January 17, 2026

Spambrella® - Data Processing Agreement (DPA)

EXHIBIT A – SPAMBRELLA – CHANNEL PARTNER/CUSTOMER TERMS & CONDITIONS

EXHIBIT A

SPAMBRELLA - CHANNEL PARTNER/CUSTOMER - PROGRAM TERMS & CONDITIONS

This GDPR Data Processing Agreement ("DPA") is between the entity identified below as the Channel Partner/Customer **("Data Controller")**, and Spambrella Ltd., 80 Churchill Square, Kings Hill, West Malling, Kent, ME19 4YU, United Kingdom ("**Processor**") and is appended to either to either (1) the General Terms and Conditions and applicable Product Exhibit(s) between the Controller and Processor, (2), the end user license agreement (a EULA, clickwrap, or clickthrough agreement) accepted by Controller's initial registration and access of the Spambrella product or service, or (3) any other written and signed license agreement between parties under which Processor provides products or services to Controller (the "**Services Agreement**"). This DPA is affective as of January 18th, 2024.

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 organisational 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 Spambrella's obligations set out in this DPA, Spambrella 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 Spambrella Ltd., and any reference to Data Exporter or Data Controller shall be deemed to be a reference to 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 Agreement hereby agree to be bound by the terms and conditions in the attached Schedules 1 and 2, and the Appendices thereto with effect from the date of this Agreement.

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 pre-signed by the Processor, Spambrella Ltd., 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 complete and signed DPA to Spambrella via email to privacy@spambrella.com

If Controller makes any deletions or other revisions to this DPA, this DPA will not be valid and will be null and void. Controllers 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 the earlier terminated pursuant to the terms of this DPA.

Accepted and agreed by Data Controller (Channel Partner / Customer)

Signature: _____

Name: _____

Date: _____

Company: _____

Address: _____

_____

Accepted and agreed by Spambrella Ltd (Processor)

Signature: 

Name: Mrs Rosie Howard - Chief Finance Officer (CFO)

Date: January 21, 2026

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 Spambrella 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@spambrella.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) or Partner Agreement 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 fulfil 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 fulfil 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 or Sub-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**. Spambrella's Subprocessor 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, Channel Partner's European union affiliated entities signing below as the **Data Exporter** and Spambrella Ltd. 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

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

1. **Data exporter (Data Controller)**

The data exporter refers to all **Strategic Partners, Channel Partner's, Customers and any affiliated European companies ("Customer").**

The Spambrella Email Security Services protect Strategic Partner, Channel Partner, Customer and its Affiliates from unwanted email that may pose a threat to compromise corporate IT systems, corporate data or Personal Data (and the privacy rights of the data subjects themselves). These SCCs and the Services do not cover email data that is outside of Partner's/Customers corporate email systems, for example, third party email or webmail exchanges on which individuals set up personal email accounts. The data exporter must provide standing instructions to internet email domain name servers to route internet email of Channel Partner/Customer and its Affiliates to the Spambrella Security Services.

2. **Data importer (Processor)**

The data importer (Processor) is **Spambrella Ltd.**

Data importer provides its on-demand Security Services from its subprocessor (Proofpoint, Inc) paired US-based datacenters and/or its paired Germany and Netherlands datacenters, at the election of the Customer and its Affiliates.

3. **Data subjects**

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

4. **Categories of data**

To the extent there is Personal Data within email sent to data exporter's corporate email systems via the Internet, then the following categories of data may apply: e-mail, email metadata and attached documents.

5. **Processing operations**

Mailflow Processes

- Inbound email flow
    - Typically, all data exporter actions are undertaken by the Customer entity that is managing the data exporter's email infrastructure. Data exporter updates its MX records to provide standing instructions to the email DNS so that when external parties send email intended for data exporter's corporate email domain, it is first routed directly to data importers Security Services for scanning, filtering and URL rewriting, and routing in transit. Provided that the external third-party sending email system supports TLS, data exporter may elect to enable TLS for all inbound email traffic providing encryption of email in transit. Data exporter may also enable TLS for all email routed to its on-premise email servers from the Security Services. Data exporter may also implement forced TLS rules for a manually maintained list of external sending email domains. Data exporter configures the duration of the temporary quarantine for suspicious (unwanted) emails to be available for manual review by the intended message recipient or data importer's email support staff. After scanning, filtering and URL rewriting, wanted email is routed to data exporter's on-premises email servers.

- Outbound email flow
    - Typically, all data exporter actions are undertaken by the Customer entity that is managing the data exporter's email infrastructure. Data exporter may enable TLS for outbound email routed from its on-premise email servers to the Security Services. Data exporter may implement forced TLS rules for a manually maintained list of external receiving email domains. Data Exporter may further enable opportunistic TLS for the remaining outbound email routed from the Security Services to the intended recipient email domain, provided that the external third-party receiving email system supports TLS.
- Data Importer's configuration, management and support functions
    - Data importer provides all necessary infrastructure, set-up configuration and support services required to offer the Security Services. Typically, all data exporter actions are undertaken by the Channel Partner entity that is managing the data exporter's email infrastructure. Data exporter is responsible for configuring, administering and managing the rule and policy-related functions of the Security Services and for managing all aspects of its own email infrastructure. Data exporter creates support tickets to receive technical support from data importer's email support staff.

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

Data importer may only correct, delete or block the data processed on behalf of the data exporter when instructed to do so by the data exporter. However, given that email is in transit through the Security Services, it is not possible to correct email and associated content that might include Personal Data.

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

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

Data importer shall not use Personal Data for any other purpose except as permitted by the Services Agreement and the normal operation of the Security Services, which includes the temporary creation of copies and duplicates required to assure proper functioning of the Security Services, or any copies or duplicates required to comply with statutory or other required retention rules. Data from suspicious and unwanted emails, including email, URL and attachment metadata (which may include Personal Data), may be stored for analysis for up to 120 days from the point of initial transit through the Services or in perpetuity, depending on the nature of the suspicious or threatening characteristic. All other data (such as Customer email policies and rules, quarantined emails, and non-malicious emails in route to Customer's email exchange) will be deleted within a reasonable period of time after termination.

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

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

Summary of Spambrella Internal Processes

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the data importer (the Provider entity processing the data) and signed by the Parties.

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):

A. Summary

This document summarizes the processes and procedures that Data Importer implements in conjunction with the provision of the Security Services. Additionally, this document includes the relevant controls evaluated on an annual basis by an independent auditor as part of the Data Importers ongoing SSAE 16 audit, or similar audit standard that Data Importer may adopt from time to time at its discretion.

B. Control Group

Identification and authentication of the user

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

Data Exporter end-users: Data Exporter administrative users and email recipients potentially may access personal data by viewing the Security Services quarantine through a web-browser based user interface. Data Exporter may elect to integrate its Active Directory with the Security Services to provide its administrators with the ability to grant or revoke access to the quarantine. Data Importer also has the ability to grant or revoke access for data exporter end users to the quarantine.

Data Importer users: Centralized authentication and logging is used to ensure that only approved Data Importer personnel have access to the Data Importer data centers and the Security Services infrastructure, including the quarantine and certain back-end services that analyze suspicious and unwanted email contents, metadata and attachments. All members of the Spambrella Security Operations team receive specific training in the administration of the Spambrella Security Services Administration.

Data Importer Controls

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

Type of access

The various types of Data Exporter end user access are documented in the Administrator Guide and are controlled by Data Exporter administrators through Active Directory. End user access can also be added importing CSV files or manually entering through the user interface.

C. Collection of data

Inbound email to the Data Exporter is filtered in memory by the Security Services. In this instance, email destined for email domains configured by Data Exporter to point to the Security Services are received at the Data Importer Production data centers, scanned and filtered in memory, and forwarded to the Data Exporter email infrastructure, unless directed to the Email Quarantine in the Data Importer Production data centers based on Email Filters and Policies configured by Data Exporter.

Data Importer Controls

All email processed through the Security Services is stored for 30 days, and then automatically deleted at the end of the 30-day period.

D. Execution of backup copies

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

Data Importer Controls

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

E. Computers and access terminals

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

Data Importer Controls

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

F. Access logs

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

The first relates to access by Data Exporter end-users to the Data Exporter Quarantine through the hosted Data Exporter End-user Interface in the Data Importer Production data centers. Access logs for Data Exporter end-users consist of Security Service-generated security logs that contain access information and are available only to Data Exporter Administrators. The second type of access logs are for the physical and logical access to Data Importer production systems by Data Importer employees. Physical access logs for all Data Importer data centers are retained for a minimum of 90 days and reviewed on a monthly basis by the Security Operations group. As well, all access attempts to Data Importer computer systems are centrally logged and unusual activity is automatically reported to Data Importer Security Operations group. In addition, Data Importer enforces account lockout policies, password complexity requirements, and password age requirements.

Data Importer Controls

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

G. Telecommunication systems

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

H. Instruction of personnel

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

Data Importer Controls

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

I. Use of computers

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

Data Importer Controls

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

J. Printing of data

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

Data Importer Controls

New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.

New employees also receive a copy of Data Importer's Employee Handbook.

K. Physical Access Control

Controls of Subprocessor (Proofpoint, Inc).

Subprocessor (Proofpoint, Inc) maintains controls over physical access to the Data Importer Production Environment in the following manner:

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

L. Physical Security Measures for Data Centers

Country	Address	Personal Data processed
United States of America	Santa Clara, CA	Email Data
United States of America	Atlanta, GA	Email Data
United States of America	Riverton, Utah	Email Data
Germany	Frankfurt	Email Data
Netherlands	Amsterdam	Email Data

Data Importer Controls

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

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

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

Data Importer Controls

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

1. All Data Importer employees and contractors are provided with unique userIDs. Account sharing is not permitted.
2. Password requirements are defined and enforced by a password synchronization tool. Requirements include:
    a. Minimum of 12 characters
    b. Complexity rules (3 of 4 – upper, lower, numbers, special characters)
    c. History of 23
    d. Required to change every 60 days
    e. Account locked out after five (5) failed login attempts
3. Logical access is granted based on role.
    a. Only members of the Operations group are granted privileged access to the Data Importer Production Environment.
4. Audit logging is in place on the VPN to the Data Importer Production Environment.
5. Audit logs are monitored in near real-time by a log aggregation and alerting tool. Alerts are configured to be sent to the Data Importer Security Operations group.
6. Data Exporter is provided with the option of enabling encryption for email data at rest in the Email Quarantine.
7. Data Exporter is provided with the option of enabling encryption for email data in transit between the Security Services and the Data Exporter email infrastructure.

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

Data Importer Controls

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

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

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

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

Data Importer Controls

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

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

Data Importer Controls

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

1. Access to the Data Importer Production Environment is via a two-factor authenticated VPN and is only provided to Data Importer employees and contractors whose role requires access.
2. Industry-standard firewalls are in place and configured to only permit traffic on ports necessary for the functioning of the Service with all others denied by default.
3. Network-based IDS is configured to monitor traffic inbound from and outbound to the Internet. Alerts are configured to be sent to the Data Importer Security Operations group.
4. All intra-Service communications are encrypted using TLS.
5. All Administrator and End-User access to the Security Services hosted web interfaces is encrypted using TLS.

System Access Controls

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

Endpoint Security

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

Server Security

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

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

Data Importer Controls

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

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

Data Importer Controls

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

T. *Monitoring and Testing phase controls*

Data Importer Controls

The functionality provided by Spambrella Security Services is performed automatically and does not require human intervention, except in order to troubleshoot issues with the Security Services. The Security Services filters email directed at the Security Services by the Data Exporter. Filtering is performed in compliance with Data Exporter-configured Rules, Policies and Filters. Data Exporter email data is not changed as part of the Security Services.

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

Data Importer Controls

Access to systems filtering Data Exporter email data are controlled in the following ways:

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

The Security Service controls access in the following way:

1. Administrative access to the Administrator Web Interface by Data Exporter administrators is granted by Data Importer at the request of Data Exporter of by the Data Exporter itself.
2. End-User access to the End-User Web Interface is granted by Data Exporter and the End-User creates a password for the End-User's login authentication. The Data Exporter's administrator can change the End-User password.
3. The Security Services generate Application Logs that include Administrator and End-User access and include the following:

    a. Successful/Failed login attempts
    b. Date
    c. Time
    d. Source IP
    e. userID

V. *Ensuring Compliant Data Processing*

Data Importer Controls

Data Importer personnel do not manually process Data Exporter data. All Data Exporter email data is automatically filtered by the Security Services, as described in the Security Services documentation.

W. *Ensuring Availability*

Data Importer Controls

The Security Services are architected to ensure Availability in-line with published Data Importer's SLA's (End User License Agreement). This is accomplished in the following way:

1. The Spambrella Security Services are configured to run in primary/alternate roles between a pair of geographically-diverse data centers. The data center roles can be changed on demand.
2. Infrastructure in each data center is configured in high-availability mode, including dual power feeds and a minimum of two diverse network connections.
3. Data centers are a minimum of Tier-3 with redundant power and redundant environmental controls.

4. Data centers have on-site generators with a minimum of three (3) day fuel supply.
5. Data Exporter Configuration Data is backed up daily for Disaster Recovery purposes.
6. A documented Disaster Recovery Plan is documented and tested annually.
7. A documented Business Continuity Action Plan is documented and tested annually.
8. A distributed monitoring infrastructure monitors for Availability.
9. Industry-standard firewalls are configured to permit ports necessary for the Service and deny all others by default.
10. All Data Importer and subprocessor owned Windows and Mac laptops, workstations and servers in the Data Importer Corporate Environment run industry leading anti-virus services.

X. ***Data Separation***

Data Importer Controls

The Spambrella Security Services maintain segregation of Data Exporter email data. This is accomplished in the following way:

1. Each Data Exporter is provided with shared IPs particular to the geographic location of the Security Services.
2. Data Exporter's instance of the Security Services is configured to only filter email for the Data Exporter.
3. Systems making up the Data Exporter's instance of the Security Services are configured to only communicate with other systems filtering the Data Exporter's email.

Data Exporter email data is not permitted in the Data Importer Development or QA environments without being specifically requested in writing by the Data Exporter as part of a troubleshooting exercise.

