PROOFPOINT EMAIL FRAUD DEFENSE (EFD) & THE GDPR

HOW EFD CAN ASSIST CUSTOMERS TO COMPLY WITH THE EU GDPR

Version January 12, 2018

INTRODUCTION

On 25 May 2018, the most extensive and far-reaching piece of European data protection legislation will come into force—the European Union's (EU's) General Data Protection Regulation (GDPR) will replace the 1995 European Union Data Protection Directive.

At its core, the GDPR aims to put EU residents in control of their personal and sensitive data. It regulates how their data is collected, processed, stored, deleted, transferred, and used. Any company that does business in the EU or handles the personal data of EU residents is obligated to comply with the regulation.

This applies to all companies processing personal data of EU residents—even companies that do not have physical operations in the EU. For any company collecting personal data on people located in the EU or for any company doing business in the EU, GDPR compliance is mandatory. Regardless of where data is processed, the GDPR requires that personal information be protected.

Learn more about the GDPR.

Developing a plan to comply with the new rules is critical for all organizations, including Proofpoint. Proofpoint is committed to compliance with the GDPR across our solutions and services. As a data processor, we maintain the privacy and confidentiality of the personal data entrusted to us.

Proofpoint Email Fraud Defense (EFD) is offered as a cloud-based service. This document details how Proofpoint's EFD solution complies with key principles of the EU GDPR.

GDPR MANDATES NEW CONTROLS

PROOFPOINT EMAIL FRAUD DEFENSE

Proofpoint's Email Fraud Defense ("EFD") monitors and analyzes Domain-based Message Authentication, Reporting & Conformance ("DMARC") aggregate and forensic reports to inform customers how and when to block malicious emails spoofing customers' domains. Email Fraud Defense provides visibility into the emails spoofing customers' domains, and helps customers take control of their email channel by enabling customers to enforce blocking policies at mailbox providers.

Powered by the cloud, Proofpoint's solution can be deployed right away and adapts as threats evolve. Businesses can maintain trust, ensure compliance and safeguard the security of EU personal data with our advanced cybersecurity solution.

You can find out more about EFD on our corporate website.

To deliver EFD, Proofpoint processes personal data embedded in emails. Personal data processed includes:

- Names
- Email addresses
- IP addresses
- *NOTE: Personal data may also be included in email subject lines, email body headers, URLs, message IDs, and attachment names*

Recital 49 of the GDPR says every data controller has a legitimate interest in "the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services.... This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems."

Proofpoint's EFD service is a powerful tool for customers (data controllers) to protect the authenticity, integrity and confidentiality of personal data.

DATA TRANSPARENCY

Right to Access: The primary purpose of EFD is to protect our customers' employees and anyone who may receive email from our customers' employees from malicious attacks. Those employees located within the European Union are data subjects under the GDPR. Authorized users from customer organizations can access relevant records that include personal data about their employees, customers and partners which are processed by Proofpoint from the EFD dashboard.

DATA TRANSFERS

We are part of the EU-US Privacy Shield and Swiss-US Privacy Shield frameworks that facilitate transfers of personal data of the US and the EU and between the US and Switzerland.

In addition, Proofpoint willingly enters into contract commitments in the form of data processing agreements (aka Model Clauses or EU Standard Contractual Clauses (SCCs)). Proofpoint commits to updating and maintaining new versions of the data processing agreements to include GDPR relevant provisions.

DATA PROCESSING

1. THE FIRST DATA SOURCE PROCESSED BY EMAIL FRAUD DEFENSE IS DMARC DATA.

This data is sent to Proofpoint from DMARC compliant email servers worldwide. This list includes most major consumer mailbox providers such as AOL, Google, Microsoft and Yahoo, as well as a growing number of private corporations and emailing receiving entities on the internet.

Co-developed by a consortium of mailbox providers and security vendors, the DMARC specification became an internet standard in March 2015. DMARC aims to put an end to domain-based consumer email threats. By leveraging existing email authentication technologies (SPF and DKIM), DMARC enables senders to instruct mailbox providers to monitor, quarantine or reject any email that fails authentication. DMARC authentication failures and forensic data help reduce the time to detect email fraud and close down phishing attacks.

Although DMARC is a public standard, Proofpoint's Email Fraud Defense solution shows the result of DMARC reporting in a format that is easy to read and understand so that senders can focus on making important policy decisions on a domain by domain basis. Proofpoint also analyzes and extracts data from the reports to identify trends, phishing outbreaks, authentication failures, and authentication failure resolutions.

Figure 1:
Sample DMARC Record

```
v=DMARC1\; p=none\; fo=1\;
rua=mailto:dmarc_rua@emaildefense.proofpoint.com\;
ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com\;
```

DMARC consists of two types of data, aggregate reports and individual forensic messages. When a sender configures their DMARC record, two Proofpoint email addresses are added to the record to receive forensic and aggregate reports:

- dmarc_rua@emaildefense.proofpoint.com for the aggregate reports
- dmarc_ruf@emaildefense.proofpoint.com for forensic reports

Assuming an example where a DMARC failed email is going from Client.Address@clientdomain.com to recipient@gmail.com, the Proofpoint email addresses

instruct the recipient mailbox provider (Gmail in our example) to forward failed DMARC emails to Proofpoint, instead of sending the email on to the original recipient@gmail.com. As such, Proofpoint is now receiving failed messages directly from Gmail's mail servers.

DMARC data is sent to Proofpoint in the form of Aggregate Reports and Forensic Reports.

DMARC Aggregate Reports

Aggregate reports reveal what messages passed and failed DMARC authentication. Aggregate reports are daily rollups of all email traffic for a Header From domain. DMARC aggregate reports consolidate data by sending IP, Mail From domain, DKIM domain, SPF result and DKIM result. In addition, DMARC aggregate reports indicate whether or not a DMARC policy was applied. DMARC aggregate reports contain:

- The DMARC policy discovered and applied (if any)
- The SPF and DKIM identifiers and results
- SPF and DKIM alignment data
- Data for sub domains, sending domains, and receiving domains
- The policy requested by the domain owner, and the policy applied
- Counts for all successful authentications
- IP addresses of the sender

DMARC Forensic Reports

Where DMARC aggregate reports paint a broad picture of email traffic, DMARC forensic reports detail an individual email that failed one or more DMARC checks. Forensic Reports are generated almost immediately after detecting DMARC authentication failures and will contain some or all original headers and either empty email bodies or full emails depending on the policy of the Internet Service Provider (ISP)/electronic mailbox provider supplying the DMARC report (the "Report Generator"). DMARC forensic reports contain:

- Message-level data that may include Personal Data
- To and From email addresses
- IP addresses of the sender

The DMARC failed emails which Proofpoint receives to the @emaildefense.proofpoint.com address fit two typical scenarios:

- Phish attempts against client's customers: These are not legitimate messages; they are attempts by fraudsters and scammers to pose as the client. Mailbox providers like Google, Yahoo! and Microsoft are forwarding these messages to Proofpoint for action; clients get visibility, and the ability to take action on this malicious traffic, where they were previously blind.
- Legitimate messages sent from misconfigured client servers: These are legitimate emails our clients send to their customers. We receive these emails because they are failing DMARC. One of the value propositions we offer is that we expose these messages to clients' IT and security administrators, so they can work to fix authentication issues and wrangle their outbound email under control.

Figure 2:
Personal Data Embedded In Example Forensic Report Highlighted

```
Feedback-Type: auth-failure
User-Agent: XMR/2.2
Version: 1.0
Original-Mail-From: <return@proofpoint.com>
Arrival-Date: Wed, 18 Nov 2015 04:20:39 -0800
Message-ID: <SNT004-MC4F21APDVXL000271ed@SNT004-MC4F21.hotmail.com>
Authentication-Results: hotmail.com; spf=fail (sender IP is 142.4.4.231; identity
alignment result is pass and alignment mode is relaxed)
smtp.mailfrom=return@proofpoint.com; dkim=none (identity alignment result is pass
and alignment mode is relaxed) header.d=proofpoint.com; x-hmca=fail
header.id=editor@proofpoint.com
Source-IP: 142.4.4.231
Auth-Failure: spf
Reported-Domain: proofpoint.com
DKIM-Domain: proofpoint.com

--5176ED31-B2FA-4738-81AC-2ECDEE6CCCDA
Content-Type: message/rfc822
Content-Disposition: inline

Authentication-Results: hotmail.com; spf=fail (sender IP is 142.4.4.231; identity
alignment result is pass and alignment mode is relaxed)
smtp.mailfrom=return@proofpoint.com; dkim=none (identity alignment result is pass
and alignment mode is relaxed) header.d=proofpoint.com; x-hmca=fail
header.id=editor@proofpoint.com
X-Envelope-Sender: return@proofpoint.com
X-SID-PRA: editor@proofpoint.com
X-AUTH-Result: FAIL
X-SID-Result: FAIL
Received: from glennihus.com ([142.4.4.231]) by SNT004-MC4F21.hotmail.com with
Microsoft SMTPSVC(7.5.7601.23143);
        Wed, 18 Nov 2015 04:20:39 -0800
Date: Wed, 18 Nov 2015 07:20:33 -0500
To: "REDACTED" <postmaster@outlook.com>
From: tefst<editor@proofpoint.com>
MIME-Version: 1.0
Content-Type: text/plain; charset="ISO-8859-1"
Content-Transfer-Encoding: 8bit
Subject: This is an email ssv3779 [142.4.4.231]
Content-Type: text/html;
Return-Path: return@proofpoint.com
Message-ID: <SNT004-MC4F21APDVXL000271ed@SNT004-MC4F21.hotmail.com>
```

2. THE SECOND DATA SOURCE PROCESSED BY EMAIL FRAUD DEFENSE IS COMMERCIAL DATA.

Proofpoint has relationships with multiple data partners with access to mailbox providers, internet service providers, and the sending community across the globe. This is a diverse network which provides a variety of data formats. Below is an exhaustive list of the types of commercial data processed by Proofpoint's Email Fraud Defense product.

Abuse Reporting Format (ARF)

Mailbox providers use this standard to share individual user complaint reports with senders and commercial data providers via a domain or IP based feedback loop.

- This Is Spam (TIS): Some mailbox providers share user TIS complaint reports in order to help senders pinpoint problems with their mail program and improve their list hygiene. There are different formats for providing these reports. Some mailbox providers share the full message and email address of users who complained, while others provide only partial messages.
- This Is Not Spam (TINS): TINS rates, or how often subscribers 'rescue' messages from their spam folders, send clear signals to mailbox providers, revealing which senders and brands consumers most want to hear from. Some mailbox providers share the full message and email address of users who complained, while others provide only partial messages.

Spam Trap Data

A spam trap network is a collection of user email accounts that are designed to catch spam or fraudulent email by way of not publishing or providing the destination mailbox's email address. Any messages received at these unpublished mailboxes are typically fraudulent in nature. This data type is referred to as spam trap feeds. Spam traps come in two flavors: pristine and recycled; one is more hazardous than the other.

- A pristine spam trap is an email address that has been fabricated by either a mailbox provider or blacklist. It is placed in an impossible location and can only be obtained by a bot that is crawling for email addresses. If a sender sends to a pristine trap, their IP reputation will drop and blocking of mail will commence.
- Recycled spam traps are far less impactful on one's sending reputation. Recycled spam traps are old addresses that subscribers have abandoned and the mailbox provider has taken back to use as a trap. The mailbox providers then sit, waiting and watching, to see which sender will send to an address that has not responded to an email. Sending to a recycled spam trap is indicative to mailbox providers of a sender that's not practicing proper list hygiene.

Customer Provided Data

Many customers agree to forward the contents of their Corporate Abuse mailboxes to Proofpoint for analysis. An example would be an abuse@ feed provided by a bank or ecommerce website. This type of data varies from full forwarded messages to hand edited forwarded messages.

DATA SECURITY & PRIVACY

DMARC, as an internet standard published by the Internet Engineering Task Force (IETF) and its global parent organization the Internet Society (ISOC), recognizes the risks to Personal Data of sharing email data, as indicated in Section 9 of the Request for Comment (RFC) 7489. Because DMARC data (aggregate and forensic reports) can be authorized to a third party via the inclusion of a ruf or rua record, it is the expectation that the third party is trusted by the owner of the Header From domain publishing the DMARC record. As the trusted third party, Proofpoint has access to both aggregate and forensic level data within DMARC reports. Some of these reports contain sender IP addresses, email addresses, and other Personal Data found in email.

Aggregate reports do not contain email addresses, email message bodies, header information or message body content, but do contain IP addresses of the sender which is considered private data in the EU. No email message body or header information is included in this data. The IP addresses in aggregate reports are those of the originating Message Transfer Agent (MTA). While people can run their own MTA, the vast majority of email is sent via MTAs that act as gateways or relays for email from many individual senders.

DMARC forensic reports will contain some or all original Headers (including the To and From email addresses), IP address of the sending email server and either empty email bodies or full message-level data depending on the policy of the DMARC Report Generator. Section 3.1 of RFC 6591 highlights the possible need for DMARC Report Generators to redact Personal Data from either the email headers or body. In short, RFC 6591 defers to yet another document, RFC 6590 for further clarification. RFC 6590 highlights best practices for data transformation in order to preserve the value of data and not expose Personal Data unnecessarily.

Local policy at each DMARC Report Generator will ultimately determine the amount and type of Personal Data included in DMARC aggregate and forensic reports. Section 3.1 of RFC 6591 provides detail on the protection mechanisms and controls Proofpoint has put in place to protect Personal Data and prevent inadvertent and / or unauthorized access to personally identifiable information.

Proofpoint has implemented technical and administrative controls to protect the integrity and confidentiality of personal data against accidental or unauthorized loss, alteration, destruction, or access.

Control	*Description*
Redaction	The DMARC specification does not have a policy requiring Report Generators to redact Personal Data. How Report Generators handle Personal Data varies; Personal Data is often redacted by Report Generatorsfrom DMARC reports and emails before transfer to Proofpoint. However, not all Personal Data is redacted by the Report Generators, for example, IP addresses remain in Proofpoint reports displayed in the portal. Through custom Proofpoint software, the Email Fraud Defense product, redacts all emails addresses found in the To field by masking the user

	identifying part and removes all message body data with the exception of URLs, prior to data display in the portal.
Encryption	Proofpoint supports Transport Layer Security (TLS); all transmissions of data to Proofpoint's infrastructure can be encrypted through the TLS protocol. However, it is up to the Report Generator to make use of this mechanism. DMARC reports are sent to us in whatever state the Report Generators deems appropriate but should they decide to send data in encrypted format, Proofpoint can support that. Once we receive DMARC data from the Report Generators, all data in transit within Proofpoint's infrastructure is encrypted. Email Fraud Defense infrastructure is deployed in AWS, all data stored in the cloud is encrypted at rest and only Proofpoint has access to the key.
Deletion	All data stored within the Proofpoint infrastructure has Time to Live (TTL) values associated with. After 90 days data is pruned from the product by either automatic TTL deletions or scheduled manual jobs. Secure data backups exist for research purposes and may use longer term TTLs for deletion.

Access controls mechanisms are established for physical and logical access to the facilities and the infrastructure hosting the services. All physical and logical access is logged and analyzed for inappropriate access. Proofpoint only permits access to the facilities and services hosting personal data to those employees whose role requires it. Physical and logical access authentication by Proofpoint personnel is performed using two-factor authentication and is granted based on the employee's role.

Physical security controls for the facilities hosting the services include 24x7 on-site security, local and remote security monitoring, and redundant power and environmental controls.

STANDARDS AND CERTIFICATIONS

Our datacenters are designed with market-leading security and privacy capabilities. Our North American co-location facilities perform annual SOC 1 or SOC 2 audits and European co-location facilities maintain ISO 27001 certifications. We have a documented Information Security Program designed to ensure that adequate technical and administrative security controls are implemented to protect personal data and the physical locations in which it is hosted.

Proofpoint engages a third-party auditor to perform an annual SOC2 Type II Report that includes the Proofpoint Email Protection service. The audit is performed for the Availability, Confidentiality and Security Trust Principles.

Proofpoint has implemented a Continuous Monitoring program to ensure that security controls remain in place and effective between the annual SOC 2 audits.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats. www.proofpoint.com

Version January 12, 2018