What is a feedback loop and when can it be used by mailbox providers?

1. Definition:

A feedback loop is a technical service provided by mailbox providers that reports back spam clicks from email recipients to the sender. This function is used when a recipient clicks on the “spam button” in the interface of his or her email account to complain about receiving an email from the mailbox provider.

The aim of this service is to improve the quality of email traffic in the long term and to let the sender know which content or practices are considered negative by the target group based on the negative feedback from the recipients. Senders of bulk emails should take this feedback into account to ensure long-term deliverability and improve email reputation.

Not all mailbox providers offer this service and a sender must also register for a provider's feedback loops using the domains and IPs.

2. Technical requirements for registration

- The sender must have administration rights for the IP/domain
- Postmaster@ and Abuse@ must be set up and managed by the sender
- The ReverseDNS of an IP must validly resolve to the domain used
- Registration often requires a good reputation with the mailbox provider
- DKIM should be used and set up for authentication

3. Automatic processing of feedback loop messages

The complaint notification contains a legible part, as well as a machine-readable part for automatic processing for the complaint contact with the sender.

For automatic processing of feedback loop messages, the sender needs a script that retrieves and parses the incoming messages from the Postmaster@ or Abuse@ inbox to extract the necessary elements and information for further processing.

A complaint is sent as an email to the Postmaster@ or Abuse@ email address of the sender in Abuse Reporting Format (ARF). It contains necessary information, such as header details of the original message in question.

Abuse Reporting Format – ARF

An ARF complaint message corresponds to the MIME type of a bounce message and is defined in RFC 3462.

The main components of an ARF complaint message are the *feedback type* and the email header of the email that a recipient is complaining about. In the case of a spam complaint, the feedback type is mainly *abuse*, but may also contain *fraud, virus* or *other*.

In the transmitted email header, the recipient data should be made unrecognizable in order to exclude direct personal reference, but the other transmission and traffic data, such as additional X headers or other individual tags, are included. By reporting the email header back to the sender, the sender is then able to process the spam complaint based on their own individual IDs.

The mailbox provider…

...transmits the complete email header of the sender in ARF to the respective abuse desk and removes the email address of the original recipient. Thus, no personal data will be processed or disclosed by the email transmission.

The sender…

...takes the spam complaint message and processes it. The sender's individual X headers, which are contained in the transmitted email header, allow the spam complaints to be evaluated internally again and the recipient to be removed from the email lists.

Example of an ARF message:

```
From: <abusedesk@example.com>
Date: Thu, 8 Mar 2005 17:40:36 EDT
Subject: FW: Earn money
To: <abuse@example.net>
MIME-Version: 1.0
Content-Type: multipart/report; report-type=feedback-report;
     boundary=“part1_13d.2e68ed54_boundary”

--part1_13d.2e68ed54_boundary
Content-Type: text/plain; charset=“US-ASCII”
```

```
Content-Transfer-Encoding: 7bit

This is an email abuse report for an email message received from IP
192.0.2.2 on Thu, 8 Mar 2005 14:00:00 EDT. For more information
about this format please see http://www.mipassoc.org/arf/.

--part1_13d.2e68ed54_boundary
Content-Type: message/feedback-report

Feedback-Type: abuse
User-Agent: SomeGenerator/1.0
Version: 1
Original-Mail-From: <somespammer@example.net>
Received-Date: Thu, 8 Mar 2005 14:00:00 EDT
Source-IP: 192.0.2.2
Authentication-Results: mail.example.com
               smtp.mail=somespammer@example.com;
               spf=fail
Reported-Domain: example.net
Reported-Uri: http://example.net/earn_money.html

--part1_13d.2e68ed54_boundary
Content-Type: message/rfc822
Content-Disposition: inline

From: <somespammer@example.net>
Received: from mailserver.example.net (mailserver.example.net
     [192.0.2.2]) by example.com with ESMTP id M63d4137594e46;
     Thu, 8 Mar 2005 14:00:00 -0400
To: <Undisclosed Recipients>
Subject: Earn money
MIME-Version: 1.0
Content-type: text/plain
Message-ID: 8787KJKJ3K4J3K4J3K4J3.mail@example.net
Date: Thu, 2 Sep 2004 12:31:03 -0500

Spam Spam Spam
Spam Spam Spam
Spam Spam Spam
Spam Spam Spam
--part1_13d.2e68ed54_boundary--
```

4. Legal requirements for the transfer of feedback loop data from the mailbox provider to the sender

a.) Context:

In this case, the General Data Protection Regulation (GDPR) of the European Union (EU) applies. It regulates the processing of personal data of natural persons by natural persons, companies or organisations in the EU. It has been in force since May 2018. This means that companies that do not have a branch in the EU, but are active on the European market are also obliged to apply the provisions of the GDPR.

b.) What data can be passed on on the basis of the GDPR by means of feedback loops?

The linchpin for the permissibility of sharing data is first of all whether the data is personal data. If this is the case, the consent of the email recipient must always be obtained.

c.) Conclusion:

Since the information forwarded by the mailbox provider to the sender in the procedure described here is not personal data as defined in Article 4 paragraph 1 of the GDPR, in this case it is possible to dispense with informing the email recipient and obtaining consent for the purpose of forwarding the data. We therefore consider this procedure to be legally unobjectionable from a data protection point of view in our interpretation of the provisions of the GDPR.

Authors:
Astrid Braken, Legal Counsel
Sebastian Kluth, Technical Lead CSA