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., 892 Ross Drive, Sunnyvale, CA 94089 ("**Processor**") and is appended to either: (1) the Proofpoint General Terms and Conditions and applicable Product Exhibit(s), (2) the end user license agreement (a EULA, clickwrap, 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 Service 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 2010/87/EU (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. 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) and 2 (Standard Contractual Clauses) and the Appendices thereto. This DPA has been presigned 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. 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: _____

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

c. **Subprocessor** means any processor engaged by Proofpoint to process Personal Data.

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

2. **Processing of Personal Data.** It is the intent of the parties that, with respect to the activities described in Appendix 1, Controller's 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. 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 Services.

3. **Rights of Data Subjects.** Beginning May 25, 2018 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, object to the processing, or its 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.

4. **Limited use of Personal Data & personnel.** Processor (i) will not acquire any rights in or to the Personal Data; (ii) 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.

5. **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 Services. 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 Agreement with respect to the protection of Controller Data to the extent applicable to the nature of the Services provided by such subprocessor. Processor will be responsible for the acts and omissions of such subprocessors to the same extent Processor would be liable under this DPA if providing the Services directly. The current list of subprocessors for the Services is identified in Appendix 3 of the Standard Contractual Clauses (attached hereto as Schedule 2). 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 Order Form(s) with respect only to those Services 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.

5. **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.

6. **Security of Personal Data.**

a. **General.** Processor shall maintain appropriate technical and organizational measures for the security and protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data. Processor will not materially decrease the overall security of the Services during the terms of the Services Agreement and this DPA.

b. **Specific Technical and Organizational measures.** 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 Data Subjects, Processor and its affiliates will implement the measures described in Appendix 2.

7. **Cooperation with Supervisory Authorities.** Upon Controller's request, Processor shall provide Controller with reasonable cooperation and assistance, at Controller's expense, needed to fulfill Controller's obligation under the GDPR to carry out a data protection impact assessment related to Controller's use of the Services, 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 Section 7 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.

8. **Legal and other disclosures.** In the event that Processor is legally obliged to disclose Controller Data to satisfy legal requirements; comply with law; respond to lawful requests or legal process; or otherwise in accordance with this DPA, promptly after it becomes aware that it will be legally obliged to make such a disclosure it shall, unless prohibited by law, notify Controller in writing of the legal directive, the reason and the form of the disclosure.

9. **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. If either party's negligence directly and solely causes a Security Breach and such unauthorized third party is one whom is reasonably suspected to misuse such Personal Data, then the negligent party shall pay the reasonable costs and expenses for breach notification and credit monitoring as required by applicable law for a period of twelve (12) months.

10. **Privacy Shield.** Processor is certified with the EU-US Privacy Shield and Swiss-US Privacy Shield regimes. Detailed information can be found at www.privacyshield.gov; look up Proofpoint on the Certified List.

SCHEDULE 2

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection, the entity on affiliated entities signing below as the **Data Exporter** and PROOFPOINT, INC. as the **Data Importer** have agreed to the following Contractual Clauses (the **Clauses**) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the data subprocessor'* means any processor engaged by the data importer or by any other data subprocessor of the data importer who agrees to receive from the data importer or from any other data subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the data subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the data subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any data subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of processing, the processing activity is carried out in accordance with Clause 11 by a data subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

    (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

    (ii) any accidental or unauthorised access, and

    (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound

by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the data subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any data subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or data subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his data subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a data subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the data subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the data subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the data subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any data subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any data subprocessor preventing the conduct of an audit of the data importer, or any data subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the data subprocessor which imposes the same obligations on the data subprocessor as are imposed on the data importer under the Clauses. Where the data subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the data subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the data subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the data subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. Data importer warrants that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is the identified as Controller on page 1 of this DPA.

Data importer

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

Data subjects

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

Categories of data

Each Proofpoint product has its own specific SCC Appendix Exhibit and the categories of data processed by Proofpoint are described therein. The product specific SCC Appendix Exhibits are found on the website www.proofpoint.com/legal/trust/dpa. Only those SCC Appendix Exhibits that cover Proofpoint products licensed to the Controller are incorporated herein and made a part of this this DPA.

Processing operations

Each Proofpoint product has its own specific SCC Appendix Exhibit and the processing operations are described therein. The product specific SCC Appendix Exhibits are found on the website www.proofpoint.com/legal/trust/dpa. Only those SCC Appendix Exhibits that cover Proofpoint products licensed to the Controller are incorporated herein and made a part of this this DPA.

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):

Each Proofpoint product has its own specific SCC Appendix Exhibit and the technical and organizational security measures implemented by Proofpoint are described therein. The product specific SCC Appendix Exhibits are found on the website www.proofpoint.com/legal/trust/dpa. Only those SCC Appendix Exhibits that cover Proofpoint products licensed to the Controller are incorporated herein and made a part of this this DPA.

These appendices form part of the Clauses and must be completed and signed by the parties. By signing the signature block on page 1 of this DPA the parties will be deemed to have signed these appendices.