Email marketing CAN-SPAM compliance guidance

Classification - Internal
October 2022
v3.0

pwc

Contents

Overview **1**

What is CAN-SPAM? 2

Why is this important? 2

What is the geographic scope of CAN-SPAM? 2

When does CAN-SPAM apply? 2

Does CAN SPAM apply? **3**

1. Is PwC initiating or sending an email? 3
2. Is the email a “commercial message”? 3
3. Is the email “transactional”? 3

CAN-SPAM Content requirements **5**

Other CAN-SPAM Requirements **6**

Considering other jurisdictions & compliance frameworks **7**

PwC Global Opt-Out Program **8**

Overview

All PwC US personnel, including but not limited to those in marketing, must comply with the CAN SPAM Act and PwC's email marketing policies and procedures, as applicable.

What is CAN-SPAM?

CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act) is a US federal law that governs commercial emails and allows individuals the right to opt-out of receiving commercial emails.

Why is this important?

Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $46,517, so non-compliance can be extremely costly.

What is the geographic scope of CAN-SPAM?

CAN-SPAM is a US law and applies only to commercial emails sent to individuals located in the US. Other countries have different legal regimes that apply to sending commercial email messages. Many of these laws are more restrictive than CAN-SPAM.

When does CAN-SPAM apply?

To determine whether CAN-SPAM applies to your email communication, **please refer to the below.**

Does CAN SPAM apply?

1. Is PwC initiating or sending an email?

CAN-SPAM will apply to both emails sent directly by PwC and emails about PwC services sent by a third party (e.g., a third-party marketing agency) on PwC's behalf.

If "yes," proceed to question 2. If "no," CAN-SPAM does not apply.

2. Is the email a "commercial message"?

Under CAN-SPAM, "commercial message" is defined as any email that has a "primary purpose of commercial advertisement or promotion of a commercial product or service."

To determine the primary purpose, remember that an email can contain three different types of information:

- Commercial content – which advertises or promotes a commercial product or service, including content on a website operated for a commercial purpose;
- Transactional or relationship content – which facilitates an already agreed-upon transaction or updates a customer about an ongoing transaction; and
- Other content – which is neither commercial nor transactional or relationship.

Email contains only commercial content→ CAN-SPAM applies.
Combination emails commercial/transactional → CAN-SPAM applies.

3. Is the email "transactional"?

Emails that have a primary purpose relating to a particular transaction or relationship between PwC and a customer are not considered "commercial messages", but rather are a transactional or relational message.

To be considered a transactional or relationship message, an email's primary purpose must be to do one or more of the following:

- Facilitate, complete or confirm a commercial transaction previously agreed to by the email recipient;
- Provide warranty, product recall, safety or security information for a product used or purchased by the email recipient;
- Provide certain information regarding a subscription, membership, account, loan or similar ongoing relationship concerning the email recipient's ongoing purchase or use of PwC products or services (e.g., a notification concerning a change in the terms or features; notification of a change

to the recipients standing or status; or account balance information or another type of account statement);

- Provide information regarding an employment relationship or related benefit plan in which the email recipient is currently involved, participating or enrolled; or
- Deliver goods or services (e.g., updates or upgrades) that the email recipient is entitled to receive as a result of a previously agreed upon transaction.

Transactional/Relationship only emails → CAN-SPAM does not apply

As stated above, if an email contains both commercial and transactional/relationship content, the email should be considered to be a “commercial message” unless OGC has been consulted and advises otherwise.

CAN-SPAM Content requirements

Once a determination has been made that CAN-SPAM applies to an email communication, follow the below for CAN-SPAM compliance.

1. **Ensure that the header information is not "materially misleading":** The email's "From," "To," Reply to" and routing information should not contain false or misleading transmission information and must identify that PwC is initiating the message.
2. **Ensure the subject heading is not deceptive:** The email's subject heading should not mislead a recipient about a material fact regarding the email's content or subject matter.
3. **Clearly and conspicuously identify that the email is an advertisement or solicitation:** This identification could be placed in one of the following locations: (i) subject line; (ii) body of the email (either at the top of the page, in a text box, or otherwise set off from the surrounding text); or (iii) next to the opt-out mechanism in clearly stated and bolded lettering. Potential wording included "This is an advertisement," "This is a solicitation," or "This is a commercial email message."
4. **Include a valid physical postal address for PwC.**

Other CAN-SPAM Requirements

1. **Include a clear and conspicuous opt-out mechanism:** The opt-out mechanism can be a functioning return email address or other Internet-based mechanism (e.g., a subscriber preference portal) that the recipient may use to request not to receive future commercial messages. The opt-out mechanism should not require the recipient to: (i) pay a fee; (ii) provide information other than the recipient's email address and opt-out preferences; or (iii) take any steps other than sending a reply email message or visiting a single page on the Internet.
2. **The opt-out mechanism for an email must remain active for at least 30 days after the email is sent.**
3. **If a recipient submits an opt-out request, PwC must process the opt-out request within 10 business days of receiving the request:** When a recipient opts out of receiving emails from PwC, this opt out should never expire.

Considering other jurisdictions & compliance frameworks

- If the US knows that recipients of marketing emails are located outside the US, other compliance frameworks may apply. If you wish to launch any marketing campaigns targeting individuals known to be outside the US, please consult your Marketing contact to discuss.

PwC Global Opt-Out Program

- In 2018, PwC launched its Global Opt-Out Program and Opt-In Consent Campaign for GDPR compliance. Individuals located outside the US were given a chance to opt-in to receiving email notifications. If the individual opted-out or failed to opt-in (was passive and ignored the email), then they were added to the global suppression list, which is essentially a global list of individuals to whom email marketing should not be sent.
- Although PwC operates as a Network of Firms, this is not always clear to our clients and marketing contacts who expect PwC to act as one entity. Therefore, in order to ensure we adhere to the GDPR requirements, PwC developed a central opt-out list (also referred to as the global suppression list or marketing suppression list) of people who have explicitly stated that they do not want to receive ANY marketing communications from PwC.
- This global suppression list includes all existing explicit marketing unsubscribes from across the PwC network, as well as future unsubscribes.

  The global suppression list is maintained in SalesForce Marketing Cloud ("SFMC"). The Explicit Marketing Consent field is used to capture an individual's marketing consent.



If a US individual/team or individual is using SFMC to compile their email recipient list, the SFMC system will look to the appropriate field(s) mentioned above and not include any contacts who would have been added to the global suppression list (i.e. opted-out or has not provided marketing consent.) The list the team/individual generates will not "pull" individuals marked as do not contact.



If a US individual/team compiles a marketing list outside of SFMC, there is no mechanism to identify contacts who have opted-out or not provided consent.

Individuals/teams should only compile marketing lists using SFMC. This will ensure any individuals (i.e. contacts) who have opted-out or not provided consent will not be added to such contact lists. Additionally, SFMC provides an audit trail for opt-outs and marketing consent choices. Using any other mechanism (e.g. a self managed list) is not in line with US Marketing team guidance. Additionally, this presents risk to the firm by potentially sending marketing communications to individuals who have explicitly stated they do not want to receive marketing communications.

© 2022 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.