

# PROOFPOINT DIGITAL RISK

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.

## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

**This Appendix forms part of the Clauses and must be completed and signed by the Parties**

### 1. **Data exporter**

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

### 2. **Data importer**

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

Data importer provides the Services from its paired US datacenters and/or its paired European Union datacenters, at the election of the Customer and its Affiliates.

### 3. **Data subjects**

To the extent there is Personal Data within the Customer's social media accounts, 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 the Customer's social media accounts, then the following categories of data may apply: social media user account IDs, social media content, and option biographical information if included in users' account profile.

### 5. **Processing operations**

- Discovery of related social media accounts. Proofpoint scans social media platforms to find accounts affiliated with a Customer for fake, fraudulent, and protest accounts related to the Customer. Scanning is continuous for any such accounts. This scanning can be automated and recurring. Alerts are created to initiate workflow and/or takedown operations.
- Analysis of static and interactive content. Proofpoint scans social media profiles and content (posts and comments) and applies smart classifiers to create alerts and take action. The system can automatically delete posts and comments that contain malware or phishing threats, and can identify bad actors who may be targeting Customer's employees with social engineering attacks. Policies can be applied to enforce the application that is used to publish content.
- Archive of social media as required for compliance. Proofpoint's social archive can store content in a way that is compliant with financial services regulations by intelligently collecting and classifying social media content for future search and eDiscovery. Proofpoint includes relevant metadata - contextual information, including remediation workflow, approval details, and content classification - in the social archive. Additionally, Proofpoint can forward this content to a 3<sup>rd</sup> party archive solution at the request of Customer.

6. **Correction, deletion and blockings of data**

Data importer may only correct, delete or block the data processed on behalf of the data exporter when instructed to do so by the data exporter.

7. **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 portal.

Data importer shall not use Personal Data for any other purpose except as permitted by the Services Agreement and the normal operation of the Services, which includes any copies or duplicates required to comply with statutory or other required retention rules.

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, provided however, in the event that data exporter pays data importer annual Services subscription fees of more than USD 250,000, then data exporter and data importer shall each pay for its own costs and expenses for any audit under Model Clause Section 5 Obligations of the data.

## 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 Services. Additionally, this document includes the relevant controls evaluated on an annual basis by an independent auditor as part of Data Importer's ongoing SSAE 16 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 Services:

Data Exporter end-users: Data Exporter administrative users potentially may access personal data through a web-browser based user interface. Data Exporter's end-users are authenticated through a central authentication mechanism, and Customer has the option to enable 2-factor authentication for such end-users. Data Exporter may elect to integrate its Active Directory with the Services to provide its administrators with the ability to grant or revoke access. Data Importer does not have the ability to grant or revoke access for data exporter end users.

Data Importer users: Centralized, 2-factor authentication and logging is used to ensure that only approved Data Importer personnel have access to the Data Importer data centers and the Services infrastructure. All members of the Security Operations team receive specific training in the administration of the 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.

**Type of access**

The various types of Data Exporter end user access are documented in the Administrator Guide and are controlled by Data Exporter administrators through Active Directory.

**C. Collection of data**

**Data Importer Controls**

Personal Data, at the request of Customer, can be anonymized

**D. Execution of backup copies**

Data Exporter Services configuration data and logs necessary to recover from certain disaster scenarios are backed up on a regular basis and stored on spinning disk.

**Data Importer Controls**

Procedures for backup and retention of data and programs have been documented and implemented.
Data and programs are backed up regularly and replicated between geographically diverse data centers.

**E. 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.

**F. Access logs**

Access logs take at least two different forms:

The first relates to access by Data Exporter end-users to the data through the hosted Data Exporter End-user Interface in the Data Importer Production data centers. Access logs for Data Exporter end-users consist of Service-generated security logs that contain access information and are available only to Data Exporter Administrators. The second type of access logs are 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 90 days and reviewed on a monthly basis by the Operations group. 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.

**G. 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.

**H. 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.

**I. 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 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.

**J. Printing of data**

Data Exporter data is processed in memory and is not available for printing. In addition, there are no printers available within the Data Importer production data centers and all print services are disabled by default on all production servers.

**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.

**K. Physical Access Control**

**Data Importer Controls**

Data Importer maintains controls over physical access to the Data Importer Production Environment in the following manner:

1. Access is only granted to Data Importer employees whose role requires it
2. Access is granted via a secure administrative portal hosted by the co-location provider
3. Swipe cards and biometric authentication is required for access to the co-location facility
4. Swipe cards are required for access to the dedicated Data Importer cage.
5. Access logs are reviewed by Data Importer monthly.
6. Access lists are reviewed by Data Importer quarterly.
7. Access is disabled upon role reassignment or termination
8. Access badges are collected upon role reassignment or termination

**L. Physical Security Measures for Data Centers**

Country	Personal Data processed	Approved Services for this location	Certification
USA	social media account IDs & content	Domain Discover, Mobile Discover, Social Archiver, Social Sight, Social Syndicate, Social Discover, Social Patrol	Annual SSAE 16 SOC 1 Type II audit report
European Union	social media account IDs & content	Domain Discover, Mobile Discover, Social Archiver, Social Sight, Social Syndicate, Social Discover, Social Patrol	Annual SSAE 16 SOC 1 Type II audit report

**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 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. .

**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 is 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 monthly.

- 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 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. 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.
4. All intra-Service communications are encrypted using TLS.
5. All Administrator and End-User access to the Services hosted web interfaces is encrypted using TLS.

***System Access Controls***

1. LDAP 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. All intra- Services communications are encrypted using TLS.
2. All Administrative and End-User access by Data Exporter to the Services is encrypted using TLS.



**S. Implementation and Operations phase controls**

**Data Importer Controls**

The functionality provided by the Services is performed automatically and does not require human intervention, except in order to troubleshoot issues with the Services. The Services are designed to function as described in the Services Agreement. Monitoring is in place to ensure that the Services are functioning with regards to the eTRUST principles Performance, Capacity, Availability and Security.

**T. Monitoring and Testing phase controls**

**Data Importer Controls**

The functionality provided by Services is performed automatically and does not require human intervention, except in order to troubleshoot issues with the Services. Data Exporter's social media content are not changed as part of the Services.

**U. Traceability of any access, change and deletion**

**Data Importer Controls**

Access to systems are controlled in the following ways:

1. Access is based on role at Data Importer.
2. Only the Data Importer Security Operations group is permitted to have privileged access to the Data Importer Production Environment.
3. Privileged access lists are reviewed monthly.
4. Audit logging is in place on the VPN and on systems in the Data Importer Production Environment.

The Service controls access in the following way:

1. Administrative access to the Administrator Web Interface by Data Exporter administrators is granted by Data Importer at the request of Data Exporter or by the Data Exporter itself.
2. End-User access to the End-User Web Interface by Data Exporter end-users is granted by Data Exporter through the use of SAML 2.0 for LDAP integration.
3. The Services generate Application Logs that include Administrator and End-User access and include the following:
  - a. Successful/Failed login attempts
  - b. Date
  - c. Time
  - d. Source IP
  - e. userID

## **V. Ensuring Compliant Data Processing**

### **Data Importer Controls**

Data Importer personnel do not manually process Data Exporter data.

## **W. Ensuring Availability**

### **Data Importer Controls**

The Services are architected to ensure Availability in-line with published Data Importer's SLA's ([www.proofpoint.com/us/license](http://www.proofpoint.com/us/license)). This is accomplished in the following way:

1. The Services are configured to run in active/active 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. Data Exporter Configuration Data is backed up daily for Disaster Recovery purposes.
6. A documented Disaster Recovery Plan is documented and tested annually.
7. A documented Business Continuity Action Plan is documented and tested annually.
8. A distributed monitoring infrastructure monitors for Availability.
9. Industry-standard firewalls are configured to permit ports necessary for the Service and deny all others by default.
10. All Data Importer owned Windows and Mac laptops, workstations and servers in the Data Importer Corporate Environment run a centrally-controlled anti-virus service.

## **X. Data Separation**

### **Data Importer Controls**

The Services maintain logical segregation of Data Exporter data.

**APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES**

**Subprocessors**

<b><u>Subprocessor Name</u></b>	<b><u>Location</u></b>
Amazon Web Services (AWS)	USA
Salesforce.com	USA
Sutherland Global Services	USA