DATA PROCESSING FLOW-DOWN TERMS ("DATA PROCESSING TERMS") SPECIFIC TO THE MIMECAST SERVICES

These Data Processing Terms shall supersede and replace all prior agreements and undertakings, oral or written, between the Customer and Partner regarding the Processing of Customer Data via the Services.

1. **Definitions.** All capitalized terms not defined herein shall have the meaning set forth in the Customer Agreement (defined below). In the event of any conflicts between the Customer Agreement and these Data Processing Terms, the Data Processing Terms shall apply.

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

"**Applicable Data Protection 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 Agreement; (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 (the "**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 No. 119 1988 (as amended), (vii) Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"); and (viii) any relevant law, statute, regulation, legislative enactment, order, or other binding instrument, that implements, supplements, or amends the foregoing;"**Customer**" means party receiving the Services under a Customer Agreement with the Partner ;

"**Customer Agreement**" means the agreement between Customer and Partner regarding the provision of certain Services by Sub-Processor;

"**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 and emails sent by or to Permitted Users of the Services;

"**Data Controller**" means the Customer receiving the Services under a Customer Agreement with Partner;

"**Data Processor**" means the Partner providing the Services to the Customer;

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

"**Data Subject Access Request**" refers to a request from a Data Subject in accordance with Applicable Data Protection 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;

"**Instructions**" are embodied in the Customer Agreement for the provision of the Services (to the extent they are communicated to the Sub-Processor), these Data Processing Terms, the applicable Service Order and as

may be additionally agreed by the Sub-Processor relating to the provision of Services to the Data Controller (the "**Business Purpose**" as defined under the CCPA);

"**Partner**" means the managed services provider reselling the Services to Customer;

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

"**Permitted User**" means individuals employed by or otherwise under Customer's control authorized to use the Services;

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

"**Regulator**" means a data protection supervisory authority that has jurisdiction over the Processing of Data Controller's 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;

"**Order**" means the transactional document that describes the Services to be provided to Customer;

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

"**Standard Contractual Clauses**" means the EU or UK government approved contract mechanism for the cross-border transfer of Personal Data to Third Countries;

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

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

"**Third-Party Sub-Processor(s)**" means the Third-Party Sub-Processors engaged by the Sub-Processor and identified at: https://www.mimecast.com/company/mimecast-trust-center/gdpr-center/sub-processors/;

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

"**Trust Center**" means the website maintained by Sub-Processor which includes relevant content referenced in these Data Processing Terms and otherwise related to Applicable Data Protection 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 Addendum to the EU Commission Standard Contractual Clauses issued by the UK's Information Commissioner's Office in Schedule 4.

2. Data Processing.

2.1 These Data Processing Terms apply to the Processing of Personal Data via the applicable Services provided by Sub-Processor. Nothing herein is intended to nor shall it create a direct contractual relationship between Sub-Processor and Data Controller. Data Processor is responsible to Data Controller for the provision of the Services in accordance with the terms set out herein.

2.2 Data Processor represents and warrants, and where applicable, shall procure that Sub-Processor represents and warrants:

(a) Sub-Processor shall only Process Personal Data 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 Data Controller 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 (defined hereinafter) 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;

(b) Data Processor shall comply with its obligations under Applicable Data Protection Law;

(c) Data Processor will ensure that Sub-Processor's personnel who are authorised to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

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

(e) if the CCPA is applicable, Sub-Processor shall be considered a Service Provider (as defined under the CCPA) to the Data Processor and shall Process Customer Personal Data in accordance with and for a Business Purpose on behalf of the Data Controller, which shall be the specific purpose of performing the Services as set forth in the MSP Agreement between Data Processor and Sub-Processor. Further, the Data Processor will ensure that the Sub-Processor is contractually prohibited from Selling Data Controller's Personal Information and otherwise is required to 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 Data Protection Law, as reasonably determined by Sub-Processor;

2.3 Data Controller represents and warrants that:

(a) Data Controller's use of the Services and the Instructions provided do not contravene Applicable Data Protection Law;

(b) it has complied and continues to comply with Applicable Data Protection Law, in particular that it has obtained any necessary consents and/or given any necessary notices, and otherwise has the right to disclose the Personal Data to Data Processor and Sub-Processor and enable the Processing set out in these Data Processing Terms and as contemplated by the provision of the Services;

(c) it has assessed the requirements of the Applicable Data Protection Law as they apply to the Data Controller with regards to Personal Data and finds that the security measures specified on Schedule 2 are adequate to meet those requirements;

(d) it will ensure compliance with and shall not in any way alter or diminish such security measures referenced in Schedule 2;

(e) where Processing hereunder includes, or may include, special categories of Personal Data, it has complied and continues to comply with requirements of Applicable Data Protection Law to notify Data Subjects of the Processing and, where relevant, obtain any consents or otherwise have the right to enable the Processing of the special categories of Personal Data.

3. Technical and organisational security requirements. Data Controller understands that Personal Data transferred to Data Processor and Sub-Processor is determined and controlled by Data Controller in its sole discretion. As such, Sub-Processor has no control over the volume, categories and sensitivity of Personal Data Processed through the Services by Data Controller or its Permitted Users. Data Processor shall ensure that Sub-Processor implements and maintains the technical and organisational security measures specified on the Schedule 2 before Processing 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 Customer Agreement.

4. Notification of Data 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 Data Controller's Personal Data ("**Security Breach"**), Data Processor shall notify Data Controller without undue delay. 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 to coordinate in good faith with Sub-Processor on developing the content of any public statements or required notices.

5. Audit and Inspection Rights.

5.1 Upon written request from Data Controller, Data Processor shall obtain and provide to Data Controller such information from Sub-Processor reasonably necessary to demonstrate compliance with Sub-Processor's obligations set forth in these Data Processing Terms. 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).

5.2 In the event the information provided in accordance with Section 5.1 above is insufficient to reasonably demonstrate compliance, any further audit and inspection rights will be in accordance with Data Processor's MSP Agreement with Sub-Processor. Further, to the extent the information provided in accordance with Section 5.1 is insufficient to reasonably demonstrate compliance to a Regulator, Data Processor shall procure that the Regulator may inspect or audit the technical and organisational measures of the Sub-Processor for the purposes of monitoring compliance with Sub-Processor's obligations under the MSP Agreement provided that any such audit or inspection shall be:

(a) at Data Controller's expense;

(b) limited to one audit per calendar year;

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

(d) agreed in advance with the Sub-Processor 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 as determined by the Sub-Processor;

(f) during local business hours as specified by Sub-Processor and, upon not less than twenty (20) business days advance written notice unless Parties agree in writing that an identifiable, material non-conformance has arisen;

(g) subject to confidentiality obligations in the Customer Agreement and/or, where a third-party auditor conducts the audit, such third-party auditor shall be bound by a professional 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.

5.3 Data Controller will provide Sub-Processor with copies of any audit reports generated in connection with any audit under this Section, unless prohibited by Applicable Data Protection Law. 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 these Data Processing Terms.

5.4 For the avoidance of doubt, the provisions of this Section 5 shall also apply to the audit provisions of any Standard Contractual Clauses entered into regarding the Processing of Personal Data related to the services provided by Sub-Processor.

6. Compliance, Co-operation and Response from Data Processor.

6.1 Data Processor will (and, where applicable shall procure that Sub-Processor will) provide reasonable assistance to Data Controller in complying with any Data Subject Access Requests or requests received by Data Controller from Regulators that occur in accordance with Applicable Data Protection Law.

6.2 If Data Processor receives a Data Subject Access Request (either directly or via Sub-Processor), Data Processor will refer the Data Subject to Data Controller, unless otherwise required by Applicable Data Protection Law. In the event Data Processor (or Sub-Processor) is legally required to respond to the Data Subject, Data Controller will fully co-operate with Data Processor or Sub-Processor, as appropriate. Data Controller agrees that provision of technical tools to enable Data Controller to take the necessary action to comply with such request/s shall be sufficient to discharge Sub-Processor's obligations of assistance hereunder.

7. Cross-Border Transfers.

7.1. If, in fulfilling its obligations under the Customer Agreement or pursuant to other lawful Instructions from the Data Controller regarding the Personal Data Processed via the applicable Services, Personal Data is to be transferred from the European Economic Area and/or Switzerland to any country that has not been recognized by the European Commission as providing an adequate level of protection for Personal Data, the Parties agree to enter into and abide by the EU Standard Contractual Clauses which are incorporated into these Data Processing Terms as follows:

(a) Data Controller is the Data Exporter and Data Processor is the Data Importer;

(b) In Clause 7, the "Docking Clause (Optional)", shall be deemed incorporated;

(c) In Clause 9, the Parties choose Option 2, "General Written Authorisation", with a time period of 20 days;

(d) the optional wording in Clause 11 shall be deemed not incorporated;

(e) In Clause 17, the Data Exporter and Data Importer agree that the EU Standard Contractual Clauses shall be governed by the laws of Germany, as applicable, and choose Option 1 to this effect;

(f) In Clause 18, the Data Exporter and Data Importer agree that any disputes shall be resolved by the courts of Munich, Germany, as applicable;

(g) Completed Schedules 1, 2 and 3 attached hereto constitute Annexes I, II and III of the EU Standard Contractual Clauses;

(h) Notwithstanding the fact that the EU Standard Contractual Clauses are incorporated herein by reference without actually being signed by the Parties, the Parties agree that the execution of these Data Processing Terms is deemed to constitute its execution of the EU 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;

(i) The parties further agree that the EU 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" by the relevant Regulator; and

(j) The provisions in these Data Processing Terms 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 to a Third Country.

7.2 If, in fulfilling its obligations under this DPA or pursuant to other lawful instructions from Data Controller regarding the Personal Data Processed via the applicable Services, Personal Data must be transferred from the UK to any country that has not been recognized by the applicable authorities in the UK as providing an adequate level of protection for Personal Data, the parties agree that the UK Addendum set forth in Schedule 4 shall apply to such cross-border transfers.

7.3 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.

7.4 Data Controller acknowledges and agrees that Sub-Processor may, in the course of providing the Services, Process (or permit any Affiliate or Third-Party Sub-Processor to Process) the Data Controller's Personal Data in one or more Third Countries, provided that such Processing takes place in accordance with the requirements of Applicable Data Protection Law. In such case, the Data Processor shall ensure that Sub-Processor shall comply with (or procure that any Affiliate or Third-Party Sub-Processor comply with) the data importer obligations in the Standard Contractual Clauses (Module 3). The Data Controller hereby grants the Sub-Processor a mandate to enter into the Standard Contractual Clauses with Third-Party Sub-Processors it appoints on behalf of Data Controller.

7.5 Data Controller acknowledges that 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 MSP Agreement.

8. Changes in Applicable Data Protection Law. The Parties agree to negotiate in good faith modifications to these Data Processing Terms if changes are required for Sub-Processor to continue to Process the Data Controller's Personal Data in compliance with Applicable Data Protection Law including but not limited to: (i) the GDPR; (ii) the UK GDPR; (iii) the CCPA; (iv) other Applicable Data Protection 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.

9. Third-Party Sub-Processors. Data Controller hereby consents to Sub-Processor's use of Affiliates and Third-Party Sub-Processors to perform the Services. Sub-Processor's list of current Third-Party Sub-Processors is set forth on Schedule 3. Subcontracting for the purpose of these Data Processing Terms is to be understood as meaning services which relate directly 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. Data Processor shall ensure that Sub-Processor has a written agreement in place with all Third-Party Sub-Processors that contains obligations on the Third-Party Sub-Processor that are no less onerous than the obligations on Sub-Processor hereunder in respect of the specific Services provided by the Third-Party Sub-Processor.

9.1 If Sub-Processor appoints a new Third-Party Sub-Processor or intends to make any changes concerning the addition or replacement of the Third-Party Sub-Processors, Sub-Processor will notify Data Processor, and Data Processor shall provide Data Controller with reasonable advance written notice. For the purposes of this Section, notice may be provided electronically, including but not limited to posting on the Sub-Processor's administrative console for the Services or via a notice on the Trust Center and/or in a newsletter sent to its customers (if Data Controller has subscribed to such e-newsletter via Sub-Processor's online preference center).

9.2 If Data Controller objects to the appointment or replacement of Third-Party Sub-Processor in writing based on legitimate data protection grounds within ten (10) days after Sub-Processor's advanced written notice of a new Third-Party Sub-Processor, Sub-Processor may, at its option, suggest a commercially reasonable change to Data Controller's use of the Services so that the relevant Third-Party Sub-Processor is not used in terms of the Service(s) procured.

9.3 If Sub-Processor is unable to enact such change within a reasonable period of time, Data Controller may, upon no less than twenty (20) days' written notice from the date of notification by Sub-Processor, terminate those Services which cannot be provided without the use of the relevant Third-Party Sub-Processor. Termination of any Order under this Section shall entitle the Data Controller to receive a pro-rata refund of any unused portion of the fees paid in advance. For the avoidance of doubt, termination under this Section 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. Termination; Consequences of termination. Termination of these Data Processing Terms shall be governed by the Customer Agreement. Upon termination of the Customer Agreement, Data Processor shall upon Data Controller's written request, secure that Sub-Processor shall:

10.1 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

10.2 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 Controller acknowledges and agrees that the nature of the Services mean that the Data Controller may extract a copy of the Personal Data at any time during the term of the Customer Agreement and providing the tools to allow Data Controller to do so shall be sufficient to show Sub-Processor has complied with this Section. If Data Controller or Data Processor requires the Sub-Processor to extract the Personal Data on its behalf, the Data Controller or Data Processor must provide the Sub-Processor with written instructions to that effect and engage Sub-Processor in a professional services project, which shall be subject to additional fees; and

10.3 in either case, cease Processing Personal Data on behalf of the Data Controller.

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

11.1 **Customer Data**. The parties acknowledge and agree that Sub-Processor has no ownership rights to Customer Data. In accordance with the Customer Agreement and these Data Processing Terms, Data Controller hereby grants to Sub-Processor all necessary rights and licenses to collect and Process Customer Data, including

certain Customer Data within Machine-Learning Data (as defined below), as well as 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.

11.2 **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 and awareness. In certain instances, Threat Data may include Personal Data.

11.3 **Machine-Learning Data**. Primarily through automated processes designed to develop and improve Sub-Processor's machine learning algorithms within 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.

11.4 **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.

12. Limitations. The Parties agree that Affiliates of the Sub-Processor and/or Third-Party Sub-Processors Processing Personal Data hereunder shall be bound by data protection obligations no less protective than the data protection obligations as specified in these Data Processing Terms and any Standard Contractual Clauses entered into pursuant to these Data Processing Terms. It is further agreed that the aggregate liability of the Sub-Processor, its Affiliates and Third-Party Sub-Processors under these Data Processing Terms and any Standard Contractual Clauses entered into regarding the Processing of Personal Data related to the Services provided by Sub-Processor will be limited to an amount equal to the greater of: (i) USD $100,000 (or the equivalent in the currency of the applicable hosting jurisdiction at the time the claim arose) or (ii) two times (2X) the fees paid by Data Controller to Data Processor for the applicable Services during the twelve months preceding the event giving rise to the claim. Data Controller shall not be entitled to recover more than once in respect of the same claim.

13. Satisfaction of claim. In the event of any claim by the Data Controller against any Third-Party Sub-Processor or any Affiliate of the Sub-Processor under these Data Processing Terms or Standard Contractual Clauses, the Data Controller shall accept payment from the Data Processor in satisfaction of such claim.

14. Law and Jurisdiction. Except as it pertains to Standard Contractual Clauses entered into pursuant to Section 7 herein, these Data Processing Terms shall be governed by and construed in all respects in accordance with the governing law, forum and jurisdiction provisions in the Customer Agreement, provided that, in the event of a conflict between the Customer Agreement and these Data Processing Terms with regards to the Processing of Personal Data, these Data Processing Terms 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
Sub-Processor's Technical and Organizational Measures

Sub-Processor has implemented 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. 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 the Data Processing Terms.

Schedule 3
Sub-Processor's Third-Party Sub-Processors

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

Schedule 4 to the DPA

UK Addendum to the EU Commission Standard Contractual Clauses

This UK Addendum to the EU Standard Contractual Clauses (the "Addendum") forms part of the EU Standard Contractual Clauses incorporated by reference in Section 7 of the Data Processing Terms.

Date of this Addendum

1. The EU Standard Contractual Clauses are dated the Effective Date of the Data Processing Terms. This Addendum is effective from the same date as the EU Standard Contractual Clauses.

Background

2. The UK Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Annex of the EU Standard Contractual Clauses, those terms shall have the same meaning as in the Annex. In addition, the following terms have the following meanings:

(a)	This Addendum	(b)	This Addendum to the Clauses
(c)	The Annex	(d)	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021
(e)	UK Data Protection Laws	(f)	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
(g)	UK GDPR	(h)	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
(i)	UK	(j)	The United Kingdom of Great Britain and Northern Ireland

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.

5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the EU Standard Contractual Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

8. This Addendum incorporates the EU Standard Contractual Clauses which are deemed to be amended to the extent necessary so they operate:

   a. for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and

   b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 7 above, include (without limitation):

   a. References to the "Clauses" means this Addendum as it incorporates the EU Standard Contractual Clauses

   b. Clause 6 Description of the transfer(s) is replaced with:

      i. "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."

   c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.

   d. References to Regulation (EU) 2018/1725 are removed.

   e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"

   f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;

   g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".

h. Clause 18 is replaced to state:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."

i. The footnotes to the EU Standard Contractual Clauses do not form part of the Addendum.

Amendments to this Addendum

10. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.

11. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 7 above.