SUB-PROCESSING CLAUSES (BETWEEN MIMECAST AND PARTNER)

Mimecast and Partner are parties to a certain Managed Services Provider Agreement (the "**Agreement"**). These Sub-Processing Clauses are incorporated into and form part of the Agreement and shall supersede and replace any and all prior agreements and undertakings, oral or written, between the Partner and Mimecast regarding the Processing of Customer Data via the Services. For the purposes of the Agreement and these Sub-processing Clauses (also referred to herein as "**DPA**"), all capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions

"**Affiliate**" means an entity that controls, is directly or indirectly controlled by, or is under common control of the relevant party;

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to Applicable Law, and (b) is permitted to use the Services pursuant to the Customer Agreement between Customer and Data Processor, but has not signed its own Customer Agreement with Data Processor and is not a "Customer" as defined under the Agreement;

"**Applicable Law**" means one or more of the following data protection laws or regulations as applicable to the Processing of Personal Data by Mimecast under this DPA: (i) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**"); (ii) the Data Protection Act 2018 and the United Kingdom Data Protection Regulation("**UK GDPR**"); (iii) the (Singapore) Personal Data Protection Act 2012 ("**PDPA**"); (iv) the data protection regulations of the United States, including but not limited to California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CCPA**"); (iv) the South Africa Protection of Personal Information Act ("**POPIA**"); (v) the Australia Privacy Act 1988 (No. 119 1988)(as amended), (vi) Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"); and (vii) any relevant law, statute, regulation, legislative enactment, order or other binding instrument that implements or amends the foregoing;

"Customer" (also "**Data Controller**") means party receiving the Services under a Customer Agreement with the Managed Services Provider;

"**Customer Agreement**" means the agreement between Customer and Partner regarding the provision of certain Services by Sub-Processor, which shall include the Data Processing Flow-Down Terms appended to the Agreement as [Appendix •];

"**Customer Data"** means the data provided by Data Controller for Processing via the applicable Services, including but not limited to, the contents of the files, emails or messages sent by or to a Permitted User of the Services Customer Data does not include Threat Data (as defined under Section 12.2);

"**Data Subject**" means (i) "data subject" as defined under the GDPR, (ii) "consumer" or "household" as defined under the CCPA; and/or (iii) such similar term as used under the relevant Applicable Law;

"**Data Subject Access Request**" refers to a request from (i) a Data Subject in accordance with the GDPR, UK GDPR and/or the CCPA and/or (ii) such similar term under the relevant Applicable Law;

"EU Standard Contractual Clauses" means the standard contractual clauses approved by the European Commission in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on 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, as applicable (referencing Module 3: Transfer Processor to Processor) and as may be amended or replaced by the European Commission from time-to-time;

"Hosting Jurisdiction" means the country where the data center hosting the Customer Data is stored and will be noted on the relevant Services Order. Notwithstanding the foregoing, the Hosting Jurisdiction for Mimecast's DMARC Analyzer Service is Ireland and for the BEP Service is Belgium and The Netherlands;

"**Instructions**" means (i) instructions from Customer as embodied in the Customer Agreement for the provision of the Services (to the extent they are communicated to the Sub-Processor), (the "**Business Purpose**" as defined under the CCPA) and (ii) those as may be additionally communicated by the Data Controller to Mimecast via the Data Processor from time-to-time;

"Partner" (also "**Data Processor**") means a managed service provider ("MSP") reselling the Services to Customers;

"**Personal Data**" means (i) "personal data" as defined under the GDPR and/or UK GDPR, (ii) "personal information" as defined under CCPA; and/or (iii) such similar term under the relevant Applicable Law, that is under the control of Customer and Processed by Sub-Processor in connection with the performance of the Services;

"**Process**", "**Processed**" or "**Processing**" means "processing" as defined under Applicable Law, the details of which are outlined in Schedule 1;

"**Regulator**" means the data protection supervisory authority which has jurisdiction over the Customer's Processing of Personal Data;

"**Sale**", "**Sell**" or "**Selling**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data with a Third Party, whether for monetary or other valuable considerations or for no consideration, for the Third Party's commercial purposes;

"**Services**" means any and all services provided by Sub-Processor as identified in the Customer Agreement and described further in an ordering document referencing the Customer Agreement;

"**Standard Contractual Clauses**" means the Eu or UK government approved contract mechanism for the cross-border transfer of Personal Data from the EEA, Switzerland or the UK (as applicable) to Third Countries;

"**Sub-Processor**" (also "**Service Provider**") means the Mimecast entity providing the Services as identified in the Agreement between the Sub-Processor and the Data Processor;

"**Third Party**" means any person (including companies, entities, organizations, etc.) that is not Customer, Partner, or Sub-Processor;

"**Third-Party Subcontractor**" means the Third-Party Subcontractors engaged by the Sub-Processor and listed in Schedule 3, as such list may be updated from time to time pursuant to Clause 9;

"**Third Country(ies)**" means countries outside of the scope of the data protection laws of the European Economic Area, Switzerland and/or the United Kingdom (as applicable), excluding countries approved as providing adequate protection for Personal Data by the European Commission or the Information Commissioner's Office (as applicable) from time-to-time;

"**Trust Center**" means the website created by Sub-Processor which includes relevant content referenced in this DPA and otherwise related to Applicable Law as well as Sub-Processor's operations and is found here: https://www.mimecast.com/company/mimecast-trust-center/; and

"UK Addendum" shall mean the UK International Data Transfer Addendum issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018 as may be updated from time to time, currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

2. Data Processing.

2.1 Sub-Processor shall only process Personal Data on behalf of the Customer in accordance with and for the purposes set out in the Instructions which, for the avoidance of doubt and depending on the Services provided, may include Sub-Processor: (i) providing the Customer with access to and use of the Services; and (ii) if applicable, improving and developing the Services, including but not limited to using Threat Data to train the Service's machine-learning algorithms, the output of which are anonymized and irreversible. Notwithstanding the foregoing, Processing may be required by Union or Member State law to which the Sub-Processor is subject; in such a case, the Sub-Processor shall inform the Data Processor of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

2.2 If the CCPA is applicable,

Sub-Processor shall act as a Service Provider and certifies that it shall Process Customer Personal Data on behalf of the Data Controller in accordance with and for a Business Purpose. Further, it will not Sell the Data Controller's Personal Information and will otherwise comply with the CCPA requirements imposed on Service Providers. Notwithstanding the foregoing, Sub-Processor may Process Customer Personal Data as may otherwise be permitted for service providers or under a comparable exemption from "Sale" under Applicable Law, as reasonably determined by Sub-Processor;

2.3 Each party shall comply with its obligations applicable to that party under Applicable Law.

2.4 Sub-Processor represents and warrants that:

(i) it shall promptly inform Data Processor if, in Sub-Processor's opinion: (a) Sub-Processor cannot comply with Applicable Law; or (b) Data Processor's or Data Controller's Instructions violate Applicable Law, provided that Sub-Processor is not obliged to perform a comprehensive legal examination with respect to an Instruction of Data Processor or Data Controller;

(ii) its personnel and Third-Party Sub-processors who are authorised to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and

(iii) it certifies and understands the restrictions placed on it under subparagraph (iii) above.

2.5 Data Processor represents and warrants and, where applicable, shall procure that Data Controller represents and warrants, that:

(i) the Data Processing Flow Down Terms are part of the Customer Agreement entered into between Data Controller and Data Processor.

(ii) its use of the Services and the Instructions provided do not contravene Applicable Law;

(iii) it has complied and continues to comply with Applicable Law, in particular that it has obtained any necessary consents and/or given any necessary notices, and/or otherwise has the right to disclose Personal Data to Sub-Processor and enable the Processing set out in this DPA and as contemplated by the Agreement;

(iv) it has assessed the requirements under Applicable Law as they apply to the Data Processor and, where appropriate, the Data Controller with regard to Personal Data and finds that the security measures referenced in Schedule 2 are adequate to meet those requirements; and

(v) it will ensure compliance with and shall not in any way alter or diminish such security measures referenced in Schedule 2 to the extent applicable to the Data Processor, or where applicable the Data Controller, through its use of the Services;

2.6 Data Processor understands that Personal Data transferred to Sub-processor is determined and controlled by Customer in its sole discretion. As such, Sub-processor has no control over the volume, categories and sensitivity of Personal Data Processed through its Services by Customer or its users. Sub-Processor shall implement and maintain the technical and organisational security measures specified in Schedule 2 attached hereto before processing Customer's Personal data and shall continue to comply with such technical and organizational security measures as a minimum standard of security during the term of the Agreement.

3. Notification of Security Breach. In the event of a declared breach of security which has led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer's Personal Data which affects the integrity, availability or confidentiality of Customer's Personal Data (**"Security Breach"**):

(a) by the Data Processor, Data Processor shall notify Sub-Processor without undue delay (and in no event more than 48 hours, with periodic updates to follow as may be necessary); or

(b) by the Sub-Processor, Sub-Processor shall notify Data Processor without undue delay (and in no event more than 48 hours, with periodic updates to follow as may be necessary). Data Processor shall notify the Data Controller of any Security Breach.

For the avoidance of doubt, Security Breaches will not include unsuccessful attempts to, or activities that do not, compromise the security of Personal Data including, without limitation, unsuccessful log in attempts, denial of service attacks and other attacks on firewalls or networked systems and no notice of the foregoing shall be required. In the event a Security Breach requires notification by Data Controller or Data Processor to Data Subjects or relevant Regulators, the parties agree, and Data Processor will obtain the cooperation of Data Controller, to coordinate in good faith on developing the content of any public statements or required notices.

4. Audit and Inspection.

4.1 Taking into account the nature of the Processing and the information available to Sub-Processor, Sub-Processor shall provide reasonable assistance in response to inquiries from Data Controller or a competent Regulator relating to Sub-Processor's Processing of Data Controller's Personal Data.

4.2 Sub-Processor shall, upon written request from Data Processor, provide Data Processor with information reasonably necessary to demonstrate compliance with Sub-Processor's obligations set forth in this DPA. This information shall consist of permitting examination of the most recent reports, certificates and/or extracts prepared by an independent auditor pursuant to Sub-Processor's ISO270001 or similarly held industry certification(s).

4.3 In the event the information provided in accordance with Section 4.2 above is insufficient to reasonably demonstrate compliance, Sub-Processor shallpermit Data Processor (or Data Controller's Regulator)

to inspect or audit the technical and organisational measures of the Sub-Processor for the purposes of monitoring compliance with Sub-Processor's obligations under this DPA. Any such inspection shall be:

(a) at Data Processor's expense;

(b) limited to no more than once per any twelve (12) calendar month period, except if (i) required by instruction of a competent Regulator; or (ii) in case of a Security Breach;

(c) limited in scope to matters specific to Data Controller;

(d) agreed in advance between the parties in writing, including scope, duration and start date and Sub-Processor's then-current rates for professional services will apply;

(e) conducted in a way which does not interfere with the Sub-Processor's day-to-day business;

(f) during local business hours ofSub-Processor and, upon not less than twenty (20) business days' advance written notice unless, in Data Processor's reasonable belief, an identifiable, material non-conformance has arisen;

(g) subject to the confidentiality obligations in the Agreement; or where the audit is conducted by a third-party auditor such third-party auditor must be a professional bound by a duty of confidentiality or subject to a suitable non-disclosure agreement; and

(h) any audit conducted under this Section shall not be conducted by a party who is a competitor of Sub-Processor or provides services to a competitor of Sub-Processor.

4.4 Data Processor will provide Sub-Processor with copies of any audit reports generated in connection with any audit under this Section, unless prohibited by Applicable Law. Data Processor and/or Data Controller may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this DPA.

4.5 For the avoidance of doubt, the provisions of Clause 4 shall also apply to the audit provisions of any Standard Contractual Clauses entered into in accordance with Clause 7 of this DPA.

5. Compliance, Co-operation and Response.

5.1 Taking into account the nature of the Processing and the information available to Sub-Processor, Sub-Processor will provide reasonable assistance to Data Processor and/or Data Controller in complying with any Data Subject Requests or requests received by Data Processor or Data Controller from Regulators that occur in accordance with Applicable Law.

5.2 If Sub-Processor receives a Data Subject Request, and it is clear from the nature of the request without the need for any independent investigation that Data Processor or the Data Controller is the applicable controller of Data Subject's Personal Data, Sub-Processor will refer the Data Subject to the Data Processor and/or Data Controller, unless otherwise required by Applicable Law.. In the event Sub-Processor is legally required to respond to the Data Subject, Data Processor will, and will require the Data Controller to, fully co-operate with Sub-Processor as appropriate. Data Processor agrees, and will procure that the Data Controller agrees, that provision of technical tools to enable Data Processor (or Data Controller as appropriate) to take the necessary action to comply with such request/s, shall be sufficient to discharge Sub-Processor's obligations of assistance hereunder. Data Processor will reimburse all reasonable costs incurred by Sub-Processor as a result of reasonable assistance provided by Sub-Processor under this Section 5.

6. Cross-Border Transfers.

6.1 Data Processor acknowledges and agrees, and shall procure that Data Controller acknowledges and agrees, that Sub-Processor may, in the course of providing the Services, Process (or permit any Affiliate or Third-Party Subcontractor to Process) Personal Data in one or more Third Countries, provided that such Processing takes place in accordance with the requirements of Applicable Law. In such case, the Sub-Processor shall comply with (or procure that any Affiliate or Third-Party Subcontractor comply with) the data importer obligations in the applicable Standard Contractual Clauses.

7.2 If, in fulfilling its obligations under the Agreement or pursuant to other lawful Instructions from the Data Controller Personal Data is to be transferred from the European Economic Area, Switzerland and/or the UK (as applicable) by Data Controller and/or Data Processor to Sub-Processor to any Third Country, the parties agree to enter into and abide by the EU Standard Contractual Clauses and/or UK Addendum (as applicable) which are incorporated into this DPA as follows:

(i) Data Processor is the Data Exporter and Sub-Processor is the Data Importer (the foregoing shall apply with respect to Table 1 of the UK Addendum);

(ii) In Clause 7, the "Docking Clause (Optional)", shall be deemed incorporated (the foregoing shall apply with respect to Table 1 of the UK Addendum);

(iii) In Clause 9, the parties choose Option 2, 'General Written Authorisation', with a time period of 20 days (the foregoing shall apply with respect to Table 2 of the UK Addendum);

(iv) the optional wording in Clause 11 shall be deemed not incorporated (the foregoing shall apply with respect to Table 2 of the UK Addendum);

(v) In Clause 13, the competent Regulator shall be the Bavarian Data Protection Authority (Bayerisches Landesamt für Datenschutzaufsicht).

(vi) In Clause 17, the Data Exporter and Data Importer agree that the EU Standard Contractual Clauses shall be governed by the laws of Germany, and choose Option 1 to this effect (Part 2, Section 15(m) of the UK Addendum shall apply);

(vii) In Clause 18, the Data Exporter and Data Importer agree that any disputes shall be resolved by the courts of Munich, Germany(Part 2, Section 15(n) of the UK Addendum shall apply);

(viii) In accordance with Section 19 of the UK Addendum and Section 6.4 of this DPA, neither party may end the UK Addendum when the UK Addendum changes;

(ix) Completed Annexes I, II and III of the EU Standard Contractual Clauses and Annexes 1B, II and III of Table 3 of the UK Addendum are included in Schedules 1-3 herein; and;

(x) Notwithstanding the fact that the Standard Contractual Clauses are incorporated herein by reference without the Standard Contractual Clauses actually being signed by the parties, the parties agree that the execution of this DPA is deemed to constitute its execution of the Standard Contractual Clauses on behalf of the Data Exporter or Data Importer (as applicable), and that it is duly authorized to do so on behalf of, and to contractually bind, the Data Exporter or Data Importer (as applicable) accordingly;

(xi) The parties agree that the Standard Contractual Clauses shall cease to apply to the Processing of Personal Data if and to the extent that the relevant transfer of Personal Data ceases to be a “restricted transfer”; and

(xii) The provisions in this DPA shall be without prejudice to the parties' ability to rely on any other legally valid international data transfer mechanism for the transfer of data out of the EEA, Switzerland and/or the UK.

7.3 The parties agree to enter into other standard contractual clauses approved under Applicable Law to the cross-border transfers of Personal Data for purposes of providing the Services.

7.4 The parties further agree that if any of the EU Standard Contractual Clauses or the UK Addendum are updated, replaced, or are no longer available for any reason, the parties will cooperate in good faith to implement updated or replacement Standard Contractual Clauses, as appropriate, or identify an alternative mechanism(s) to authorize the contemplated cross-border transfers.

7.5 Sub-Processor and its Affiliates have executed an Intercompany Agreement, a copy of which is available on the Trust Center (at https://www.mimecast.com/company/mimecast-trust-center/gdpr-center/mimecasts-intercompany-agreement/), to provide for the adequate safeguards for the transfer of Personal Data among its Affiliates as such transfer may be necessary in order for Sub-Processor to fulfil its obligations under the Agreement.

7. Changes in Applicable Law. The parties agree to negotiate in good faith modifications to this DPA if changes are required for Sub-Processor to continue to Process the Personal Data in compliance with Applicable Law including but not limited to: (i) the GDPR; (ii) the UK GDPR; (iii) the CCPA; (iv) other Applicable Law (v) the Standard Contractual Clauses; or (vi) if changes to the membership status of a country in the European Union or the European Economic Area require such modification.

8. Sub-contracting

Use of Third-Party Subcontractors.

8.1 Data Processor hereby consents, and shall procure Data Controller's consent, to the use of the Third-Party Subcontractors to perform the Services. Subcontracting for the purpose of this DPA is to be understood as meaning services which relate directly to the provision of the principal obligation related to the processing of Personal Data pursuant to the Customer Agreement. This does not include ancillary services, such as telecommunication services, postal/transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. Sub-Processor shall implement written agreements with all Third-Party Subcontractors that contain technical and organisational obligations on the Third-Party Subcontractors to safeguard the security and integrity of Personal that are no less protective than the obligations on Sub-Processor under this DPA in respect of the specific Services provided by the Third-Party Subcontractor.

8.2 **Change to Third Party Subcontractors.** If Sub-Processor appoints a new Third-Party Subcontractor or intends to make any changes concerning the addition or replacement of the Third-Party Subcontractor, it shall provide the Data Processor with at least 20 days' written notice. For the purposes of this Section 8.2, notice may be provided electronically, including but not limited to posting on the Sub-Processor's administrative console of the Services, a notice on the Trust Center and/or in a e-newsletter sent to Data Processor and/or Data Controller (if either has subscribed to such e-newsletter via Sub-Processor's online preference center). Data Processor must inform Data Controller of any such appointment notified by Sub-Processor hereunder in a timely manner.

9.3 If Data Controller receiving the Services under a Customer Agreement objects to the appointment or replacement of Third-Party Subcontractor in writing based on legitimate data protection grounds within ten (10) days after Sub-Processor's advanced written notice of a new Third-Party Subcontractor, Data Processor must notify Sub-Processor immediately and Sub-Processor may, at its option, suggest a commercially reasonable

change to the Data Controller's use of the Services so that the relevant Third-Party Subcontractor is not used in terms of the Service(s) procured.

9.4 If Sub-Processor is unable to enact such change within a reasonable period of time; Data Processor may upon not less than twenty (20) days' written notice from the date of notification by Sub-Processor, terminate the applicable Services Order with respect to those Services which cannot be provided without the use of the relevant Third-Party Subcontractor. If Data Processor does not provide a written objection within such ten (10) day period, Data Processor is deemed to have consented to such appointment or change in Third-Party Subcontractor. Termination of any ordering document under this Clause 8 shall entitle Data Controller to a pro-rata refund and Data Processor shall ensure that any such refunds are passed to the Data Controller accordingly. Any termination in accordance with this subsection 8.4 shall be without further obligation on Sub-Processor to continue to provide the Services to the relevant Data Controller. For the avoidance of doubt, termination under this Section 8.4 shall not entitle Data Controller or Data Processor to any refund of fees paid for the period up to the effective date of termination.

10. Confidentiality. The Confidentiality provisions in the Agreement shall apply equally to this DPA and where applicable the Standard Contractual Clauses pursuant to Clause 6 herein.

11. Termination; Consequences of termination. Termination of this DPA shall be governed by the Agreement. Upon termination of a Customer Agreement, Sub-Processor shall, at Data Processor's written request:

(a) delete all Personal Data Processed on behalf of the Data Controller, unless applicable laws, regulations, subpoenas, or court orders require it to be retained; or

(b) assist Data Processor with return to the Data Controller of the Personal Data which it is Processing or has Processed upon behalf of that Data Controller. The Data Processor acknowledges and agrees, and shall procure that the Data Controller acknowledges and agrees, that the nature of the Services mean that the Data Processor and/or Controller may extract a copy of the Personal Data at any time during the term of the Agreement and providing the tools to allow Data Processor and/or Controller to do so shall be sufficient to show Sub-Processor has complied with this Clause. If Data Controller or Data Processor requires the Sub-Processor to extract the Personal Data on its behalf, the Data Processor or Data Controller must provide written Instructions to that effect and engage the Sub-Processor in a professional services project, which shall be subject to additional fees. In the event the request is from the Data Processor, Data Processor must provide Sub-Processor with written Instructions from Customer requesting such extraction; and

(c) in either case, cease Processing Personal Data on behalf of the Data Controller.

12. Threat Data, Machine-Learning Data and Aggregated Usage Data.

12.1 The parties acknowledge and agree that Sub-Processor has no ownership rights to Customer Data. In accordance with the Customer Agreement and the Data Processing Terms, Data Controller hereby grants to Sub-Processor all necessary rights and licenses to Process Customer Data, including Customer Data within Machine-Learning Data (as defined below), and Threat Data (as defined below) for the purposes of: (i) providing the Services; (ii) improving threat detection, analysis, awareness, and prevention; and/or (iii) improving and developing the Services.

12.2 **Threat Data**. As part of the Services, Sub-Processor Processes certain data reasonably identified to be malicious, including, without limitation, data which may perpetuate data breaches, malware infections, cyberattacks or other threat activity (collectively, "**Threat Data**"). Sub-Processor Processes Threat Data primarily through automated processes and may share limited Threat Data with Third Parties within the cybersecurity ecosystem for the purpose of improving threat detection, analysis, awareness and prevention. In certain instances, Threat Data may include Personal Data.

12.3 **Machine-Learning Data**. Primarily through automated pattern recognition designed to develop and improve the efficacy and accuracy of Sub-Processor's machine learning algorithms within the Services, Sub-Processor Processes Machine-Learning Data that may include Customer Data and other data that describes and/or gives information about Customer Data. "**Machine-Learning Data"** includes, but is not limited to metadata, files, URLs, derived features and other data. These machine-learning algorithms are hosted by Mimecast and/or Third-Party Subcontractors. The output of these machine learning algorithms is owned by Mimecast, does not contain Customer Data or Personal Data, and is anonymized and irreversible. Sub-Processor does not share Machine-Learning Data with Third Parties.

12.4 **Aggregated Usage Data**. Sub-Processor Processes certain aggregated data derived from the Services, including usage data, such as utilization statistics, reports, logs and information regarding spam, viruses and/or other malware ("**Aggregated Usage Data**"). Sub-Processor owns all Aggregated Usage Data.

13. Limitations.

(a) The parties agree that Affiliates of Sub-Processor and/or Third-Party Subcontractors Processing Personal Data hereunder shall be bound by data protection obligations no less protective than the data protection obligations as specified in this DPA and any Standard Contractual Clauses entered into pursuant to Clause 6 herein. It is further agreed that the aggregate liability of the Affiliates, Third-Party Subcontractors and Sub-Processor under this DPA and any Standard Contractual Clauses entered into pursuant to this DPA, shall be no greater than the aggregate liability of Sub-Processor under the Agreement, to the extent permissible by Applicable Law. To the extent such act or omission of the Sub-Processor affects Services under multiple Orders, the aggregate cap of $500,000 USD shall apply. Neither Data Processor nor any of its Authorized Affiliates shall be entitled to recover more than once in respect of the same claim under this DPA.

(b) In the event of a breach of this DPA which also gives rise to a claim under a DPA directly between Sub-Processor and Data Controller (if any), Sub-Processor shall be liable only under that DPA and Data Processor shall have no right to recover for such loss notwithstanding any provision to the contrary herein.

(c) **Satisfaction of claim.** In the event of any claim by the Data Processor against any Third-Party Sub-processor or any Affiliate of the Sub-Processor under this DPA or Standard Contractual Clauses, the Data Processor shall accept payment from the Sub-Processor entity with whom the Data Processor entered into the Agreement, on behalf of the relevant Affiliate or Third-Party Sub-processor, in satisfaction of such claim.

15. Law and Jurisdiction. Except as it pertains to Standard Contractual Clauses entered into pursuant to Section 6 herein, this DPA shall be governed by and construed in all respects in accordance with the governing law, forum and jurisdiction provisions in the Agreement, provided that, in the event of a conflict between the Agreement and this DPA with regards to the Processing of Personal Data, this DPA shall control.

Schedule 1
Processing Details

The details of the Processing relevant to the Services provided by the Sub-Processor can be found at:
https://www.mimecast.com/company/mimecast-trust-center/gdpr-center/processing-details/

Schedule 2

Technical and Organisation Security Measures

Sub-Processor shall implement the technical and organisational security measures specified on the Trust Center https://www.mimecast.com/company/mimecast-trust-center/gdpr-center/technical-organizational-measures/ as a minimum security standard. Data Processor acknowledges and agrees that the nature of the Services mean that the technical and organisational measures may be updated by Sub-Processor from time-to-time but such updates shall not result in a lesser standard of security to that in place upon signature of this DPA.

Schedule 3
Third-Party Sub-processors

Sub-Processor shall maintain a list of Third-Party Sub-Processors at:
https://www.mimecast.com/company/mimecast-trust-center/gdpr-center/sub-processors/