GDPR Data Processing Agreement and Standard Contractual Clauses

This GDPR Data Processing Agreement ("**DPA**") is between the entity identified below as the Controller (the "**Controller**"), and Proofpoint, Inc., 925 W. Maude Avenue, Sunnyvale, CA 94085 ("**Processor**" or "**Proofpoint**") and is appended to either: (1) the Proofpoint Master Subscription Agreement or General Terms and Conditions and applicable Product Exhibit(s), (2) an end user license agreement (the online Customer Agreement, a EULA, clickwrap if any, or clickthrough agreement) accepted by Controller on Controller's initial registration and access of the Proofpoint product or service, or (3) any another written and signed license agreement between the parties under which Processor provides products or services to Controller (the "**Services Agreement**"). This DPA is effective as of the date signed by the Controller, but only if Proofpoint receives the signed DPA in accordance with the instructions below.

This DPA sets forth the terms and conditions under which Processor may receive and process Personal Data from Controller. This DPA takes into account the nature of the processing pursuant to the Services Agreement and describes the appropriate technical and organizational measures undertaken by Processor in the processing of Personal Data.

Furthermore, this DPA incorporates the Standard Contractual Clauses annexed to the EU European Commission Decision (EU) 2021/914 (the "**SCC**"). In addition to Proofpoint's obligations set out in this DPA, Proofpoint will comply with the obligations of a Data Importer as set out in the SCC. Any reference to **Data Importer** shall be deemed to be a reference to **Proofpoint, Inc., or the Processor** and any reference to **Data Exporter** or Data Controller shall be deemed to be a reference to **Controller** and its European Union affiliated companies. Controller hereby covenants and warrants that it has the right and authority to enter into this DPA on behalf of itself and its affiliated companies.

The Parties to this DPA hereby agree to be bound by the terms and conditions in the attached Schedules 1 (Data Processing Terms), the Appendices thereto, and 2 (Standard Contractual Clauses). This DPA has been pre-signed by Processor, Proofpoint, Inc. In order for this DPA to be effective, Controller must first:

1. Complete and sign the information block below with the Controller full legal entity name, address, and signatory information; and
2. Submit the completed and signed DPA to Proofpoint via email to privacy@proofpoint.com.

If Controller makes any deletions or other revisions to this DPA, those deletions or revisions are hereby rejected and invalid, unless agreed by Proofpoint. Controller's signatory represents and warrants that he or she has the legal authority to bind Controller to this DPA. This DPA will terminate automatically upon termination of the Services Agreement, or as earlier terminated pursuant to the terms of this DPA.

Accepted and agreed by Controller:

Signature: _____

Name: _____

Date: _____

Company: _____

Address: _____

_____

Accepted and agreed by **Proofpoint, Inc.:** (**Processor**

Signature: DocuSigned by: Paul Auvil 2955B8CEBD2B45C...

Name: Paul Auvil, CFO

SCHEDULE 1

DATA PROCESSING TERMS

1. Definitions.

a. All terms used without definition in this DPA have the meanings ascribed to them: first, in the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**GDPR**); and second, in the Services Agreement.

b. **Controller Data** means the Personal Data of the Controller, Personal Data having the same definition as in the GDPR.

c. **Data Protection Laws** means all applicable laws and regulations regarding the Processing of Personal Data to the extent in connection of the provision of Proofpoint Products and Service under the Services Agreement.

d. **Data Subject** means the identified or identifiable person to whom Personal Data relates.

e. **Processing** (and its cognates) has the meaning as set-forth in article 4.2 of the GDPR.

f. **Subprocessor** means any processor engaged by Processor to process Personal Data.

g. **Supervisory Authority** means a public authority which is established by an EU Member State pursuant to GDPR.

2. Processing of Personal Data.

a. It is the intent of the parties that, with respect to the activities described in Appendix 1, Controller and its European Union affiliated companies (or their affiliates or clients) will be the data controller/ data exporter and Processor will be the data processor/ data importer to the extent it processes Personal Data. Controller agrees and warrants that its instructions to Processor regarding the processing of Personal Data are and shall be in accordance with the relevant provisions of the applicable Data Protection Laws.

b. The subject matter and duration of the Processing of Personal Data are set out in the Services Agreement, which describes the provision of the Service to Controller. The nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set forth in Appendix 1 to this DPA.

c. Controller is responsible for the accuracy, quality, and legality of the Personal Data, and the means by which Controller acquired the Personal Data.

d. The Services Agreement and this DPA hereby form Controller's instructions to Processor regarding: (1) the Processing of Personal Data, and (2) the transfer such Personal Data to any country or territory, when reasonably necessary for the provision of the Service.

3. Data Protection Impact Assessment ("DPIA")

Taking into account the nature of the Processing, Processor may provide Controller with reasonable cooperation and assistance needed to fulfill Controller's obligation under the GDPR to carry out a data protection impact assessment related to Controller's use of the Service, to the extent Controller does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide reasonable assistance to Controller in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Controller's DPIA obligation, to the extent required under the GDPR.

4. Rights of Data Subjects. Processor will, to the extent legally permitted, promptly notify Controller if Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, right to be forgotten, data portability, objection to the processing, or right not to be subject to an automated individual decision making. Taking into account the nature of the Processing, Processor

shall assist Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Controller's obligation to respond to the Data Subject's request.

5. **Limited use of Personal Data & personnel.** Except as otherwise set forth in the Services Agreement, (i) Processor will not acquire any rights in or to the Personal Data; and (ii) Processor and its affiliates shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any contracted Subprocessor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Services Agreement, and to comply with applicable data protection and privacy laws, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. **Subprocessors**.

a. **Appointment of Subprocessors**. Controller provides general consent to Processor to use of Subprocessors. Controller acknowledges and agrees that (a) Processor's affiliates may be retained as Subprocessors; and (b) Processor and its affiliates respectively may engage third-party Subprocessors in connection with the provision of the Service. Processor or its affiliate(s) has entered into a written agreement with each Subprocessor containing data protection obligations not less protective than those in this DPA with respect to the protection of Controller Data to the extent applicable to the nature of the Service provided by such Subprocessor. Processor shall remain fully responsible to the Controller for the performance of Subprocessors' obligations in accordance with its contract with the Processor.

b. **List**. The current list of Subprocessors for the Service is available on the Proofpoint Trust Site at: https://www.proofpoint.com/us/legal/trust. In the event Processor makes any changes or additions to such list, to the extent Controller has subscribed to receive notifications on the Trust Site, Processor shall provide notice of such changes by e-mail. The parties agree this notification satisfies the notification requirements of Section 28.2 of the GDPR and Clause 9 of the Standard Contractual Clauses.

c. **Objection**. Controller may object to Processor's use of a new Subprocessor by notifying Processor promptly in writing to privacy@proofpoint.com. In the event Controller objects to a new Subprocessor Processor will (after receipt of Controller's written objection as stated in the previous sentence) reasonably determine whether accommodations can be made available to Controller to avoid processing of Personal Data by the objected-to new Subprocessor without unduly burdening the Controller. If Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days Controller may terminate the applicable ordering document with respect only to the Service which cannot be provided by Processor without the use of the objected-to new Subprocessor by providing written notice to Processor within thirty (30) days of Processor's determination.

7. **Special categories of Personal Data**. Controller (and its European Union affiliates) shall be solely responsible for compliance with data protection and privacy laws, as applicable to Controller (and its European Union affiliates), including any Personal Data that requires special handling or special categories of Personal Data such as, without limitation, that which relates to an individual's race or ethnicity, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, or personal finances.

8. **Security of Personal Data.**

a. The Processor shall at a minimum implement the technical and organizational measures specified in Appendix 2 to ensure the security of the Personal Data. This includes protecting the Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the Personal Data. In assessing the appropriate level of security, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the Data Subjects.

b. The Processor shall grant access to the Personal Data undergoing processing to members of its personnel only to the extent necessary for implementing, managing and monitoring of the Services Agreement. The Processor shall ensure that persons authorized to process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9. Cooperation with Supervisory Authorities. Processor shall provide reasonable assistance to Controller in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 8 of this DPA, to the extent required under the GDPR. Additionally, in connection with the Supervisory Authority's request, at Controller's expense Processor shall make reasonable efforts to acquire the reasonable cooperation and assistance of Subprocessors in providing access to relevant information needed to fulfill Controller's obligations under GDPR.

10. Personal Data Breach.

a. In the event of a known unauthorized use, disclosure or acquisition by a third party of Personal Data that compromises the security, confidentiality, or integrity of Personal Data maintained by Processor ("Security Breach"), Processor will notify Controller in writing of the breach within 48 hours and provide periodic updates afterwards.

b. Such notification shall contain, at least
   (i) a description of the nature of the Security Breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);
   (ii) the details of a contact point where more information concerning the Personal Data breach can be obtained; and
   (iii) its likely consequences and the measures taken or proposed to be taken to address the Security Breach, including to mitigate its possible adverse effects.

c. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

11. International Transfer of Data

a. **General**. Processor will abide by the requirements of applicable Data Protection Laws regarding the international transfer of Personal Data from the European Economic Area. Solely for the provision of Service to Controller under the Services Agreement, Personal Data may be transferred to and stored and/or Processed in any country in which Processor or its Subprocessors operate, which may include third party countries. All transfers of Personal Data out of the European Economic Area shall be governed by the Standard Contractual Clauses which the parties hereby enter into and incorporate into this DPA as Schedule 2.

b. **Data Transfer Assessment.** Several of Processor's security services require that some amount of Personal Data be transferred to the United States, and so in furtherance of Clause 14(b) of the Standard Contractual Clauses Processor has compiled a Data Transfer Assessment (also known as a Transfer Impact Assessment), which can be found at https://www.proofpoint.com/sites/default/files/misc/pfpt-us-data-transfer-assessment-20201028.pdf.

12. Governmental Queries.

a. In furtherance of Clause 15 of the Standard Contractual Clauses Processor will not disclose to any third party government body or public authority, any Controller Data, except in each case, as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends Processor a demand for sensitive Controller Data, Processor will attempt to redirect the governmental body to request that data directly from Controller. As part of this effort, Processor may provide Controller's basic contact information to the governmental body. If compelled to disclose Controller Data to a

governmental body, then Processor will give Controller reasonable notice of the demand to allow Controller to seek a protective order or other appropriate remedy unless Processor is legally prohibited from doing so. Under the United States' Foreign Intelligence Surveillance Act (FISA), Processor is a "remote computing service" and not a telecom provider and therefore unlikely (in Processor's opinion) to be the subject of a government request under such laws.

b. In order to ensure that Controller becomes and remains aware of the risks attached to the transfer of data to a third country, Processor, may from time to time, upon reasonable request from Controller, not to exceed once per calendar year, provide response(s) to a structured questionnaire from Controller about the laws and regulations in the destination country applicable to the Processor or its Subprocessors that would permit access by public authorities to the Controller Data that are subject to the transfer, in particular, in the areas of intelligence, law enforcement, and administrative and regulatory supervision applicable to the transferred data. Processor must be able to provide Controller with this type of information to the best of its knowledge and after having used its best efforts to obtain such information.

13. Verification and audit

a) Pursuant to Section 28.3 (h) of the GDPR, Processor shall make available to Controller, upon reasonable written request and subject to the execution of a dedicated non-disclosure agreement, information related to the Processing of Personal Data of Controller as necessary to demonstrate Processor's compliance with the obligations under this DPA. Processor shall allow for onsite inspection requests by Controller or an independent auditor in relation to the Processing of Personal Data to verify that Processor is in compliances with this DPA, if (a) Processor has not provided sufficient written evidence of its compliance with the technical and organizational measures; (b) a Security Breach has occurred; (c) an inspection is officially requested by Controller's Supervisory Authority; or (d) Data Protection Law provides Controller with a mandatory on-site inspection right; and provided that Controller shall not exercise this right more than once per year unless mandatory Data Protection Law requires more frequent inspections. Any information provided by Processor and/or audits performed pursuant to this section are subject to the execution of a dedicated non-disclosure agreement. Such facility inspections shall be conducted in a manner that does not impact the ongoing safety, security, confidentiality, integrity, availability, continuity and resilience of the inspected facilities, nor otherwise expose or compromise any confidential data Processed therein.

b) Each party shall bear its own cost is costs associated with any audit or inspection. This shall also apply to any provision of information or audit pursuant to Section 8.9 (c-e) of the Standard Contractual Clauses.

14. Termination

Controller acknowledges and agrees that in the event of a suspension or termination of any data Processing under this DPA or Clause 18 of the Standard Contractual Clauses, the timeframe for Processor's cessation of all Processing and deletion of personal data will be governed by the Services Agreement.

APPENDIX 1 TO THE DPA – DETAILS OF THE PROCESSING

This Appendix 1 includes certain details of the Processing of Customer's Personal Data as required by Article 28(3) GDPR (or as applicable, equivalent provisions of any other Data Protection Law).

Product	Data Subjects	Categories of Personal Data Processed	Processing Operations	Retention Period
Archive	Employees, contractors, and customers	Any Personal Data included in captured content (including e-mails, instant messages, social media content, associated message telemetry and attachments)	• Archive is a cloud-based archiving solution designed for legal discovery, regulatory compliance and data access for Customer's end users, and it provides a central, searchable repository that supports a wide range of content types.	As determined by the Controller
CAD/CASB	Employees, contractors	Cloud account holder metadata (e-mail addresses, names, position), file metadata and cloud account access logs	Cloud Account Defense helps Customer detect suspicious activities around Customer's cloud accounts and identify compromised cloud accounts. Cloud App Security Broker uses policies to prevent the loss of Customer's sensitive or confidential data contained in Customer's cloud accounts. CASB IaaS Protection helps customer identify its IaaS resources, protect sensitive data within IaaS storage, and monitor and stop unauthorized logins to Customer's Cloud accounts	Up to 180 days from the end of Controller's subscription maximum
Cloudmark Active Filter, Authority, Content Categories, Insight Server, and Sender Intelligence; Cloudmark Spam Reporting Service	Employees, contractors, customers	Telemetry data associated with E-mail, SMS, MMS, and RCS, including email addresses, IP addresses, phone numbers	Cloudmark products leverage intelligent threat analysis to provide email and mobile messaging security against spam and malware.	30 days for messages reported by recipient as potentially harmful. 30 days for messages reported by recipient as not harmful.
Cloudmark Safe Messaging Cloud, Cloudmark Safe Messaging Cloud Hybrid	Employees, contractors, customers	Telemetry data associated with E-mail, SMS, MMS, and RCS, including email addresses, IP addresses, phone numbers	Cloudmark products leverage intelligent threat analysis to provide email and mobile messaging security against spam and malware.	30 days for messages reported by recipient as potentially harmful. 30 days for messages reported by recipient as not harmful.

				Otherwise as negotiated by Controller.
Compliance Gateway	Employees, contractors and customers	Any personal data included in captured content (including e-mails, instant messages, social media content, associated message telemetry and attachments	Compliance Gateway acts as a central hub to filter and route message content to Customer's archive, supervision and analytic systems.	Up to 14 days from the end of Controller's subscription maximum
Content Capture	Employees, contractors and customers	Any personal data included in captured content (including e-mails, instant messages, social media content, associated message telemetry and attachments	Content Capture captures content from supported messaging and Cloud storage platforms and delivers it compliance services such as e-discovery, archive and supervision.	Up to 90 days from the end of Controller's subscription maximum
Content Patrol	Employees, contractors and customers	Any personal data included in captured content (including e-mails, instant messages, social media content, associated message telemetry and attachments	Content Patrol allows Customers to capture, monitor, remediate and generate compliance reports about their end users' activities on Customer controlled social media accounts.	Up to 90 days from the end of Controller's subscription maximum
Continuity	Employees, contractors, and any other individuals sending or receiving e-mails via Controller's corporate e-mail system	Any Personal Data included in an e-mail	Continuity provides temporary storage of Customer inbound and outbound email within the on-demand, Web-based email. Continuity serves only as a secondary, emergency failover option in the event of failure of Customer's email service, and not as a primary email archive solution or a primary failover solution	Messages expire after 30 days.
Digital Discover, Digital Protection, and Digital Compliance	Employees, contractors, customers, or any other individuals posting to Customer's social media accounts	Corporate social media user account IDs, social media content, and option biographical information if included in corporate users' account profile	Scanning of social media platforms to find accounts affiliated with a customer for fake, fraudulent, and defamatory accounts related to the customer. Analysis of static and interactive content. Connectors to the Archive service of social media as required for compliance	Up to 90 days from the end of Controller's subscription maximum
Email Data Loss Prevention (DLP)	Employees, contractors, and any other individuals sending or receiving e-mails via Customer's corporate e-mail system	Any Personal Data included in an e-mail	Email DLP utilizes policies to prevent the loss of Customer's sensitive or confidential data through email.	Up to 366 days after collection except for Threat Analytics, which are retained for up to 18 months after collection.

Email Fraud Defense	Employees, contractors, customers and any other individual sending or receiving e-mails via Customer's corporate e-mail system	Email header information, including email addresses, IP addresses, sender and recipient names.	EFD processes Domain-based Message Authentication, Reporting & Conformance (DMARC) aggregate reports and DMARC forensic message sample traffic for customer domains and evaluates the authenticity of senders based on sender authentication information, and to highlight traffic sent from unauthenticated and unauthorized sources.	Cloudmark forensic data is retained for 30 days after collection. DMARC forensic data is retained for 90 days after collection.
Email Encryption	Employees, contractors, customers and any other individual sending or receiving e-mails via Customer's corporate e-mail system	Any Personal Data included in an e-mail	Email Encryption provides a fully integrated message encryption and decryption solution.	Encrypted message content is retained as determined by the Controller (up to 366 days).
Email Protection	Employees, contractors, and any other individuals sending or receiving e-mails via Controller's corporate e-mail system	Any Personal Data included in an e-mail	Email Protection includes functions such as spam detection functions to identify and classify spam messages; virus protection functions to detect and filter messages containing known viruses; zero-hour anti-virus functions to detect and filter messages containing suspicious content; a quarantine folder to analysis and disposition of suspicious content	Up to 18 months after collection
Endpoint Data Loss Protection	Employees, contractors	Metadata recorded for Controller's users	Endpoint Data Loss Prevention deploys software (an Agent) onto Customer owned or controlled desktops and servers on supported platforms. These Agents capture metadata recorded from the activities of licensed Users and store this data in Proofpoint's Endpoint Data Loss Prevention archive.	Up to 90 days from the end of Controller's subscription maximum
Essentials	Employees, contractors, customers	Any Personal Data included in an e-mail	• Scanning, filtering, and routing in transit of e-mails sent to and received from parties external to the customer, via the customer's corporate e-mail system. • If archive functionality is used, then see "Archive" above • If TAP sandboxing is used, see TAP below	Up to 18 months after collection.
Insider Threat Management SaaS	Employees, contractors: a) ITM SaaS Administrators or analysts, using the web portal. b) Endpoint users, using data	email address, device identifier such as IP address, user information such as name and user ID, website information such as URL and page name, Application information such as application name, executable	ITM deploys an endpoint agent onto designated laptop, desktop and server devices owned or controlled by data controller. The agents collect telemetry data about the activities of the device users, the data subjects. If enabled by data controller the agents can also capture screenshots of the users' device activities. Customer solely determines whether to enable the screen capture capabilities, and the data retention period of such content. The telemetry and screen capture data is stored on Proofpoint's multi-tenant ITM SaaS storage.	As In accordance with Controller's selected retention period up to a maximum period of 366 days.

	exporter's endpoints on which the ITM SaaS agent has been installed.	name, and window title. Additionally, ITM has the capability to capture screen content, which is configured and controlled by the customer. Screen capture could include any additional personal data displayed on the user's screen.		
Intelligent Classification and Protection	Employees, contractors, customers and any individual viewing the document.	Any Personal Data included in a document.	Automatically locates and identifies sensitive and business-critical data to enhance existing data protection solutions such as labelling, encryption, access Control, data loss prevention, CASB and suggests protection rules and/or policies to the Customer	Up to 90 days from the end of Controller's subscription maximum
Internal Mail Defense (IMD)	Employees, contractors	Any Personal Data included in an e-mail	IMD leverages Email Protection and TAP features to protect Customer's internal email communications against spam and malicious content.	Up to 18 months after collection.
Browser and E-mail Isolation	Employees and contractors	e-mail addresses, user site cookies, and browser history, and isolation container datacenter location.	Browser and Email Isolation products establish an isolated remote web browser or web email environment to protect the Customer from potential threats when Users connect to the Internet or web-based email accounts on Customer owned or controller devices. Customer will not allow Users to transmit through (or post on) Isolation any infringing, defamatory, threatening or offensive material.	Up to 90 days from the end of Controller's subscription maximum
NexusAI for Compliance	Employees, contractors, and customers	Any personal data included in captured content (including e-mails, instant messages, social media content, associated message telemetry and attachments)	NexusAI for Compliance uses machine learning to evaluate supported archived messages (such as email, social media, collaboration platforms, and mobile messages) flagged for Customer's review by Proofpoint's Intelligent Supervision product.	Up to 24 hours from the end of Controller's subscription maximum
Nexus People Risk Explorer	Employees, contractors	Names, e-mail addresses, any Personal Data contained in Threat Analytics	Proofpoint Nexus People Risk Explorer leverages people centric security data from Proofpoint's Targeted Attack Protection, Security Awareness Training, Cloud Account Defense and Cloud Account Security Broker to provide insights into the types, severity and frequency of threats targeted at Customer and its employees.	Up to 90 days from the end of Controller's subscription maximum
Anti-Phishing Suite : includes PhishAlarm and PhishAlarmAnalyzer:	Employees, contractors	Name E-mail address Any Personal Data included in an e-mail	Routing and scanning suspicious emails reported by the end users with the PhishAlarm button. PhishAlarm Analyzer delivers highly responsive identification of phishing attacks in real time. Emails reported via PhishAlarm & PhishAlarm Analyzer are accessed and categorized and they are immediately available to Customer's response teams.	Up to 30 days from the end of Controller's subscription maximum; with the exception of Threat Analytics, which are retained for up to 18 months after collection

Proofpoint Security Awareness Training (PSAT)	Employees, contractors	name, e-mail address, and additional data fields selected by the customer for upload to PSAT from customer's Active Directory	Personal data is used for the rollout of employee Cyber Security Awareness training and employee security assessments and reporting	Up to 90 days from the end of Controller's subscription maximum; however, during Controller's subscription, Controller's admins may make changes to and delete users.
Secure E-Mail Relay (SER)	Employees Contractors Any recipients of bulk e-mails sent via Customer's corporate e-mail system	Name E-mail address Any Personal Data included in an e-mail	Secure Email Relay (SER) is a hosted, multi-tenant solution that puts Customer in control of applications that send email using Customer's owned or controlled domains. It adds a layer of security to each application and distributes the email to the Internet in a DMARC-compliant fashion after Proofpoint AS/AV checks are performed. SER may only be used for delivery of emails that comply with applicable bulk or unsolicited message laws.	Up to 30 days from the end of Controller's subscription maximum
SecureShare	Employees, contractors, any other individual invited to view a shared file	Name, e-mail addresses	SecureShare is a secure method for the sharing of files and temporary storage of such files.	Up to 180 days after collection.
Targeted Attack Protection (TAP)	Employees, contractors, customers any other individual sending or receiving e-mails via Customer's corporate e-mail system	Name E-mail address Any Personal Data included in an e-mail	TAP identifies and protects against malicious URLs and malicious attachments in emails using a dynamic malware analysis engine.	Up to 18 months after collection.
Threat Response Auto-pull (TRAP)	Employees, contractors, customers any other individual sending or receiving e-mails via Customer's corporate e-mail system	Name E-mail address Any Personal Data included in an e-mail	TRAP is an incident management platform that includes automation to analyze and remove unwanted emails.	Retention of closed incidents is established by Controller. Full message MIME data purged every 30 days for closed incidents.
ThreatSimulator	Employees, contractors	Name E-mail address	Personal data is used for simulated phishing campaigns. Customer may only conduct simulated phishing emails to domains owned or controlled by the Customer.	Upon customer request and within 90 days following such request.
Zero Trust Network Access (formerly Meta)	Employees, contractors	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	Meta overlays a zero-trust network on top of customer'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	Up to 90 days from the end of Controller's subscription maximum

		disable logging internet traffic events)	corporate network is accessed based on the user's unique identity	

1. Subprocessors

A current list of subprocessors can be found at https://www.proofpoint.com/us/legal/trust.

APPENDIX 2 TO THE DPA – SECURITY OF PROCESSING

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall implement the measures outlined below to ensure an appropriate level of security for the provision of the Services:

A. *User Authentication*

Management has established and approved an information security program.
A framework of information security policies and standards has been developed, which supports the objectives of the information security program.
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 role using the concept of least privilege.
A process is in place to monitor failed login attempts. Identified security violations are resolved.
Access to the Processor production environment by Processor employees is granted 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 customer end user access are documented in the service-specific Administrator Guides and are controlled by customer administrators through the service dashboard, user interface or SAML integration.

B. *Execution of backup copies*

Customer configuration and report data are backed up on a regular basis and stored on spinning disk.

Procedures for backup and retention of data and programs have been documented and implemented.

C. *Computers and access terminals*

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

Data Processor 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 Processor's Security Code of Conduct, a summary of Processor's information security program, which they are required to acknowledge receipt of.
Access to the Processor production environment by Processor employees is granted based on business need. A two-factor authenticated VPN is utilized.

Centralized configuration management tools are used to ensure employee endpoints are appropriately configured.

D. ***Access logs***

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

All access attempts to Data Processor computer systems are centrally logged and unusual activity is automatically reported to Processor's Global Information Security group. In addition, Processor enforces account lockout policies and password requirements. Logs of customer access to the Services are generated and retained as applicable for each Service.

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.

E. ***Telecommunication systems***

All Processor production facilities have redundant internet feeds from diverse bandwidth providers.

F. ***Instruction of personnel***

All Processor personnel are required to complete an annual online Security and Awareness training program. In addition, personnel may receive on-going training specific to their roles. This training may be provided by Proofpoint or other third-party organizations.

Processor 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 Processor corporate functions.
Personnel roles and responsibilities are clearly defined.

G. ***Use of computers***

Remote access to Processor production networks is restricted to systems running Processor-approved and managed security software. All Processor systems provided to personnel are managed by a centralized configuration system. All Processor employees are made aware of Processor's acceptable use policies for Processor computers, internet access and email communications. Processor employees must acknowledge these policies and agree to abide by them.

New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.
New employees review and acknowledge Processor's Security Code of Conduct.

H. ***Printing of data***

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

K. ***Physical Access Control***

Data Processor Controls

With products hosted from Processor's co-location providers, Processor maintains controls over physical access to the Processor infrastructure. With products hosted from hosting providers AWS, Azure or Google Cloud, physical access is controlled by the hosting provider.

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

Co-location facilities' physical security controls are aligned with Tier-III data center standards, including 24x7 on-site security, staffed points of access, anti piggy-backing mechanisms, dual-factor authentication and monitored CCTV. Facilities used by AWS, Azure or Google Cloud are aligned with Tier-III data center standards.

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

Data Processor Controls

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

1. All Data Processor employees and contractors are provided with unique user IDs. 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. Must not appear on public lists of breached passwords
    c. History of 23
    d. Required to change every 180 days
    e. Account locked out after five (5) failed login attempts
3. Logical access is granted based on role.
4. Audit logging is in place on the VPN to the Data Processor 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 Processor Global Information Security group.

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

Customer data is not permitted to reside in the Processor corporate environment. Access to systems hosting the Services are controlled in the following ways:

1. Access is based on role at Processor.
2. Only authorized Processor personnel are permitted to have privileged access to a Processor Production Environment.

O. ***Audit logging*** is in place on the VPN and on systems in the Processor Production Environment.

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

Access to the Processor Production Environment is granted based on role.

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

Processor does not permit Customer data to reside in the Processor Corporate Environment, where Processor employees and contractors reside. The Processor Production Environment is logically and physically separated from the Processor Corporate Environment:

1. Access to the Processor Production Environment is via a two-factor authenticated VPN using Processor-approved devices and is only provided to Processor 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 Services with all others denied by default.
3. All Administrator access to the Services hosted web interfaces is encrypted using HTTPS/TLS.

System Access Controls

1. LDAP is used to authenticate Processor personnel to the production environments.
2. Privileged access is only granted to authorized Processor personnel.

Endpoint Security

1. Endpoints used to access the Data Processor production environment are centrally-managed, have applicable security patches installed, run standardized security software and are regularly scanned for vulnerabilities.

Server Security

1. Applicable security patches are applied based on criticality.
2. Unnecessary services are disabled.
3. Default passwords are changed.

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

1. All Administrative access by Processor to the Services is encrypted using HTTPS/TLS.

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

The functionality provided by the Services is performed automatically and does not require human intervention, except for analytic purposes and in order to troubleshoot issues with the Services. The Services are designed to function as described in the Services Agreement.

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

Access to systems used by the Services are controlled in the following ways:

1. Access is granted based on role at Processor.
2. Only authorized personnel are permitted to have privileged access to the Processor Production Environment.
3. Audit logging is in place on the VPN and on systems in the Processor Production Environment.
4. Service-generated audit logs capture access to Services by Data Controller personnel.

U. ***Ensuring Compliant Data Processing***

Except for analytic purposes and to troubleshoot issues with the Services Processor personnel do not manually process customer data. All customer data is automatically processed by the Services, as described in the Services documentation.

V. ***Ensuring Availability***

This is accomplished in the following way:

1. Infrastructure in each production facility is configured in high-availability mode, including dual power feeds and a minimum of two diverse network connections.
2. Co-location facilities are aligned with Tier-III data center standards, including redundant power and redundant environmental controls.
3. Co-location facilties have on-site generators with a minimum of two (2) day fuel supply.
4. A Business Continuity Action Plan for the protection of Data Processor personnel and the recovery of Data Processor business processes is documented and tested annually.
5. A distributed monitoring infrastructure monitors for availability and performance.
6. .

W. ***Data Separation***

The Services maintain separation of customer data. This is accomplished in the following way:

1. Logical separation is maintained by the service using some or all of the following:
    a. Unique Client IDs for each client that are used to tag client data within the service;
    b. Unique IPs; or
    c. Unique encryption keys.

SCHEDULE 2

Standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

STANDARD CONTRACTUAL CLAUSES

controller to processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 –Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);
(viii) Clause 18 – Clause 18(a) and (b)
(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause – Not Applicable

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

Transfer controller to processor

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other

confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time,

the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

(4) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
(ii) refer the dispute to the competent courts within the meaning of Clause 18.
(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority. [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679]: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);
   (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

---

(12) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of

the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be: (a) the laws of the country specified in the Services Agreement if the Services Agreement is governed by the laws of an EU member state, or (b) the laws of the Netherlands if the Services Agreement is governed by the laws of a third country.

Clause 18
Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(a) The Parties agree that those shall be the courts (i) specified in the Services Agreement if the Services Agreement has appointed a Court of an EU member state, or (ii) the Courts of Amsterdam if the Services Agreement has appointed a Court of a third country.
(b) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(c) The Parties agree to submit themselves to the jurisdiction of such courts.

EXPLANATORY NOTE:

APPENDIX

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s): The data exporter is the identified as Controller on page 1 of this DPA**.**

Data importer(s): The data importer is Proofpoint, Inc., a provider of email and social media security services, threat analytics, and security training.

B. **DESCRIPTION OF TRANSFER**

Data subjects are Controller's employees and contractors, and the employees and contractors of Controller's customers and vendors

Categories of data: The categories of data are identified in Appendix 1 to this DPA. Controller will not transfer sensitive data to Proofpoint.

Processing operations: The frequency of transfer, nature and purpose of the processing, retention period are identified in Appendix 1 to this DPA.

C. **COMPETENT SUPERVISORY AUTHORITY** ***Identify the competent supervisory authority/ies in accordance with Clause 13***

[Where the data exporter is established in an EU Member State:] The supervisory authority of the Member State of the registered office of the data exporter.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State of the registered office of the data exporter.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of the Netherlands

---

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The security, technical and organizational measure are described in Appendix 2 to this DPA.

ANNEX III

LIST OF SUB-PROCESSORS

The current list of subprocessors for the Service is available on Proofpoint Trust Site at: https://www.proofpoint.com/us/legal/trust

---