pièges critiques 5 envois à des adresses pièges importantes
Adresses pièges RP Network 1 (cumul sur 30 jours)	100 envois à des adresses pièges
Adresses pièges Cloudmark (cumul sur 30 jours)	100 envois à des adresses pièges
Taux de plaintes Cloudmark (moyenne sur 30 jours)	Volume d'envoi total 1,0 %
Listes noires (placement actuel)	1 placement sur une liste critique 2 placements sur une liste importante

Remarque : Le programme de Certification n'applique les seuils de taux de plaintes propres aux opérateurs de messagerie que si l'expéditeur certifié a reçu un nombre minimum de plaintes auprès d'opérateurs spécifiques :

- Microsoft : 200 plaintes

- Yahoo! : 200 plaintes
- Comcast : 100 plaintes
- Cloudmark : 100 plaintes

Besoin d'aide ?

Pour plus d'informations sur le programme de Certification et ses exigences, ou pour découvrir comment résoudre les problèmes de délivrabilité et de réputation, visitez notre Centre d'aide.