PROOFPOINT TARGETED ATTACK PROTECTION (TAP) & THE GDPR

HOW TAP 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 Targeted Attack Protection (TAP) is offered as a cloud-based service. This document details how Proofpoint's TAP solution complies with key principles of the EU GDPR.

GDPR MANDATES NEW CONTROLS

PROOFPOINT TARGETED ATTACK PROTECTION

According to the Verizon Data Breach Report, 75% of data breaches are perpetrated by outsiders. And an estimated 91% of all cyber-attacks occur through email; that's why securing this channel is critical.

Proofpoint Targeted Attack Protection (TAP) helps detect and mitigate advanced threats that target people through email. We detect both known and new, never-seen-before attacks that use malicious attachments and URLs to install malware on a device or trick users to share their passwords or other sensitive information. TAP is unmatched in stopping targeted attacks that use polymorphic malware, weaponized documents, and credential phishing to access sensitive information or steal money.

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 TAP on our corporate website.

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

- Names
- Email addresses
- Passwords
- IP addresses
- Location data
- *NOTE: Personal data may also be included in email subject lines, email body headers, URLs, message IDs, attachment names, and attachments (such as .DOC and .DOCX files)*

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 damage to computer and electronic communication systems."

It is clear that the data of customers and data subjects is safer when secured by an advanced malicious detection service such as Proofpoint's Targeted Attack Protection because up to 90% of targeted email attacks against customers who do not use TAP reach their intended victims (potentially resulting in the breach, loss and theft of personal data). It is Proofpoint's belief that our TAP service helps customers achieve the aims of the GDPR through securing and protecting individuals' privacy in their personal data, and both customers and the data subjects whose

personal data they handle are better protected when using a service such as Proofpoint's Targeted Attack Protection.

DATA TRANSPARENCY

Right to Access: The primary purpose of TAP is to protect 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 TAP 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

As the data processor, Proofpoint largely only processes personal data on behalf of the data controller (our customers); where Proofpoint processes personal data on behalf of data controllers, it does so on written authorization from the data controller (i.e. through a contract). In addition, we only process personal data necessary to deliver our TAP services. The personal data processed on behalf of the data controller will be accurate, complete, and kept up-to-date as much as technically possible.

TAP stops and prevents future malicious attacks through its forensic analysis of malicious URLs and attachments. In order to provide this service and protect both the customer's data and data subjects' privacy it is necessary for some personal data contained within those malicious messages be retained up to 18 months (or longer in the case of metadata from message log files such as sender and recipient email addresses) and then deleted in accordance with Proofpoint's data retention policies.

DATA SECURITY & PRIVACY

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

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.

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

Wherever applicable Proofpoint deploys encryption and hashing to protect personal information. Attachments in the Attachment Store, where personal data may be at rest, is encrypted using unique AES-256 encryption keys. Data in Transit is encrypted using a TLS session encrypted with a 2048-bit RSA asymmetric key. Proofpoint also provides organizations tools to limit some data collections.

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 has implemented a Continuous Monitoring program to ensure that security controls remain in place and effective at all times.

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