Data Processing Addendum

This Data Processing Addendum ("**DPA**") is entered into by the customer ("**Customer**") and the applicable Mimecast entity providing the Services ("**Mimecast**"), with each of the Customer or Mimecast referred to as a party and collectively as the parties. This DPA shall form part of and is incorporated into the services agreement entered into between the parties hereto (jointly referred to as the "**Agreement**") and is effective from the date of last signature below (the "**Effective Date**").

By signing below, Customer enters into this DPA on behalf of itself and, to the extent required under Applicable Law (defined hereinafter), in the name and on behalf of its Authorized Affiliates, if and to the extent Mimecast Processes Personal Data for such Authorized Affiliates and they qualify as, for the purposes of the GDPR, the controller and, for the purposes of the CCPA, the business. For the purposes of the GDPR, Mimecast is the processor and, for the purposes of the CCPA, the service provider. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In the course of providing the Services to Customer pursuant to the Agreement, Mimecast may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2 and 3.

2. This DPA has been pre-signed on behalf of Mimecast. To complete this DPA, Customer must complete the information in the signature box and sign on Page 10.

3. Send the completed and signed DPA to Mimecast by email, indicating the Customer's Account Number (as set out on the applicable Mimecast Order Form or invoice), to the Customer's applicable Customer Success Manager. Upon confirmed receipt of the validly completed DPA by Mimecast, this DPA will become legally binding.

HOW THIS DPA APPLIES:

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Mimecast entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA is neither a party to a Services Order nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

For the avoidance of doubt, if a Services Order or an Agreement does not exist between Mimecast and a party signing this DPA on behalf of Customer, this DPA is not valid and of no force and effect.

The Mimecast entity that has entered into the applicable Services Order or Agreement and is providing the Services under such Services Order or Agreement will be deemed to be the Mimecast party entering into this DPA. All signatures provided on behalf of other Mimecast entities do not apply.

In the event of a conflict between this DPA and any other terms or conditions regarding the Processing of Personal Data contained in the Agreement (including any existing data processing addendum to the Agreement), this DPA shall control.

The terms herein apply to the Processing of Personal Data for the purposes set forth in the Agreement and this DPA.

1. Definitions. All capitalized terms used in this DPA and not otherwise defined shall have the same meaning attributed to them in the Agreement. The following definitions have the meanings set out below:

"**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 Agreement between Customer and Mimecast, but has not signed its own Agreement with Mimecast 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 United Kingdom ("**UK**") Data Protection Act 2018 and the UK General 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"**); (v) the South Africa Protection of Personal Information Act ("**POPIA**"); (vi) 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 Data**" means data provided by Customer for processing via the Services including, without limitation, the contents of the files, emails or messages sent by or to a Permitted User. Customer Data does not include Threat Data (as defined under Section 9.2);

"**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 under the relevant Applicable Law;

"**Data Subject Request**" refers to a request from (i) a Data Subject in accordance with the 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 2: Transfer Controller 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 this Agreement (the "**Business Purpose**", as defined under the CCPA), and (ii) those as may be additionally communicated in writing by Customer to Mimecast from time-to-time;

"**Personal Data**" means (i) "personal data" as defined under the 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 Mimecast in connection with the performance of the Services;

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

"**Regulator**" means the data protection supervisory authority which has jurisdiction over 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 Mimecast as identified in the Agreement and described further in an ordering document referencing the Agreement;

"Standard Contractual Clauses" means 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;

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

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

"**Third-Party Subcontractor**" means the third-party subcontractors listed in Schedule 2, as such list may be updated from time to time pursuant to Clause 8;

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

"UK Addendum" shall mean the 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 Mimecast shall only Process Personal Data on behalf of 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 Mimecast (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 Mimecast is subject. In such a case, Mimecast shall inform Customer 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,

2.2.1 Mimecast shall act as a "service provider" and certifies that it shall Process Customer Personal Data on behalf of Customer in accordance with and for the Business Purpose. Notwithstanding the foregoing, Mimecast 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 Mimecast.

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

2.3.1 Mimecast represents and warrants that:

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

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

(iii) Mimecast understands the restrictions placed on it under Section 2.2.

2.3.2 Customer represents and warrants that:

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

(ii) 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 Mimecast and enable the Processing set out in this DPA and as contemplated by the Agreement;

(iii) it has assessed the requirements under Applicable Law as they apply to Customer with regard to Personal Data and finds that the security measures referenced in Schedule 3 are adequate to meet those requirements; and

(iv) it will ensure compliance with and shall not in any way alter or diminish such security measures referenced in Schedule 3 to the extent applicable to Customer through its use of the Services.

2.4 Customer understands that Personal Data within Customer Data transferred to Mimecast is determined and controlled by Customer in its sole discretion. As such, Mimecast has no control over the volume, categories and sensitivity of Personal Data Processed through its Services by Customer or users. Mimecast shall implement and maintain the technical and organisational security measures specified in Schedule 3 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. Mimecast shall notify Customer without undue delay (and in no event more than 48 hours, with periodic updates to follow as may be necessary) 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**"). 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 Customer to Data Subjects or relevant Regulators, the parties agree 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 Mimecast, Mimecast shall provide reasonable assistance in response to inquiries from Customer or a competent Regulator relating to Mimecast's Processing of Customer's Personal Data.

4.2 Mimecast shall, upon written request from Customer, provide Customer with information reasonably necessary to demonstrate compliance with its 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 Mimecast's ISO27001 or similarly held industry certification.

4.3 In the event the information provided in accordance with Clause 4.2 above is insufficient to reasonably demonstrate compliance, Mimecast shall permit Customer to inspect or audit the technical and organisational measures of Mimecast for the purposes of monitoring compliance with Mimecast's obligations under this DPA. Any such audit or inspection shall be:

(i) at Customer's expense;

(ii) limited in scope to matters specific to Customer;

(iii) agreed in advance between the parties in writing, including scope, duration, start date and Mimecast's then-current rates for professional services;

(iv) conducted in a way that does not interfere with Mimecast's day-to-day business;

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

(vi) 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; and

(vii) subject to the confidentiality obligations in the Agreement or, where a third-party auditor conducts the audit, such third-party auditor must be a professional bound by a duty of confidentiality or subject to a suitable non-disclosure agreement.

4.4 Any audit conducted under this Section shall not be conducted by a party who is a competitor of Mimecast or provides services to a competitor of Mimecast.

4.5 Customer will provide Mimecast with copies of any audit reports generated in connection with any audit under this Section, unless prohibited by Applicable Law. Customer 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.

4.6 For the avoidance of doubt, the provisions of this Clause 4 shall also apply to the audit provisions of any Standard Contractual Clauses entered into in accordance with Clause 6 of this DPA.

5. Compliance, Co-operation, and Response.

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

5.2 If Mimecast receives a Data Subject Request, and it is clear from the nature of the request without the need for any independent investigation that Customer is the applicable controller of Data Subject's Personal Data, Mimecast will refer the Data Subject to Customer, unless otherwise required by Applicable Law. In the event Mimecast is legally required to respond to the Data Subject, Customer will fully co-operate with Mimecast as appropriate. Customer agrees that provision of technical tools to enable Customer to take the necessary action to comply with such request/s shall be sufficient to discharge Mimecast's obligations of assistance hereunder.

5.3 Customer will reimburse all reasonable costs incurred by Mimecast as a result of reasonable assistance provided by Mimecast under this Clause 5.

6. Cross-Border Transfers.

6.1 Customer acknowledges and agrees that Mimecast may, in the course of providing the Services, Process (or permit any Affiliate or Third-Party Subcontractor to Process) Customer's 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, Mimecast shall, comply with (or procure that any Affiliate or Third-Party Subcontractor comply with) the data importer obligations in the applicable Standard Contractual Clauses.

6.2 If, in fulfilling its obligations under the Agreement or pursuant to other lawful instructions from Customer, Personal Data is to be transferred from the European Economic Area, Switzerland and/or the UK (as applicable) by Customer to Mimecast in 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) Customer is the Data Exporter and Mimecast 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 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”.

(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 and/or Switzerland.

6.3 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.

6.4 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.

6.5 Mimecast 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 Mimecast 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 Mimecast to continue to Process Personal Data in compliance with Applicable Law, including but not limited to (i) the GDPR; (ii) the CCPA; (iii) any Standard Contractual Clauses; or (iv) if changes

to the membership status of a country in the European Union or the European Economic Area require such modification.

8. Sub-Contracting.

8.1. Use of Third-Party Subcontractors. Customer hereby consents to the use of the Third-Party Subcontractors to perform 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 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. Mimecast 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 Data that are no less protective than the obligations on Mimecast under this DPA in respect of the specific Services provided by the Third-Party Subcontractors.

8.2. Change to Third Party Subcontractors. If Mimecast appoints a new Third-Party Subcontractor or intends to make any changes concerning the addition or replacement of the Third-Party Subcontractors, it shall provide Customer with at least 20 days written notice. For the purposes of this Clause 8.2, notice may be provided electronically, including but not limited to posting on the Mimecast administrative console of the Services, a notice on the Trust Center and/or in a e-newsletter sent to Customer (if Customer has subscribed to such e-newsletter via Mimecast's online preference center). If Customer objects to the appointment or replacement of Third-Party Subcontractor in writing based on legitimate data protection grounds within ten (10) days after Mimecast's advanced written notice of a new Third-Party Subcontractor, Mimecast, at its option may suggest a commercially reasonable change to Customer's use of the Services so that the relevant Third-Party Subcontractor is not used in terms of the Service/s procured. If Mimecast is unable to enact such change within a reasonable period of time, Customer may, upon not less than twenty (20) days' written notice from the date of notification by Mimecast, terminate the applicable Services Order with respect to those Services which cannot be provided without the use of the relevant Third-Party Subcontractor. If Customer does not provide a written objection within such ten (10) day period, Customer 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 Customer to receive a pro-rata refund of any unused portion of the fees paid in advance. For the avoidance of doubt, termination under this Clause 8 shall not entitle Customer to any refund of fees paid for the period up to the effective date of termination.

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

9.1 The parties acknowledge and agree that Mimecast has no ownership rights to Customer Data. In accordance with the Agreement and this DPA, Customer hereby grants to Mimecast a worldwide, irrevocable license to Process Customer Data, including certain Customer Data within Machine-Learning Data (as defined below), as well as Personal Data within 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.

9.2 Threat Data. As part of the Services, Mimecast 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**"). Mimecast 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.

9.3 Machine-Learning Data. Through automated pattern recognition designed to develop and improve the efficacy and accuracy of our machine learning algorithms within the Services, Mimecast processes certain Customer Data and other data that describes and/or gives information about Customer Data, including but not limited to metadata, files, URLs, derived features and other data ("**Machine-Learning Data**"). Mimecast does not share Machine-Learning Data with Third Parties. Machine-Learning Data does not include full message content of Customer Data.

9.4 **Aggregated Usage Data.** Mimecast 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**"). Mimecast owns all Aggregated Usage Data.

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 therein.

11. **Liability.**

11.1. **Limitations.** The parties agree that Affiliates of Mimecast 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 Mimecast under this DPA and any Standard Contractual Clauses entered into pursuant to this DPA, shall be no greater than the aggregate liability of Mimecast under the Agreement, to the extent permissible by Applicable Law. If Customer has contracted the Services through a managed services provider ("**MSP**"), Customer shall have no direct right of action against Mimecast with regards to the general provision of the Services and/or any instruction received from or access granted by the MSP, and all such claims should be brought against Customer's MSP. For the avoidance of doubt, the limitations of liability in the Agreement shall apply to this DPA and any Standard Contractual Clauses entered into in accordance with Clause 6 herein. Neither Customer nor any of its Authorized Affiliates shall be entitled to recover more than once in respect of the same claim under this DPA.

11.2. **Satisfaction of claim.** In the event of any claim by Customer against any Affiliate of Mimecast under the Standard Contractual Clauses, Customer shall accept payment from the Mimecast entity with whom Customer entered into the Agreement, on behalf of the relevant Affiliate of Mimecast in satisfaction of such claim.

12. **Termination.** Termination of this DPA shall be governed by the Agreement.

13. **Consequences of Termination.** Upon termination of this DPA in accordance with Clause 12, Mimecast shall, at Customer's request:

13.1 delete all Personal Data Processed on behalf of Customer, unless applicable laws, regulations, subpoenas or court orders require it to be retained; or

13.2 assist Customer with the return to Customer of Personal Data and any copies thereof which it is Processing or has Processed upon behalf of Customer. Customer acknowledges and agrees that the nature of the Services mean that Customer may extract a copy of Personal Data at any time during the term of the Agreement and providing the tools to allow Customer to do so shall be sufficient to show Mimecast has complied with this Clause 13.2. If Customer requires Mimecast to extract Personal Data on its behalf, Customer must engage Mimecast in a professional services project, which shall be subject to additional fees; and

13.3 in either case, cease Processing Personal Data on behalf of Customer, except as may otherwise be required in accordance with subparagraph (i) above.

14. **Law and Jurisdiction.** Except as it pertains to cross-border transfers as set forth in Clause 6, this DPA shall be governed by and construed in all respects in accordance with the governing law 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.

15. **Parties to this DPA.** The Section "HOW THIS DPA APPLIES" specifies which Mimecast entity is party to this DPA. Notwithstanding the signatures below of any other Mimecast entity, such other Mimecast entities are not a party to this DPA or the Standard Contractual Clauses.

This DPA may be executed in any number of counterparts, each of which is an original and all of which evidence the same agreement between the parties. For the avoidance of doubt, only the signature of the Mimecast entity that is providing the Services shall apply. All signatures on behalf of the other Mimecast entities shall have no force or effect.

Customer

By:_____

Name:_____

Title:_____

Date:_____

Company Name: _____

Mimecast Services Limited

DocuSigned by: Michael Paisley 0343CC7D5EC6483...

By:_____

Name: Michael Paisley
Title: Data Protection Officer

Date: March 1, 2023 | 09:56 PST

Mimecast South Africa (Pty) Ltd.

DocuSigned by: Michael Paisley 0343CC7D5EC6483...

By:_____

Name: Michael Paisley
Title: Data Protection Officer

Date: March 1, 2023 | 09:56 PST

Mimecast Germany GmbH

DocuSigned by: Michael Paisley 0343CC7D5EC6483...

By:_____

Name: Michael Paisley
Title: Data Protection Officer

Date: March 1, 2023 | 09:56 PST

Mimecast North America Inc.

DocuSigned by: Michael Paisley 0343CC7D5EC6483...

By:_____

Name: Michael Paisley
Title: Data Protection Officer

Date: March 1, 2023 | 09:56 PST

Mimecast Australia Pty. Ltd.

DocuSigned by: Michael Paisley 0343CC7D5EC6483...

By:_____

Name: Michael Paisley
Title: Data Protection Officer

Date: March 1, 2023 | 09:56 PST

Mimecast Israel Ltd.

DocuSigned by: Michael Paisley 0343CC7D5EC6483...

By:_____

Name: Michael Paisley
Title: Data Protection Officer

Date: March 1, 2023 | 09:56 PST

Mimecast Canada Limited

DocuSigned by: Michael Paisley 0343CC7D5EC6483...

By:_____

Name: Michael Paisley
Title: Data Protection Officer

Date: March 1, 2023 | 09:56 PST

Mimecast Singapore Pte Ltd.

DocuSigned by: Michael Paisley 0343CC7D5EC6483...

By:_____

Name: Michael Paisley
Title: Data Protection Officer

Date: March 1, 2023 | 09:56 PST

Schedule 1 to the DPA

Processing Details

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

Schedule 2 to the DPA

Third-party subcontractors

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

Schedule 3 to the DPA

Technical and Organisation Security Measures

Mimecast 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. Customer acknowledges and agrees that the nature of the Services mean that the technical and organisational measures may be updated by Mimecast 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.