proofpoint.

www.proofpoint.com

PROOFPOINT EMAIL PROTECTION & THE GDPR

HOW EMAIL PROTECTION CAN ASSIST CUSTOMERS TO COMPLY WITH THE EU GDPR

Version January 12, 2018

Proofpoint is not in the business of providing legal counsel and this document is not to intended to provide, and should not be construed as, legal advise.

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.

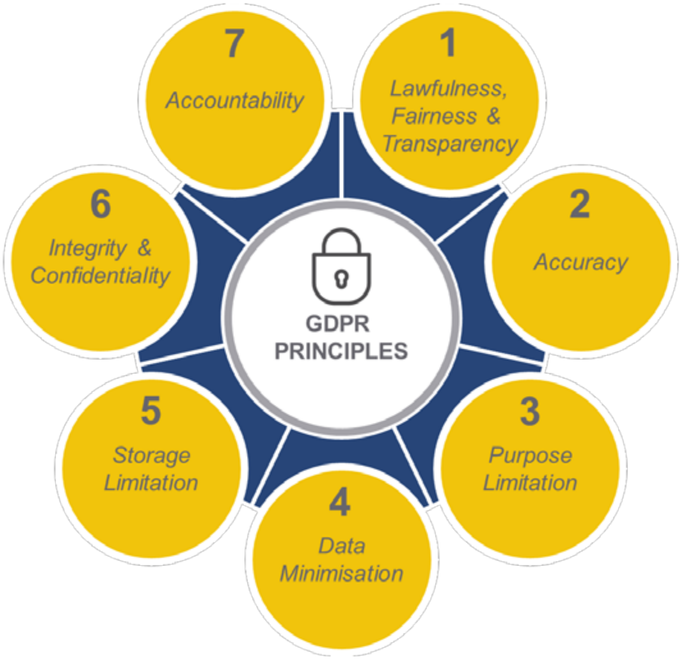
This applies to all companies processing personal data of EU residents—even companies that do not have physical operations in the EU. For any company collecting personal data on people located in the EU or for any company doing business in the EU, GDPR compliance is mandatory. Regardless of where data 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 Protection is offered as an on-premise appliance or as a cloud-based service. This document details how Proofpoint's cloud-based Email Protection solution complies with the seven key principles of the EU GDPR.

GDPR MANDATES NEW CONTROLS



Version January 12, 2018

Proofpoint is not in the business of providing legal counsel and this document is not to intended to provide, and should not be construed as, legal advise.

PROOFPOINT EMAIL PROTECTION

Proofpoint Email Protection helps organization secure and control inbound and outbound email. It stops malware and non-malware threats such as phishing, impostor email, and business email compromise (BEC) attacks. Deployed as a cloud service, it provides granular filtering to control bulk "graymail" and other unwanted email. And business continuity capabilities keep email communications flowing, even when email servers fail. Proofpoint Email Protection provides the tools organizations need to keep their employees safe from email threats. You can find out more about Email Protection on our corporate website.

To deliver Email Protection, 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, and attachment names*

The purpose of data collection is limited to providing or enhancing the protection capabilities of the solution.

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.” It is Proofpoint’s belief that our Email Protection service achieves the aims of the GDPR to secure and protect individuals’ privacy in their personal data, and both data subjects and our customers are bettered secured when protected by Proofpoint’s Email Protection.

DATA TRANSPARENCY

Right to Access: The primary purpose of Email Protection is to protect employees from email-borne threats. Authorized users from customer organizations can access relevant records from an easy to use console.

Proofpoint is not in the business of providing legal counsel and this document is not to intended to provide, and should not be construed as, legal advise.

Right to be Forgotten: Authorized users from customer organizations can delete user records from the admin console. As an example, if an employee leaves the customer's organization, authorized administrators can delete that user's records.

Proofpoint will make available to the data controller information that may assist the data controller in demonstration its compliance with the GDPR.

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 only processes personal data on behalf of the data controller (our customers) and on written authorization from the data controller (i.e. through a contract). In addition, we only process personal data necessary to deliver our Email Protection 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.

Proofpoint only stores personal data for the duration of the contract with the data controller, with the following exception: any email caught by the Email Protection detection service as potentially containing malicious content may be retained for up to 15 months (or longer in the case of metadata from message log files), after which time it may be automatically deleted from our service. The length of time data is retained by Proofpoint is due to the fact that in order to provide our valuable Email Protection 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 (and in rare cases the entire email that contains malicious content may be retained).

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 monitoring, and redundant power and environmental controls.

Proofpoint is not in the business of providing legal counsel and this document is not to intended to provide, and should not be construed as, legal advise.

Wherever applicable Proofpoint deploys encryption and hashing to protect personal information. The customer's Email Quarantine, where personal data may be at rest, may, at the data controller's discretion, be encrypted using a unique AES-256 encryption key. Data in Transit, may at the data controller's discretion be encrypted using a TLS session encrypted with a 2048-bit RSA asymmetric key. Proofpoint also provides organizations tools to limit the data collected. For example: organizations can choose to disable collection of traffic statistics.

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

Proofpoint is not in the business of providing legal counsel and this document is not to intended to provide, and should not be construed as, legal advise.