

# DIGITAL MARKETING ADDENDUM

---

## 1. ÁMBITO

Este apéndice Digital Marketing se aplicará al uso del software de MAPP, especialmente, aunque sin limitación, al Digital Marketing Center (DMC) de MAPP, con fines de marketing digital, especialmente, aunque sin limitación, al marketing digital directo a través de mensajes electrónicos y para envíos en general. Este apéndice debe leerse junto con el contrato entre el cliente y MAPP.

## 2. DEFINICIONES

- 2.1 “Dirección” hace referencia a una dirección de correo electrónico, número de teléfono móvil o cualquier otra información de dirección electrónica o número de fax utilizada para enviar mensajes a través del software.
- 2.2 “Día hábil” hace referencia a un día laboral que no sea sábado, domingo ni festivo en el domicilio de MAPP.
- 2.3 “Capacidad de entrega” hace referencia a la capacidad de entregar mensajes de correo electrónico en las bandejas de entrada de los destinatarios y evitar que los mensajes de correo electrónico se pierdan, bloqueen o dirijan a la carpeta de correo no deseado.
- 2.4 “Dirección IP” hace referencia a la dirección de protocolo de internet, asignada a los servidores de correo utilizados para los envíos.
- 2.5 “ISP” hace referencia a los proveedores de servicios de correo electrónico y correo web como HoMappil, Gmail, etc.
- 2.6 “Lista” hace referencia a una lista de direcciones utilizadas o destinadas a utilizarse para realizar envíos a través del software.
- 2.7 “Mensaje” hace referencia a un mensaje electrónico (incluyendo, aunque sin limitación, correo electrónico, SMS/MMS, mensajes de inserción, mensajes en aplicación, mensajes instantáneos y mensajes, publicaciones y notificaciones en plataformas de medios sociales) o un mensaje de fax.
- 2.8 “Datos de carácter personal” hace referencia a cualquier información relativa a una persona física identificada o identificable, según esté definido en las leyes de protección de datos aplicables.
- 2.9 “Entrega rechazada” es la información de respuesta de un servidor de correo electrónico que indica que la dirección a la que se ha enviado un correo electrónico no existe o está desactivada de forma permanente.
- 2.10 “Envío” hace referencia a enviar/transmitir un mensaje a través del software.
- 2.11 “Queja de correo no deseado” hace referencia al mensaje de un ISP en el que informa a MAPP de que un correo electrónico enviado a través del software ha sido marcado por el destinatario como “basura” o “correo no deseado”.

## 3. PROVISIÓN Y USO DEL DMC

- 3.1 El sistema DMC del cliente se proporciona bajo un subdominio delegado por cliente (por ejemplo, noticias.cliente.com). El cliente deberá delegar un subdominio a MAPP y proporcionar cualquier otra información y cooperación necesarias para la configuración del sistema al menos cinco (5) días hábiles antes de la configuración programada del sistema.
- 3.2 La transferencia de datos en un formato no cifrado puede poner en peligro la confidencialidad de los datos. Por lo tanto, los datos transferidos a MAPP para su importación al DMC deben transferirse a través de una conexión segura (por ejemplo, sFTP). Es un principio básico de MAPP que los datos proporcionados por el cliente solo se almacenen dentro del entorno seguro del DMC. Por motivos de seguridad, los datos facilitados a través de servidores FTP/sFTP se eliminarán de dichos servidores de forma regular.
- 3.3 El almacenamiento de información e informes relativos a envíos específicos requiere grandes capacidades de almacenamiento dentro del entorno del DMC. Por ello, la información y los informes se archivan 12 meses después de realizar el envío específico y ya no es posible acceder directamente a ellos a través del DMC. MAPP podrá recuperar copias de seguridad e información archivada, pero cargando sus tarifas por hora estándar vigentes en ese momento. Las imágenes y gráficos o archivos adjuntos a los mensajes se suprimen 6 meses después de la fecha del envío.
- 3.4 Todos los datos alojados y tratados por MAPP en nombre del cliente se suprimen del sistema DMC del cliente inmediatamente si así lo solicita el cliente y al terminar el contrato. La supresión del sistema DMC no afecta a los datos de las copias de seguridad del sistema DMC. En caso de terminación del contrato, se requerirá al cliente que descargue/exporte sus datos de su sistema DMC antes de la fecha de terminación efectiva. Tras la terminación, el cliente ya no podrá acceder a su sistema DMC. El cliente es responsable de cumplir con todas las obligaciones y requisitos de retención. MAPP no está obligada a almacenar o mantener registros en nombre del cliente.
- 3.5 MAPP tiene derecho a analizar los envíos del cliente de forma agregada/anónima y a utilizar estos análisis para el mantenimiento y mejora del DMC y con fines estadísticos, para investigación de mercado y para publicaciones (por

ejemplo, para determinar la tasa de apertura promedio de boletines enviados por correo electrónico en el sector de bienes de consumo). El cliente no será identificado en este tipo de publicaciones.

#### 4. POLÍTICA DE CONFORMIDAD

- 4.1 El cliente debe cumplir todas las leyes, normativas y normas de buenas prácticas del sector aplicables en relación al uso del software, lo que incluye el tratamiento de datos personales a través del DMC, la realización de envíos a través del DMC y el uso de servicios relacionados, como el alojamiento de sitios web/páginas de aterrizaje. El cliente es responsable de identificar e interpretar las leyes, normativas y normas de buenas prácticas del sector aplicables que afectan al uso del DMC por parte del cliente y al rendimiento de los servicios de MAPP para y/o en nombre del cliente. Es responsabilidad del cliente garantizar el cumplimiento de esos requisitos.
- 4.2 MAPP no está obligada a proporcionar el DMC a clientes que realizan envíos que incumplen las leyes, normativas y normas de buenas prácticas del sector aplicables, ni a procesar dichos envíos.
- 4.3 Los mensajes comerciales/de marketing, según lo definido por las leyes, normativas y normas de buenas prácticas del sector aplicables, solo se pueden enviar a través del DMC si el destinatario ha dado su consentimiento para recibir dichos mensajes o si el envío de dichos mensajes cumple lo dispuesto en las leyes y normativas aplicables, en particular las que se refieren a la protección de datos y comercio justo, y en las normas de buenas prácticas del sector aplicables. El consentimiento del destinatario, si es necesario, debe cumplir los requisitos legales en cuanto a forma y contenido, y debe estar documentado y ser verificable de acuerdo con las leyes, normativas y normas de buenas prácticas del sector aplicables. El carácter comercial de los mensajes comerciales/de marketing no debe quedar disfrazado o escondido.
- 4.4 Los mensajes comerciales/de marketing deben contener información de contacto del cliente que cumpla las leyes, normativas y normas de buenas prácticas del sector aplicables y deben contener un vínculo para anular la suscripción u otra posibilidad de contacto adecuada para que los destinatarios puedan revocar su consentimiento y/o darse de baja de otros mensajes comerciales/de marketing. Las anulaciones de suscripción enviadas a través de la función de cancelación de suscripción integrada en el DMC se procesarán de forma automática y la dirección correspondiente quedará bloqueada para futuros envíos. Cualquier otro proceso de anulación de suscripción proporcionado por el cliente no debe ser excesivamente complicado. Las anulaciones de suscripción recibidas directamente por el cliente deberán ser procesadas en un plazo de (3) tres días hábiles. El cliente debe garantizar que todos los mensajes dirigidos a “de dirección” y a la dirección de respuesta indicada en el mensaje se procesan inmediatamente. Algunos ISP informan a MAPP si un mensaje enviado a través del DMC ha sido marcado como “basura” o “correo no deseado” por el destinatario (lo que se denomina “bucle de realimentación”). DMC tratará dichas marcas como una anulación de la suscripción y la dirección correspondiente quedará bloqueada para futuros envíos.
- 4.5 En el caso de que un mensaje enviado por el cliente (i) genere una reclamación presentada por un destinatario ante MAPP, (ii) provoque la inclusión en una lista negra por parte de una organización de lucha contra el correo no deseado (como Spamhaus o Spamcop) o (iii) provoque que MAPP reciba una reclamación o una investigación por parte de una autoridad reguladora o de supervisión o de una asociación pertinente (como asociaciones de marketing directo o asociaciones de defensa del consumidor), el cliente, a solicitud de MAPP y en el plazo de un día hábil, deberá presentar pruebas que demuestren la legalidad del envío correspondiente. MAPP tendrá derecho a revelar esas pruebas a terceros en caso necesario y en la medida en que se requiera.
- 4.6 El cliente no debe (i) enviar, guardar, enlazar ni de otro modo indicar contenido que sea pornográfico, sexualmente sugerente de forma implícita o explícita, amenazante, insultante, verbalmente agresivo, difamatorio, fraudulento, vulgar, obsceno, incite al odio, sea extremista de izquierda o de derecha, enaltezca la violencia, invada derechos personales, contravenga las leyes de protección de la juventud o pida o instigue a la violación de las leyes, (ii) enviar, guardar, enlazar ni de otro modo indicar contenido que infrinja derechos de terceros, incluyendo, aunque sin limitarse a ello, derechos de marcas comerciales y derechos sobre otros símbolos, derechos de autor, patentes, diseños, modelos de utilidad y secretos comerciales, y (iii) no enviar, guardar ni enlazar con ningún tipo de malware (como virus) o de otro modo señalado como malware.
- 4.7 El DMC ofrece numerosas características y funciones (como el seguimiento de campañas, la generación de perfiles de usuario y la orientación por comportamiento o geografía). El uso de estas características y funciones puede requerir la notificación o el consentimiento previo del interesado. El cliente debe asegurarse de que todas las características y funciones se utilizan de acuerdo con las leyes, normativas y normas de buenas prácticas del sector aplicables. El cliente debe conciliar la configuración predeterminada del software con sus requisitos específicos. Es obligación del cliente registrarse y/u obtener la aprobación de las autoridades competentes, si así lo exigen las leyes y normativas aplicables.
- 4.8 El cliente realiza todos los envíos en su propio nombre, bajo su marca y nada en el mensaje debe indicar que MAPP es el remitente oficial del mensaje. MAPP no está obligada ni tiene la capacidad para supervisar que los envíos cumplen las leyes, normativas y normas de buenas prácticas del sector aplicables. El cliente debe disponer de las autorizaciones, licencias y permisos necesarios para los servicios o productos promocionados a través del DMC.

#### 5. POLÍTICA DE CAPACIDAD DE ENTREGA

- 5.1 La capacidad de entrega depende de numerosos factores. MAPP trabaja con una gestión de entrega profesional y concede gran importancia a su reputación de IP. MAPP hará todos los esfuerzos comercialmente razonables y utilizará tecnología de vanguardia para garantizar la capacidad de entrega de todos los mensajes enviados a través del DMC. No obstante, el cliente acepta que la capacidad de entrega de los mensajes depende de factores que están fuera del control e influencia de MAPP y que, por lo tanto, MAPP no es responsable del éxito de la entrega.

- 5.2 La capacidad de entrega depende en gran medida de la calidad de las listas de los clientes. Por lo tanto, las listas deben cumplir los requisitos siguientes:
- Algunos ISP bloquean las direcciones que no han sido utilizadas por sus titulares durante largos periodos de tiempo y envían un mensaje de entrega rechazada durante un cierto tiempo. Posteriormente algunas de estas direcciones se convierten en trampas de correo no deseado y si se sigue escribiendo a dichas direcciones, la dirección IP o el dominio del remitente pueden quedar bloqueados. Por lo tanto, para las direcciones a las que se pretende escribir a través del software, se requiere haber obtenido el consentimiento en los dos últimos meses antes del envío inicial o que se haya escrito a esas direcciones de forma regular al menos cada dos meses.
  - Las listas deben estar limpias de direcciones que provocan entregas rechazadas. El cliente debe asegurarse de que las direcciones que causan entregas rechazadas se bloquean regularmente (cada dos meses como mínimo) o se suprimen también de sus listas antes de usar el software. La configuración predeterminada del software hace que las direcciones que provocan una entrega rechazada se bloqueen automáticamente después del primer rechazo.
  - Un envío a una lista específica no debe superar la tasa del 5 % de entregas rechazadas. La tasa de entregas rechazadas viene determinada por el cociente entre el número de entregas rechazadas y el volumen de envío total a la lista. Si una lista contiene más de un 5 % de direcciones que generan entregas rechazadas, se supone que la lista no se ha actualizado durante un largo periodo de tiempo. En la mayoría de los ISP, una tasa de entrega rechazada superior al 10 % da lugar al bloqueo o la inclusión en listas negras de las direcciones IP o los dominios del remitente afectados.
  - Un envío a una lista específica no debe superar la tasa del 3 % de quejas de correo no deseado. La tasa de quejas de correo no deseado se determina individualmente para cada ISP (participante), por el cociente entre el número de quejas de correo no deseado recibidas por un ISP específico y el volumen de envío total a ese ISP (ambos relacionados con un envío específico a una lista concreta). En la mayoría de los ISP, una tasa de quejas de correo no deseado superior al 3 % da lugar al bloqueo o la inclusión en listas negras de las direcciones IP o los dominios del remitente afectados. La obligación de limpiar las listas de entregas rechazadas de la cláusula 5.6 no se ve afectada.
  - Las listas deben cumplir criterios específicos de aceptación de calidad en las direcciones y no deben contener más de un 10 % de (i) direcciones genéricas, como tech@dominio.com o root@dominio.com, (ii) las denominadas “direcciones desechables”, que solo son válidas durante un corto periodo de tiempo y que se utilizan, entre otras cosas, para participar en sorteos de premios (como @micorreobasura.com o @correode10minutos.com), (iii) direcciones con nombres de dominio no existentes (como @lycos.es), (iv) direcciones que no son técnicamente posibles (como direcciones de correo electrónico sin la @) y (v) direcciones no permitidas en el ISP correspondiente (por ejemplo, algunos ISP exigen que las direcciones de correo electrónico contengan al menos cuatro (4) caracteres antes de la @).
- 5.3 Para optimizar continuamente la capacidad de entrega de todos los clientes, MAPP tiene derecho, aunque no está obligada a ello, a agregar las direcciones que provocan entregas rechazadas a una lista general de rebote, a fin de evitar el envío de mensajes a direcciones que previamente han generado entregas rechazadas, utilizando la lista general de rebote como una lista negra general para todos los envíos de todos los clientes.

## 6. AUDITORÍA DE LISTA Y NO CONFORMIDAD

- MAPP tiene derecho a realizar una auditoría de lista para comprobar que una lista cumple la política de conformidad y/o la política de capacidad de entrega a su entera discreción. A petición de MAPP, el cliente deberá proporcionar información detallada que demuestre que una lista cumple la política de conformidad (por ejemplo, información sobre el origen de las direcciones y el uso anterior de la lista). MAPP puede comparar una lista concreta con la lista general de rebote para identificar direcciones de dicha lista que provocarán entregas rechazadas y evaluar así la tasa potencial de entregas rechazadas de la lista.
- Con la aprobación previa del cliente, MAPP podrá realizar un envío de prueba a una lista. Los envíos de prueba se realizan a una velocidad de transmisión reducida (máximo 10.000 correos electrónicos por hora) y a un máximo del 10 % de las direcciones de la lista (pero sin superar las 50.000 direcciones).
- Cualquier infracción de la política de conformidad y/o de la política de capacidad de entrega identificada durante una auditoría de lista o un envío de prueba, o que se haga evidente durante o como resultado de un envío regular, dará derecho, aunque no obligará, a MAPP a bloquear envíos posteriores y a detener de inmediato los envíos en curso a la lista implicada. El bloqueo se limitará al ámbito de aplicación necesario para evitar más infracciones. Un bloqueo no da lugar a la reducción de los gastos. Los gastos recurrentes continuarán.
- En caso de infracción de la política de conformidad y/o de la política de capacidad de entrega, MAPP, tendrá derecho, aunque no estará obligada a ello, a reducir la velocidad de transmisión de los envíos de la lista (máximo de 10.000 correos electrónicos por hora) como alternativa al bloqueo de la lista.
- MAPP levantará el bloqueo de una lista o la reducción de la velocidad de transmisión cuando ya no se prevean más infracciones de la política de conformidad y/o de la política de capacidad de entrega. Se prevé que no se producirán nuevas infracciones tan pronto como el cliente haya proporcionado una explicación de las medidas tomadas para impedir dichas infracciones (por ejemplo, limpieza de las direcciones de la lista que provocan entregas rechazadas). El cliente puede encargar a MAPP la realización de una auditoría de capacidad de entrega. La auditoría de capacidad de entrega consiste en un análisis detallado y una limpieza de una lista con el objetivo de mejorar la capacidad de entrega y garantizar el cumplimiento de estas políticas de conformidad y de capacidad de entrega (disponible por una tarifa).
- En caso de infracciones graves o repetidas de la política de conformidad y/o de la política de capacidad de entrega, MAPP tendrá el derecho, aunque no la obligación, de asignar el sistema del cliente a un grupo de IP independiente

dedicado que puede no proporcionar el mismo nivel de reputación de IP que el grupo de IP general de MAPP, lo que puede influir negativamente en la capacidad de entrega de los envíos del cliente.

- 6.7 Una infracción grave y/o repetida de la política de conformidad y/o de la política de capacidad de entrega se considerará una violación material del contrato.
- 6.8 Para evitar dudas, el cliente será el único responsable del cumplimiento de estas políticas de conformidad y de capacidad de entrega también/incluso si MAPP realiza una auditoría de lista, una auditoría de capacidad de entrega y/o un envío de prueba y no bloquea una lista y/o levanta el bloqueo de una lista.