PROOFPOINT CLOUD APP SECURITY & THE GDPR

HOW CLOUD APP SECURITY ENABLES CUSTOMERS TO COMPLY WITH THE EU GDPR

Version July 25, 2019

INTRODUCTION

On 25 May 2018, the most extensive and far-reaching piece of European data protection legislation came into force—the European Union's (EU's) General Data Protection Regulation (GDPR) replaced 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 Cloud App Security solutions, including TAP SaaS Defense, Cloud Account Defense and Cloud App Security Broker, are offered as cloud-based services. This document details how Proofpoint's Cloud App Security solutions comply with key principles of the EU GDPR.

PROOFPOINT CLOUD APP SECURITY

Cloud apps are changing the way people collaborate and run their businesses. But cloud apps introduce new security and privacy risks. In a recent six-month study of major cloud service tenants, Proofpoint found that:

- 72% of tenants were targeted at least once by threat actors
- 40% of tenants had at least one compromised account in their environment.

Proofpoint Cloud App Security solutions protect organizations from advanced threats, oversharing of sensitive data and compliance risks in the cloud. We provide a granular people-centered view of app access and data handling. Our solutions combine account compromise detection, access control, data loss prevention (DLP), third-party apps control, and analytics to help you secure Microsoft Office 365, Google's G Suite, Box and more. Our powerful analytics help you grant the right levels of access to users and third-party apps based on the risk factors that matter to you.

Powered by the cloud, Proofpoint's solutions 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 Cloud App Security on our corporate website.

To deliver Cloud App Security, Proofpoint processes personal data embedded in event logs, files, emails and instant messages accessible via firewalls, proxies and the cloud app APIs based on permissions granted to Proofpoint by the customer. Personal data processed may include:

- Names
- Email addresses
- IP addresses
- Location data

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, constitutes a legitimate interest of the data controller concerned. 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."

Version July 25, 2019

Data of customers and data subjects is safer when secured by an advanced threat detection and DLP service such as Proofpoint's Cloud App Security. It is Proofpoint's belief that our Cloud App Security solutions achieve the aims of the GDPR to secure and protect individuals' privacy in their personal data, and both data subjects and customers are bettered secured when protected by Proofpoint's Cloud App Security solutions.

DATA TRANSPARENCY

Right to Access: The primary purpose of Cloud App Security solutions 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 organizations can access relevant records that include personal data from the solution console or via APIs available for SIEM integration.

DATA TRANSFERS

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, STORAGE & DELETION

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 data necessary to deliver our Cloud App Security 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.

Cloud App Security detects cloud attacks and oversharing of sensitive data through its forensic analysis of cloud events. In order to provide this service and protect both the customer's data and data subjects' privacy it is necessary for some personal data to be retained. Such data can be deleted upon customer request. Justification exists under the GDPR for retaining personal data as part of such a security service. Under Article 6(1)(e) any private organization acting in the public interest has a legitimate interest in processing personal data, taking into account the rights of the data subject.

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. Proofpoint only permits access to the facilities and services hosting personal data to those employees whose role requires it.

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 deploys encryption to protect personal information. Data in transit to Proofpoint is encrypted using TLS. Proofpoint also provides organizations tools to limit some data collections.

STANDARDS AND CERTIFICATIONS

Our datacenters are designed with market-leading security and privacy capabilities, including compliance with rigorous international standards, such as ISO 27001 for technical measures, ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1, and EU-specific certifications such as BSI's Common Cloud Computing Controls Catalogue (C5) and ENS High.

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. (PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

Version July 25, 2019