DATA PROCESSING ADDENDUM for Global Clients

This Data Processing Addendum ("DPA") is made the _____ day of _____ 202_ between:

(A) **Exclaimer Limited** (company number 04938619) whose registered office is located at 250 Fowler Avenue, Farnborough, Hampshire GU14 7JP UK ("**Exclaimer**", "**we**", "**us**" or "**Processor**"); and
(B) **[name of client]** whose registered office/place of business is at [address] ("**you**", "**your**" or "**Controller**").

WHEREAS:

(A) The parties have entered into a subscription contract for a license to use Exclaimer's solutions within the Controller's business, such license terms being the applicable Exclaimer Licenses Terms published at https://exclaimer.com/legal/end-user-license-agreements/ ("the License Terms");
(B) This DPA is entered into by the parties as an addendum to the License Terms in order to record how Exclaimer will process the Controller's Personal Data (as defined below);

NOW IT IS AGREED AS FOLLOWS:

The parties agree that unless otherwise stated, the terms and conditions in the License Terms shall apply to this DPA. In the event of conflict between the License Terms and this DPA, this DPA shall prevail in relation to the processing of Personal Data.

1. DEFINITIONS

All definitions used in the License Terms shall apply equally here unless otherwise stated. In addition, the following definitions are used in DPA:

1.1. **Data Controller, Data Processor, Data Subject, Personal Data, Data Breach, Processing, Processed** and **Process** and **appropriate technical and organisational measures** shall have the meaning as defined in the Data Protection Legislation or if there is no such definition in the relevant Data Protection Legislation it shall have the meaning given to the phrase which mostly closely resembles the definition of "data controller" in the Data Protection Legislation.

1.2. **Data Protection Legislation** means in each case as applicable to the activities undertaken by the respective parties under or in connection with these Terms: the UK Data Protection Legislation, the General Data Protection Regulations (EU 2016/679) ("GDPR"), the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations, The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, the Australia Privacy Act 1988 and all other equivalent legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications) as each may be amended from time to time; and the guidance and codes of practice issued by the relevant data protection or supervisory authority and applicable to a party.

1.3. **UK Data Protection Legislation** means all applicable data protection and privacy legislation in force from time to time in the UK including the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as applicable in the UK; the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

2. OBLIGATIONS OF THE PARTIES

2.1. Each of the parties agrees to comply with all applicable requirements of the relevant Data Protection Legislation. This is in addition to, and does not relieve, remove or replace, either of our obligations under the Data Protection Legislation. We agree to comply with the terms of Schedule 1 as applicable to your Personal Data.

2.2. When you sign up to our Email Signature Manager Service (the "Service") you will be allocated a Data Centre based on your address. A full list of the data centres and allocations is found here:

https://www.exclaimer.com/legal/exclaimer-cloud-endpoints/ All Active Directory data that is aggregated from Azure Active Directory and stored within our cloud service only remains within the region that the tenancy exists. As an example, for a tenancy within the USA region, Active Directory data will only reside within the USA regional data centres that we operate and not get transferred to any of our other Data Centres. Except as stated below or in the Schedules, we agree that we will not, when performing the Services, process Personal Data contained in your emails outside of the data centre(s) you are allocated when you set up the Service. You may request to move to a different data centre during your subscription of our Service.

2.3. As you are sending your Personal Data to us for processing as part of the Service, You warrant to us that you have taken all steps that are required to enable us to process the Personal Data in compliance with all Data Protection Laws and any other applicable laws, enactments, regulations, orders, standards and other similar instruments, including without limitation that you have in place the necessary notices, consents from Data Subjects for you to lawfully transfer their Personal Data to us, or have another appropriate legal basis in place to enable lawful transfer of the Personal Data to us and for us to process use and transfer such personal data in connection with the provision of the Services.

2.4. We shall process your Personal Data only in accordance with your lawful instructions, including with regard to transfers of Personal Data to a further third country or an international organisation, unless required to do so by applicable law to which we are subject; in such a case, we shall inform you of that legal requirement before processing, unless such applicable law prohibits Exclaimer from so notifying you.

2.5. We may from time to time process your Personal Data (excluding that contained in your emails) in order to provide you a more tailored service, additional information about our other products and services, technical support, chatbot and other services on our website and generally to improve our products and service offerings outside of the data centre allocated to your emails.

2.6. We never sell your Personal Data to any third parties.

3. DESCRIPTION OF PROCESSING(S)

3.1. The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on your behalf, are specified in Annex I.

Purpose limitation

3.2. We shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I, unless we receive further instructions from you.

Duration of the processing of personal data

3.3. Processing by us shall only take place for the duration specified in Annex I.

Security of processing

3.4. We shall at least implement the technical and organisational measures specified in Annex II to ensure the security of the Personal Data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects**.**

Access to your Personal Data

3.5. We shall grant access to the Personal Data undergoing processing to members of our personnel (including contractors and representatives) only to the extent strictly necessary for implementing, managing and monitoring of the contract with you for our Services. We shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

Sensitive data

3.6. We do not expect or need to receive or process any such sensitive data from you. If you advise us that your Personal Data contains sensitive data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual

orientation, data relating to criminal convictions and offences ("sensitive data"), we shall use all reasonable efforts to apply specific restrictions and/or additional safeguards to the sensitive data.

Documentation of compliance

3.7. The Parties shall be able to demonstrate compliance with this DPA.

3.7.1. We shall deal promptly and adequately with inquiries from you about the processing of your Personal Data in accordance with the applicable Data Protection Legislation.

3.7.2. We shall make available to the you all information necessary to demonstrate our compliance with the obligations that stem directly from the applicable Data Protection Legislation. At your request, we shall also permit and contribute information to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, you shall take into account relevant certifications held by us. In particular, you acknowledge that we are ISO27001 certified and audited for compliance with that standard from time to time by independent third parties. You agree that such certification and audits shall normally satisfy your audit requirements under this clause 3.7.2.

3.7.3. Any formal audit must be made only after you have given us reasonable notice of the audit, being at least 30 days and shall not interfere unnecessarily with our day to day business. You may choose to conduct the audit by yourself or mandate an independent auditor. Audits may also include inspections at our premises or physical facilities and shall, where appropriate, be carried out with reasonable notice and subject always to the duty of confidentiality. You will be responsible for all of your costs of conducting the audit.

3.7.4. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

Use of sub-processors

3.8. You authorise us to engage sub-processors listed in Annex III. We shall inform you in writing of any intended any changes of that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving you sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). We shall provide you with the information necessary to enable us to exercise the right to object. In emergencies (such as failure of a third party data centre) we may appoint a new sub-processor immediately to protect your personal data and ensure continuity of the Service in which case we will notify you as soon as practically possible.

3.9. Where we engage a sub-processor for carrying out specific processing activities (on your behalf), we shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on us in accordance with this DPA. We shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these this DPA and applicable Data Protection Legislation.

3.10. At your request, we shall provide to you a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secret or other confidential information, including personal data, we may redact the text of the agreement prior to sharing the copy.

3.11. We shall remain fully responsible to you for the performance of the sub-processor's obligations in accordance with its contract with us. We shall notify you of any failure by the sub-processor to fulfil its contractual obligations.

4. REGULATORY REQUESTS

4.1. We shall promptly notify you of any request we have received from a data subject. We shall not respond to the request itself, unless authorised to do so by you.

4.2. We shall assist you in fulfilling your obligations under applicable Data Protection Legislation to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling our obligations in accordance with (a) and (b), we shall comply with your instructions.

4.3. In addition to our obligation to assist you pursuant to Clause 4.2, we shall furthermore assist you in ensuring compliance with the following obligations if applicable under the relevant Data Protection Legislation, taking into account the nature of the data processing and the information available to us:

4.3.1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

4.3.2. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

5. *NOTIFICATION OF PERSONAL DATA BREACH*

5.1. In the event of a Personal Data breach, we shall cooperate with and assist you to comply with your obligations under the applicable Data Protection Legislation taking into account the nature of processing and the information available to us.

Data breach concerning data processed by the Controller

5.2. In the event of a Personal Data breach concerning data processed by you, we shall assist you:

5.2.1. in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after you have become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

5.2.2. in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after you have become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

5.2.3. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

Data breach concerning data processed by the Processor

5.3. In the event of a Personal Data breach concerning data processed by us, we shall notify you without undue delay after we become aware of the breach. Such notification shall contain, at least:

5.3.1. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

5.3.2. the details of a contact point where more information concerning the personal data breach can be obtained;

5.3.3. its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

5.3.4. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

6. NON-COMPLIANCE WITH THE DPA AND TERMINATION

6.1. Without prejudice to any provisions of applicable Data Protection Legislation, in the event that we are in breach of our obligations under this DPA, you may instruct us to suspend the processing of Personal Data until we comply with this DPA or the License Terms are terminated. We shall promptly inform you in case we are unable to comply with this DPA, for whatever reason.

6.2. You shall be entitled to terminate the License Terms and your subscription to our Services insofar as it concerns processing of Personal Data in accordance with this DPA if:

6.2.1. the processing of Personal Data by us has been suspended by you pursuant to clause 6.2 and if compliance with this DPA is not restored within a reasonable time and in any event within one month following suspension;

6.2.2. We are in substantial or persistent breach of this DPA or our obligations under applicable Data Protection Legislation;

6.2.3. we fail to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding our obligations pursuant to this DPA or to applicable Data Protection Legislation.

6.3. We shall be entitled to terminate the License Terms and your subscription to our Services insofar as it concerns processing of Personal Data under this DPA where, after having informed you that your instructions infringe applicable legal requirements, you insist on compliance with the instructions.

6.4. Following termination of the License Terms and your subscription to our Servces, we shall, at your choice, delete all personal data processed on your behalf and certify that we have done so, or, return all the Personal Data to you and delete existing copies unless applicable Data Protection Legislation or other laws require storage of the Personal Data. Until the data is deleted or returned, we shall continue to ensure compliance with this DPA.

SIGNED

EXCLAIMER LIMITED	**[client name]**
Signature	Signature
Print Name	Print Name
Title	Title
Date	Date

Annex 1
Processing Services

SCOPE AND PURPOSE OF PROCESSING	We will process Personal Data provided by you or collected by us in order to manage your account with us and to fulfil our contractual obligations to you. We may also process Personal Data in an aggregated and anonymised manner to analyse trends and to track your usages of and interactions with our Services to the extent necessary for our legitimate interest in developing and improving our Services and providing you with more relevant content and service offerings. We will process the Personal Data for the duration of the period in which we provide Services to you.
CATEGORIES OF DATA SUBJECTS AND PERSONAL DATA PROCESSED	Personal Data provided by you to us or collected by us in order to manage your account. This includes the following: • Customer employees' name. • Customer employees' email address. • Customer employees' business address. • Customer employees' telephone number. • Customer credit card or direct debit information (if paying by those methods) including. Debit/Credit card name. Debit/Credit card type. DebitCredit card expiry date. Debit/Credit card number. Where you log a technical support case, we will process the name and contact details of the user logging the case and the other users involved in the case. If we are provided access to email content by you to deal with your support query (with your express permission having been granted), we will have access to any Personal Data set out in that email. If you choose a server side deployment, Personal Data provided by you to us or collected by us in order to provide the Services. This includes data aggregated from your Active Directory or Google Directory or from Lists and Content such as: • Sender's/Recipient's First, Last and Full name. • Sender's/Recipient's business address. • Sender's/Recipient's company name. • Sender's/Recipient's telephone number. • Sender's/Recipient's email address. • Sender's email subject line and content information for the inclusion of the signature block. • Any other information that you expose to us via Custom Attributes within the signature block. If you choose a client side deployment, the only Personal Data we collect are the contact details of those employees of yours that we may interact with to deliver the Service (such as your IT admin or finance person (for invoices). No sensitive data is processed by us unless you include it in the content of emails.
NATURE OF PROCESSING	Personal Data provided by you to us or collected by us in order to manage your account is stored for the duration of your relationship with us. Where you log a technical support case, the data relating to the case is stored within our CRM. Personal Data provided by you to us or collected by us in order to provide the Service(s) is aggregated from your Active Directory or Google Directory and stored. This stored copy of the data is then used during the processing of the signature block prior to inclusion within the signature. This data is held separately from the main signature block, with the signature block being deleted once it has been included within the email. The aggregated data is stored for the duration of your relationship with us, after which time it is deleted in its entirety.
SUBPROCESSORS	The data centre that runs the Exclaimer Email Signature Service is owned and operated by a sub-processor named in Annex 3. We also use CRM and other systems of third parties to assist us in providing the Services to you as stated in Annex 3
DURATION AND FREQUENCY OF PROCESSING	Only for the duration of your subscription to the Service and frequency is determined by the number of emails sent by you through our data centre.
CONTACT	dpo@exclaimer.com or or write to us at FAO: The DPO, Exclaimer Limited, 250 Fowler Avenue, Farnborough, Hampshire GU14 7JP UK

ANNEX 2

Technical and Organisational measures to ensure the security of your Personal Data implemented by Exclaimer:

Security Requirement	How Data Importer implements security measures
Physical access control measures to prevent unauthorized persons from gaining access to Processing systems or premises where Personal Data are Processed or used.	*Card access control system with documentation of key holders.* *Security patrolled business park.* *Physical security service inside building.* *Monitored alarm system.* *CCTV.* *Locked server room with authorized personnel access only.*
Access control measures to prevent Processing systems from being used without authorization. Including Importer's representatives access permissions segregation to Processing systems and Personal Data such as read, copy, modify, delete.	*Individual user log-in to corporate network.* *All development, staging, production systems are located within secure Data Centres.* *Access to production level infrastructure per tenancy is limited to secure certificate endpoint.* *Processors Password policy procedures are regulated by Password Policy.* *Automatic password-protected blocking of computer after a certain period of time without user activity.*
Transmission control measures taken in by Importer and Exporter to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Information by means of data transmission facilities is envisaged.	*Encrypted access via TLS* *Hard drive encryption of all processor employee machines used to facilitate business performance protected by Bitlocker.* *Locked server room at Processor's premises with authorized personnel access only.*
Describe the measures of input control to ensure that it is possible to check and establish whether and by whom Personal Data have been entered into Processing systems, modified or removed.	*Access rights.* *Functional responsibilities.*
Assignment control measures Importer takes to ensure that, in the case of commissioned Processing, the Personal Information are Processed strictly in accordance with the instructions of the principal.	*Training of all Processor's representatives involved in Personal Data Processing for technical and organizational security measures. Follow-up training at regular intervals.* *Specific clauses in Contractor/Employment agreements with all Processor's representatives, such as: The Right for Work Results, Confidentiality, Policies and work processes, Non-compete, Non Disclosure.* *Appointment of contact person in charge of data protection (dpo@exclaimer.com).*
Availability control measures Importer applies to ensure that Personal Data are protected from accidental destruction or loss.	*Replication/Back-up processes.* *Active/Active and regional Data Centres.* *Centralized virus protection and firewall at Processor's infrastructure* *Air conditioning for work and server/network environment.* *Fire alarm system.* *Monitored alarm system.* *CCTV.* *Contingency plans.*
Measures of pseudonymisation and encryption of personal data	*All data at rest is encrypted.* *Data in transit encrypted via TLS between user end-points and core services.* *Pseudonymisation techniques assigned to all data sat within queues or at rest.*
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	*Data Protection Officer, CTO and Director of Technical Services meet regularly to review current processes and risk register.* *Regular Penetration tests carried out on infrastructure and application (service and code level).* *3rd party IDS and Cloud Native security products built into solution.*
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	*Multiple data centres operate in an active/active configuration.* *All personal data is aggregated across all per-geo data centres.*

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	*3rd party assessments of our security process and policies as part of our various ISO accreditations.* *Regular management reviews of process and risk register.* *Tooling to ensure adherence to process and policies, including but not limited to IDS, automated compliance tools, Managed Detection and Response systems and Zero Trust Access systems.*
Measures for user identification and authorisation	*MFA coupled with Zero trust.*
Measures for the protection of data during transmission	*TLS Encryption at all points of transmission, including between internal services.*
Measures for the protection of data during storage	*Data storage can only be accessed by internal services, all of which are protected by secured MFA access.* *Secure and encrypted transmission of data prior to storage.* *Storage technologies that incorporate encryption as standard.* *Customers only have access to their own data based on secure authentication and authorisation.*
Measures for ensuring physical security of locations at which personal data are processed	*Access controls at all Data Centres and Exclaimer offices.* *Secure door access, which is recorded and regularly reviewed.* *Camera surveillance and 24/7 security guard patrols in place.*
Measures for ensuring events logging	*3rd party tooling to ensure all external events are logged.* *In product logging of all key events.*
Measures for ensuring system configuration, including default configuration	*New tenancies are created using standard image which is regularly checked against a baseline.* *All delivery pipelines update default configurations where necessary, ensuring built-in security and compliance to standard images.*
Measures for internal IT and IT security governance and management	*Accredited to ISO27001 & 27018.* *Robust process, policies and tooling to ensure compliance.*
Measures for certification/assurance of processes and products	*Regular external 3rd party penetration testing of product and infrastructure (on material infrastructure change, product change or annually).* *3rd party quarterly assessment of compliance to process and certifications.* *Real-time tooling notifications on compliance to process and certifications.*
Measures for ensuring data minimisation	*Independent audit and product peer review of all data collected.*
Measures for ensuring data quality	*Independent teams assess multiple streams of data, with a focus on quality. Any quality issues are fed back into the process and resolved promptly.*
Measures for ensuring limited data retention	*All data storage retention timeframes are regularly reviewed and assessed.* *Audits of data storage are conducted by independent teams to ensure adherence to policies.*
Measures for ensuring accountability	*All core processes and procedures are owned by senior members of Exclaimer.* *All employees, contractual sub processors or other service providers are contractually bound to respect the confidential nature of all sensitive information.*
Measures for allowing data portability and ensuring erasure	*All data stored can be easily recreated from customers own store. Export and import routines exist across core data points.* *Data erasure policies exist as part of our wider information security policies.*

ANNEX 3

List of sub-processors

	Name of Sub-Processor	Company number	Address	Service Provided
1.	Microsoft Operations Limited (Where Signatures for O365 is used)	256796	70 Sir John Rogerson's Quay Dublin 2 D02R296 IRELAND	Cloud Provider for Email Signature solutions
2.	GPUK LLP	OC337146	51 De Montfort Street Leicester LE1 7BB UNITED KINGDOM	Credit Card Processing Services (only utilised if paying by Credit Card)
3	GoCardless	07495895	Sutton Yard 65 Goswell Road London EC1V 7EN UNITED KINGDOM	Direct debit payment handling facility.
4.	Google Cloud EMEA Limited (and each member of the group of companies to which it belongs) (Where Signature for G-Suite is used)	03977902	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Cloud Provider for Email Signature Solutions (only utilised if using Google Workspace email service).
5.	Salesforce UK Limited	05094083	Floor 26, Salesforce Tower, 110 Bishopsgate, London EC2N 4AY	CRM Provider
6.	Mimecast Services Limited	4901524	1 Finsbury Avenue, London, United Kingdom, EC2M 2PF	Backup provider for Exclaimer internal systems (including email archive).
7	Zendesk Inc	N/A	181 Fremont St. San Francisco, CA 94105, USA	Technical Support system for logging and tracking support queries (with UK/EU data centres allocated)