

PROOFPOINT META

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

1. **Data exporter**

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

The data importer's Meta services ("Services") protect access to data exporter's (and its Affiliates') corporate network and Cloud storage services, including any Personal Data processed or stored within data exporter's network (thereby protecting the privacy rights of the data subjects themselves). The data exporter hereby provides standing instructions for data importer to implement and use the Services to protect access to data exporter's corporate network.

2. **Data importer**

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

Data importer provides its on-demand Meta services from its US-based datacenters hosted by Amazon Web Services.

3. **Data subjects**

End-users who access data exporter's corporate network, including employees and contractors.

4. **Categories of data**

To the extent there is Personal Data used or stored by Meta's authentication and routing protocols: user email address and name and (optional phone number) and intranet traffic events such as accept/drop events and DNS queries (Customer has the option to enable or disable logging internet traffic events).

5. **Processing operations**

Meta Processes

- Meta overlays a zero-trust network on top of data exporter's corporate network. Users access the corporate network by connecting to the Meta network layer through a VPN with their login credentials. Once logged into the Meta network each user is assigned a unique identity that connects to the data exporter's underlying corporate network and access to assets within the data exporter's corporate network is accessed based on the user's unique identity.

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, however the parties recognize and agree that only the data exporter can correct, delete or block the user's access to the Meta Service.

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 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.

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.

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 when logging into the administrator portal through a web-browser based user interface.

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 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.

C. Collection of data

User initiates authentication to data exporter's corporate network using the data exporter's identity provider (IdP) or alternatively the Meta IdP. Connection is established using a unique client-side certificate.

Data Importer Controls

Encrypted network tunnels are used to protect Data Exporter data in transit whenever possible. This limits each Data Exporter's access to only their own data.

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 (Services only)

Procedures for backup and retention of data and programs have been documented and implemented.
Data and programs are backed up regularly and replicated within multiple AWS availability zones.

E. Computers and access terminals

Computers used by Data Importer employees to access the Data Importer infrastructure are require multi-factor authentication to access the AWS instance(s) containing Data Exporter data. 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 authentication is utilized.

F. Access logs

In relation to the Services, access logs take at least two different forms:

Access logs for Data Exporter end-users consist of Security Service-generated security logs that contain access information and are available only to Data Exporter Administrators. 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 systems hosted by AWS 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 and internet access. 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 is no printing service available from AWS hosting environment.

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 AWS hosted environment
3. Access logs are reviewed by Data Importer monthly.
4. Access lists are reviewed by Data Importer quarterly.
5. Access is disabled upon role reassignment or termination

L. Physical Security Measures for AWS Hosting Environment

Country	Address	Personal Data processed	Approved Services for this location
USA	East Coast	Username, email address, phone number (optional)	Meta services are hosted by Amazon Web Services. Physical access is controlled by AWS.

Data Importer Controls

The hosting facilities utilized by AWS 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 facility 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 8 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.

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 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 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 authentication and is only provided to Data Importer employees and contractors whose role requires access.
2. AWS managed 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 intra-Service communications are encrypted using TLS.
4. All Administrator and End-User access to the Services hosted web interfaces is encrypted using TLS.

System Access Controls

1. Identity provider service is used to manage access.
2. Privileged access is only granted to members of the Data Importer Security Operations group.

Endpoint Security

1. AWS managed 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.

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 as described in the Services Agreement including alignment with applicable SOC2 Trust Services Criteria and eTRUST principles.

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.

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

Data Importer Controls

Access to systems filtering Data Exporter data 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 for systems in the Data Importer Production Environment.

The Security 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.
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. All Data Exporter data is automatically filtered by the Services, as described in the Services documentation.

W. *Ensuring Availability*

Data Importer Controls

The Services are architected to ensure Availability in-line. This is accomplished in the following way:

1. The Services are configured to run in active/active mode in multiple AWS availability zones.
2. Infrastructure is configured in high-availability mode, including dual power feeds and a minimum of two diverse network connections.
3. The AWS hosting environment are a minimum of Tier-3 with redundant power and redundant environmental controls.
4. The AWS hosting environment has 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.