M³AAWG Support Document

The GDPR and ESP Suppression Lists

December 2024

When the client of an Email Service Provider (ESP) requests that an email be sent on their behalf to an email address list, the ESP may use suppression lists to ensure, for a variety of reasons, that no email is sent to particular addresses. This document helps ESPs understand how the European Union's General Data Protection Regulation (GDPR) may affect their processes for handling email addresses on these suppression lists.

This document is not intended to provide legal advice. It is intended to provide useful background information when considering the use of suppression lists by ESPs. Specific legal questions should be referred to your general counsel or other legal entity.

Definitions

A "Data Controller" is any "body which, alone or jointly with others, determines the purposes and means of the processing of personal data…." (Article 4(7), GDPR).

A "Data Processor" is any "body which processes personal data on behalf of the controller…." (Article 4(8), GDPR).

Background

Email addresses are generally considered personal data. There are exceptions – generic role addresses (info@example.com, for example), or generic addresses used for replies (lotteryentry@example.com, for example) – but it is best to design systems on the assumption that all of the email addresses involved are personal data. In particular, the domain itself may in some circumstances be very likely to be considered personal data, such as js@john-smith.example.com.

To be a "Data Processor" is to process personal data on behalf of a Data Controller. Of the two roles, the processor has less risk or liability for the processing – provided it can show it has followed the controller's instructions and did not process data for any purpose by any means that went beyond what the controller determined.

Under the GDPR, each act of data processing for personal data requires a legal basis. For ESPs acting as Data Processors, the legal basis for sending email to an email address on behalf of their clients will be their contract with that client (Article 6(1)(b) of the GDPR). ESPs can also suppress non-personal data (such as known spam traps) without engaging the GDPR.

When using their own suppression list to avoid sending email to addresses which the client instructed them to process, the ESP risks taking an action which is contrary to their contract with the client to act "on their

behalf." The GDPR definitions mean that this action would move the ESP into the role of "determining the purposes and means of the processing of personal data" – that is, they have become a Data Controller.

Suppression lists

Address suppression arises in the normal course of ESP operations. However, the method or specific act of suppression can happen through a variety of circumstances or can be driven by different events including:

1. Invalid addresses
   An address might be invalid because the top-level domain does not exist, e.g., "example.con." It is common for ESPs to prevent further emailsfrom being sent to that domain, by any client.

2. Addresses likely to be invalid
   An address might be valid, but experience shows that the domain is unlikely to be what was intended due to a common misspelling or typo, e.g., "hotmail.com" being misspelled as "hotmial.com." ESPs may prevent email from being sent to that domain.

3. Country code suppression
   An address within a domain associated with a country might be valid, but it is inappropriate or unwise to send emails about particular topics to citizens of that country. For example, there may be a sanctions regime operating, or activities such as gambling may be subject to country-specific legislation. This is a matter for each ESP to assess, given their knowledge of country-specific domains and the circumstances that may or may not indicate that recipients are within that associated country; it is likely that .de for Germany would be treated differently to .tv for Tuvalu.

4. Disposable addresses
   The address may be valid but is recognized to be a single-use address, and hence further email is bound to be rejected. Note that suppression of an address, when the contract with a customer does not envision this, may result in the ESP being found to have taken on the role of Data Controller.

5. Role addresses
   The address may be recognized as a role address (for example, noreply@example.com), and the nature of the email to be sent is inconsistent with the intended use of that role address. This is a matter for each ESP to assess on a case-by-case basis, as some role addresses may be considered personal data, being directly assignable to known individuals.

6. Email delivery failures
   It may be that the address has failed to be deliverable to in the past – that is, the mail server refuses to accept delivery. The associated error message may shed some light on why this occurs; for example, the email address may not exist, the destination mailbox may be "full," or the content of the email may be deemed unacceptable. Where the failure is very likely to recur for a given email (or for a given type of message) then no further attempts may be made to deliver.

7. Bounce messages
   Even though email was apparently successfully delivered in the past, a subsequent bounce message may have been received which indicated that delivery failed. Analyzing the reason for the bounce may mean that no further attempts are made to deliver to the particular email address.

8. Feedback loop info
   Some mailbox providers make feedback information available which may reveal whether email was placed into a spam folder or marked as spam by the recipient. This information may indicate that further delivery to an email address should be suppressed.

9. Opening / engagement information
   Some ESPs "instrument" email with a view to learning whether recipients have engaged with the email. A lack of engagement over time may cause an ESP to add the relevant email address to a suppression list.

10. Requests to unsubscribe
    The ESP may receive requests for no further email to be sent. These may be hand-crafted requests, but more commonly arise as a result of the recipient clicking on relevant links within the email, or their email client making use of "unsubscribe" information in email headers. Further email to such an address needs to be suppressed.

11. Abuse complaints
    The ESP may receive correspondence from an email recipient from which the conclusion can be drawn that further email from the same sender is not wanted.

12. Known spam trap addresses
    The ESP may be aware that a particular email address is in fact a spam trap, and that sending email to it will cause the reputation of their sending IP, sending domain, etc., to be adversely affected, making deliveries to other email addresses more difficult or indeed impossible. Hence the ESP may suppress such addresses.

13. Requests to be forgotten
    An ESP may receive a request to be "forgotten" by a data subject living in a territory governed by GDPR or a similar regulation, or instructing that their personal data should no longer be processed.

The GDPR and Suppression Lists

Suppression lists can be operated on a per-client basis, in which case they are more than likely composed of people who have marked messages from a specific sender as spam, who have specifically requested to unsubscribe, or from whose email address email has bounced. It is possible to operate such lists and continue to be just a Data Processor.

The contract between the ESP and their client should make clear how this type of suppression will work in practice. When a bounce occurs, will the ESP keep track of this on behalf of the client, or is the client

expected to update their list themselves? When the contract term ends, how will the client (the Data Controller) learn about any unsubscribe requests that have been received? These are requests that they are obliged to honor even when sending via another ESP.

ESPs may view the operation of global rather than per-client suppression lists as essential for them to remain in business. It may become difficult to provide a good service to any client, if clients ask ESPs to send to spam trap addresses or to recipients who regularly send abuse complaints.

The suppression of objectively invalid addresses (i.e. those which cannot possibly be valid) does not involve any personal data being processed outside the purposes of the ESP's contract, but many of the other events described above will.

Removing an email address because its owner is known to be deceased does not involve personal data because the dead do not have rights under GDPR.

If personal data is being processed by the ESP in a manner that does not fit within the Data Processor arrangements with each client, then the ESP will have become a Data Controller and must operate accordingly. This document does not cover the details of Data Controller requirements, but the UK Information Commissioner's Office (ICO) provides a helpful checklist of areas of compliance which would be a good starting point to understand what is required:
https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/controllers-checklist/

In some circumstances, it will be clear that personal data is being processed in a manner that goes beyond the role of a Data Processor. This is very likely to be the case if the ESP maintains its own suppression list and uses it to prevent the delivery of email to specific addresses, suppressing email addresses of individuals that are antagonistic to the ESP's business, for example, or the addresses of role accounts, trap domains, known hard bounces, and so forth.

It should be noted that various data protection complications will occur if an ESP takes actions that have not been requested by their client. Thus, if an ESP operates a global suppression list, then the contract with the client should cover the way in which it is applied, and hence how the client can meet their own obligations as a Data Controller.

Questions about whether you are a Data Processor or a Data Controller or how the GDPR applies to you should be referred to your legal counsel. As noted above, this Support Document is not intended to provide legal advice.