CLOUDMARK ACTIVE FILTER, AUTHORITY, CONTENT CATEGORIES, INSIGHT SERVER & SENDER INTELLIGENCE

These detailed Appendices form part of the Clauses and are deemed have to been incorporated into the Clauses when the parties signed page 1 of the Proofpoint Data Processing Agreement.

1. **Data exporter**

The data exporter is **data exporter's affiliated European companies**

The data importer Security Services protect data exporter and its Affiliates from unwanted email and/or mobile messages that may pose a threat to compromise the data exporter's IT systems, data or Personal Data (and the privacy rights of the data subjects themselves). These SCCs and the Services do not cover email and/or mobile data that is outside of data exporter's messaging systems, for example, third party email, webmail, or mobile exchanges on which individuals set up personal messaging accounts.

2. **Data importer**

The data importer is **Proofpoint, Inc.**

Data importer provides its Cloudmark Authority messaging security content filtering services through a combination of on-premises filtering engine technology, backed by the cloud-based Cloudmark Network Feedback System platform for feedback processing, to analyze new threats and generate threat updates from its paired US-based datacenters, at the election of the data exporter and its Affiliates.

3. **Data subjects**

To the extent there is Personal Data within messaging content sent to data exporter's email or mobile messaging systems via the Internet, then the following categories of data subjects may apply: data exporter's end-users including employees, contractors, and customers.

4. **Categories of data**

To the extent there is Personal Data within messaging content sent to data exporter's email or mobile messaging systems, then the following categories of data may apply: e-mail, SMS, MMS, RCS, and OTT messages and included files/documents/metadata.

5. **Processing operations**

<u>Messaging Processes</u>

- On-premises message scanning
    - Typically, all data exporter message scanning actions are undertaken by the Cloudmark Authority software running within the data exporter entity's data centers that house the data exporter's email and/or mobile messaging infrastructure. During the course of email and/or mobile messaging traffic processing, select aggregated and anonymized message metadata is optionally extracted by the Cloudmark Authority engine. These message metadata and scan statistics are summarized,

encrypted, and uploaded via TLS to Cloudmark servers for analysis and used to tune future threat updates and reputation systems.

- Feedback processing

    - In the course of scanning email and/or mobile traffic, periodically some of this messaging traffic is misclassified by the Security Service, resulting in the return of an incorrect score, threat category, or content category label. End users or administrators who observe these misclassifications are provided mechanisms by the data exporter to report such messages, either whole or in part, to Cloudmark for analysis. These message feedback reports are used by the Cloudmark Network Feedback System to potentially adjust future processing of like messages.

- Data Importer's configuration, management and support functions

    - Data importer provides all necessary infrastructure, set-up configuration and support services required to offer the Security Services. Typically all data exporter actions are undertaken by the data exporter entity that is managing the data exporter's email and/or mobile messaging infrastructure. Data exporter is responsible for configuring, administering and managing the Cloudmark Authority engine and for managing all aspects of its own email and/or mobile messaging infrastructure. Data exporter creates support tickets to receive technical support from data importer's product support staff.

6. **Data exporter's right to issue instructions**

The Services Agreement between the data exporter and the data importer are the instructions for the data processing. Data exporter may provide any additional instructions in writing to data importer via amendment or via the data importer's technical support staff.

Data importer shall not use Personal Data for any other purpose except as permitted by the Services Agreement and the normal operation of the Security Services, which includes the processing of feedback required to assure proper functioning of the Security Services, or any copies or duplicates required to comply with statutory or other required retention rules. Reported messages from the Data Exporter's users, including email content, mobile message content, attachments, and metadata (which may include Personal Data), may be stored for analysis in native format for up to 30 days from the point of initial transit through the Services or in perpetuity, depending on the nature of the suspicious or threatening characteristic for the purposes of delivering Security Services.

Data importer shall inform the data exporter promptly upon reasonable belief that there has been an infringement of an applicable statutory data protection provision. Data importer may postpone the execution of the relevant data exporter instruction until it is confirmed or changed by the data importer's representative.

Data exporter shall pay for data importer costs and expenses for any audit under Model Clause Section 5 Obligations of the Data Importer.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached)

Summary of Proofpoint Internal Processes

A. *Summary*

This document summarizes the processes and procedures that Data Importer implements in conjunction with the provision of the Security Services. Additionally, this document includes the relevant controls evaluated on an annual basis by an independent auditor as part of Data Importer's ongoing SOC 1, Type II and SOC 2, Type II audit, or similar audit standard that Data Importer may adopt from time to time at its discretion.

B. *Control Group*

Identification and authentication of the user

There are two classes of users that interact with the Security Services:

Data Exporter Administrative users: Data Exporter administrative users configure the email and/or mobile messaging platforms that integrate the Security Services..

Data Importer users: Centralized authentication and logging is used to ensure that only approved Data Importer personnel have access to the Data Importer data centers and the backend systems that support the Security Services, including certain back-end services that analyze suspicious and unwanted email and/or mobile messaging contents, metadata and attachments. All members of the Security Operations team receive specific training in the administration of the Security Services, in addition to annual Security Awareness training.

Data Importer Controls

Management has established and approved an information security policy.
A framework of security standards has been developed, which supports the objectives of the security policy.
Procedures exist for and to ensure adherence to, authenticating and authorizing users to systems.
Procedures exist for and to ensure adherence to policies for requesting, establishing, issuing, suspending, deleting, and closing user accounts and associated access privileges, e.g. system access is granted based upon position, job function, and manager approval.
A process is in place to monitor failed login attempts. Identified security violations are resolved.
Access to the Data Importer production environment by employees is authorized by the Director of operations and the relevant department head, and is based on business need. A two-factor authenticated VPN is utilized.
Controls are in place to restrict implementation of changes to production only to authorized individuals.

C. *Collection of data*

Email and/or mobile messaging traffic processed by the Security Service within the Data Exporter's infrastructure is filtered in memory, and some elements of the scanning activity and message metadata may be logged locally there, depending on configuration.

Data Importer Controls

If enabled within the Security Service configuration by the administrator, messaging traffic scan statistics for message scan events are stored in memory for a short period of time before being encrypted and uploaded via TLS to Cloudmark systems.

D. *Computers and access terminals*

Computers used by Data Importer employees to access the Data Importer infrastructure are required to use a secure VPN tunnel to access the Data Importer data centers. All computers are required to run up to date anti-virus software and policies and procedures exist to restrict software that may be installed on these machines. All Data Importer employees are required to authenticate to a centralized authentication system in order to access the Data Importer corporate and production networks.

Data Importer Controls

New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.
New employees also receive a copy of Data Importer's information security policy, which they are required to acknowledge receipt of.
Access to the Data Importer production environment by employees is authorized by the Director of operations and the relevant department head, and is based on business need. A two-factor authenticated VPN is utilized.

E. *Access logs*

Access logs are generated for the physical and logical access to Data Importer production systems by Data Importer employees. Physical access logs for all Data Importer data centers are retained for a minimum of 30 days. As well, all access attempts to Data Importer computer systems are centrally logged and unusual activity is automatically reported to Data Importer Security Operations group. In addition, Data Importer enforces account lockout policies, password complexity requirements, and password age requirements.

Data Importer Controls

Procedures exist for and to ensure adherence to, authenticating and authorizing users to systems.
A control process exists and is followed to periodically review and confirm access privileges remain authorized and appropriate.
A process is in place to monitor failed login attempts. Identified security violations are investigated and resolved.
Application event data are retained to provide chronological information and logs to enable the review, examination, reconstruction of systems and data processing and application events.

F. *Telecommunication systems*

All Data Importer production data centers have redundant internet feeds from diverse bandwidth providers. Data Importer controls all routing for our internet-bound traffic and can balance dynamically across these providers.

G. *Instruction of personnel*

All Data Importer personnel are required to complete an annual Security and Awareness training program offered online through a third-party training organization. In addition, members of the Data Importer Security Operations team receive on-going training specific to their roles. This training may be provided by vendors or other third-party organizations.

Data Importer Controls

Data Importer has an organization plan, which separates incompatible roles and duties of relevant personnel.
Separate management roles and responsibilities have been designed to segregate the roles of computer operations, system development, and maintenance and general Data Importer corporate functions.
Personnel roles and responsibilities are clearly defined.

H. *Use of computers*

Access to Data Importer production networks is restricted to systems running Data Importer-approved and managed anti-virus software. As well, all Data Importer computer systems are managed by a centralized authentication system. All Data Importer employees are made aware of Data Importer acceptable use policies for Data Importer computers, internet access and email communications. Data Importer employees must acknowledge these policies and sign a document stating they agree to abide by them.

Data Importer Controls

New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.
New employees also receive a copy of Data Importer's Employee Handbook.

I. *Printing of data*

No printers available within the Data Importer production data centers and all print services are disabled by default on all production servers.

K. *Physical Access Control*

Data Importer Controls

Data Importer relies on a third-party data center provider who maintains controls over physical access to the Data Importer Production Environment in data center locations noted below in “L. Physical Security Measures for Data Centers”.

L. Physical Security Measures for Data Centers

Country	Address	Personal Data processed	Approved Services for this location	
USA	Santa Jose, CA (Equinix Silicon Valley SV1)	email and mobile messaging feedback data; IP address-associated filtering telemetry data	Cloudmark Network Feedback System; Cloudmark Authority Licensing; Cloudmark Authority Threat Updates	ISO 27001, SOC 1, Type II and SOC 2, Type II
USA	North Bergen, NJ (Equinix New York NY7)	email and mobile messaging feedback data; IP address-associated filtering telemetry data	Cloudmark Network Feedback System; Cloudmark Authority Licensing; Cloudmark Authority Threat Updates	ISO 27001, SOC 1, Type II and SOC 2, Type II

USA	Various (not specifically selectable within Google BigQuery configuration)	IP address-associated filtering telemetry data	Datastore backend for IP-address associated filtering; Traffic scan telemetry data	ISO 27001, SOC 1, Type II and SOC 2, Type II

Data Importer Controls

The co-location facilities utilized by Data Importer are considered Tier-3 facilities and include the following:

1. 24x7 on-site security
2. 24x7 on-site and remote facilities monitoring
3. Single point of access
4. Swipe cards and biometrics required for access
5. 'Man Traps' in place
6. Cameras at all entrances and exits.
7. Fences, gates and barriers are in place.
8. Locked shipping docks with no direct access to data center floor.
9. VESDA-type smoke detection
10. Dual-action dry-pipe fire suppression system
11. Redundant power, including battery UPS and on-site generators
12. Redundant environmental controls in N+1 configuration

M. ***Access control to IT systems***

Data Importer Controls

Data Importer controls access to systems providing Security Services in the following ways:

1. All Data Importer employees and contractors are provided with unique userIDs. Account sharing is not permitted.
2. Password requirements are defined and enforced by a password synchronization tool. Requirements include:
    a. Minimum of 12 characters
    b. Complexity rules (3 of 4 – upper, lower, numbers, special characters)
    c. History of 23
    d. Required to change every 60 days
    e. Account locked out after five (5) failed login attempts
3. Logical access is granted based on role.
    a. Only members of the Operations group are granted privileged access to the Data Importer Production Environment.

4. Audit logging is in place on the VPN to the Data Importer Production Environment.
5. Audit logs are monitored in near real-time by a log aggregation and alerting tool. Alerts are configured to be sent to the Data Importer Security Operations group.
6. Data Exporter is provided with the option of enabling encryption for email data in transit between the Security Services and the Data Exporter email infrastructure.

N. ***Access control to data***

Data Importer Controls

Data Exporter data is not permitted to reside in the Data Importer Corporate Environment. Access to systems filtering Data Exporter email data are controlled in the following ways:

1. Access is based on role at Data Importer.
2. Only the Data Importer Operations group is permitted to have privileged access to the Data Importer Production Environment.
3. Privileged access lists are reviewed periodically.

O. Audit logging is in place on the VPN and on systems in the Data Importer Production Environment.

P. ***Implement least privilege access control***

Data Importer Controls

Access to the Data Importer Production Environment is granted based on role. Only members of the Data Importer Security Operations group are granted privileged access to the Production Environment. Privileged access is reviewed monthly to ensure it remains appropriate.

Q. ***Security while transferring and processing***

Data Importer Controls

Data Importer does not permit Data Exporter email and/or mobile messaging data to reside in the Data Importer Corporate Environment, where Data Importer employees and contractors reside. The Data Importer Production Environment is logically and physically segregated from the Data Importer Corporate Environment:

1. Access to the Data Importer Production Environment is via a two-factor authenticated VPN and is only provided to Data Importer employees and contractors whose role requires access.
2. Industry-standard firewalls are in place and configured to only permit traffic on ports necessary for the functioning of the Service with all others denied by default.
3. All Administrator and End-User access to the Security Services hosted web interfaces is encrypted using TLS.

System Access Controls

1. LDAP and/or host-level role-based access controls and authentication is used to manage access.
2. Privileged access is only granted to members of the Data Importer Security Operations group.

Endpoint Security

1. Industry-standard firewalls are in place and configured to only permit traffic on ports necessary for the functioning of the Service with all others denied by default.
2. Network-based IDS is configured to monitor traffic inbound from and outbound to the Internet. Alerts are configured to be sent to the Data Importer Security Operations group.

Server Security

1. Operating systems are patched.
2. Unnecessary services are disabled.
3. Default passwords are changed.

R. ***Security while transmitting data over public networks***

Data Importer Controls

1. Data Exporter may elect to enable TLS for the encryption of Data Exporter email between the Security Services and the Data Exporter email infrastructure.
2. All intra- Security Services communications are encrypted using TLS.
3. All Administrative and End-User access by Data Exporter to the Security Services is encrypted using TLS.

S. ***Implementation and Operations phase controls***

Data Importer Controls

The functionality provided by the Security Services is performed automatically and does not require human intervention, except in order to troubleshoot issues with the Security Services. The Security Services are designed to function as described in the Services Agreement. Monitoring is in place to ensure that the Cloudmark Network Feedback System Services are functioning in order to maintain the ability for the Security Services to function as described in the Services Agreement including alignment with applicable SOC2 Trust Services Criteria and eTRUST principles.

T. ***Ensuring Compliant Data Processing***

Data Importer Controls

All Data Exporter email and/or mobile messaging data is automatically filtered by the Security Services, as described in the Security Services documentation, at the Data Exporter premises.

U. ***Ensuring Availability***

Data Importer Controls

The Security Services are architected to ensure Availability in-line with Data Importer's contracted SLA's. This is accomplished in the following way:

1. The backend Cloudmark Network Feedback System infrastructure that supports Security Services are configured to run in active/passive mode between a pair of geographically-diverse data centers.
2. Infrastructure in each data center is configured in high-availability mode, including dual power feeds and a minimum of two diverse network connections.
3. Data centers are a minimum of Tier-3 with redundant power and redundant environmental controls.
4. Data centers have on-site generators with a minimum of three (3) day fuel supply.
5. A Disaster Recovery Plan is documented and tested annually.
6. A Business Continuity Action Plan is documented and tested annually.
7. A distributed monitoring infrastructure monitors for Availability.
8. Industry-standard firewalls are configured to permit ports necessary for the Service and deny all others by default.
9. All Data Importer owned Windows and Mac laptops, workstations and servers in the Data Importer Corporate Environment run a centrally-controlled anti-virus service.

Appendix 3
Subprocessors

Subprocessor Name	**Location**
Amazon Web Services (AWS)	USA
Equinix	USA
Google Compute Platform	USA
Salesforce.com	USA