



DATA PROCESSING AGREEMENT (EU)

This Data Processing Agreement is made the 30. day of September 2022 between:

- (1) **Exclaimer Europe B.V.** having its registered office at Bollenmarkt 8 E, 1681 PJ Zwaagdijk-Oost, The Netherlands (Chamber of Commerce registration number 37161598) (hereinafter referred to as “us”, “we” or “Exclaimer”); and
- (2) Mentor IT A/S whose registered office/place of business is at Lindevej 8, 6710 Esbjerg Kommune, Denmark (hereinafter referred to as “you”, “your” or “Customer”).

SECTION I

Clause 1 Purpose and scope

- (a) The purpose of these Standard Contractual Clauses (“the Clauses”) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) as well as compliance with the Dutch GDPR Implementation Act (*Uitvoeringswet AVG*) (together referred to as “the Data Protection Legislation”).
- (b) You are the Data Controller and we are the Data Processor for the purposes of this Agreement and the Data Protection Legislation. The parties have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Annex I.
- (d) Annexes I to III are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

Clause 3 Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects. **Clause 4**

Hierarchy

In the event of a contradiction between these Clauses and the provisions of the Terms between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

SECTION II OBLIGATIONS OF THE PARTIES

Clause 5 Description of processing(s)

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.



Clause 6 Obligations of the Parties

6.1. Instructions

- (a) We shall process personal data only on your documented instructions, unless required to do so by UK, Union or Member State law to which we are subject. In this case, we shall inform you of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by you throughout the duration of the processing of personal data. These instructions shall always be documented. For this purpose, you specifically agree to our processing of your personal data as stated in this Schedule.
- (b) We shall immediately inform you if, in our opinion, instructions given by you infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Netherlands or Member State data protection provisions.

6.2. Purpose limitation

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.

6.3. Duration of the processing of personal data

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

6.4. Security of processing

- (a) 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.
- (b) 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. 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.

6.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards. We do not expect or need to receive or process any such sensitive data from you.

6.6. Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) We shall deal promptly and adequately with inquiries from you about the processing of data in accordance with these Clauses.
- (c) We shall make available to the you all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At your request, we shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, you should 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 audits shall normally satisfy the audit requirements of this clause 6.6.
- (d) 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.

- (e) 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.

6.7. Use of sub-processors

- (a) You authorise us to engage sub-processors listed in Annex III. We shall use reasonable efforts to inform you in writing of any intended any changes of that list through the addition or replacement of sub-processors at least 45 days in advance, thereby giving you sufficient time to be able to object to such changes prior to the engagement of the concerned subprocessor(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.
- (b) 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 these Clauses. We shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) 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.
- (d) 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.
- (e) We shall agree a third party beneficiary clause with the sub-processor whereby - in the event we have factually disappeared, ceased to exist in law or has become insolvent - you shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return any personal data it has stored or retained.

6.8. International transfers

- (a) Any transfer by us of personal data to a third country or an international organisation that is not recognised under GDPR as having adequate safeguards in place with respect to your personal data shall be done only on the basis of documented instructions from you or in order to fulfil a specific requirement under Netherlands, Union or Member State law to which we are subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725. For this purpose, the parties agree to the Standard Contractual Clauses to comply with Regulation (EU) 2016/679 as set out under the Data Protection Legislation to the extent that any of your personal data is transferred to a country outside the EEA that is not deemed by the European Union to have adequate safeguards in place.

Clause 7 Assistance to the controller

- (a) 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.
- (b) We shall assist you in fulfilling your obligations 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



- (c) In addition to our obligation to assist you pursuant to Clause 7(b), we shall furthermore assist you in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to us:
- (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;
 - (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;
 - (3) the obligation to ensure that personal data is accurate and up to date, by informing you without delay if we become aware that the personal data we are processing is inaccurate or has become outdated;
 - (4) the obligations in Article 32 of Regulation (EU) 2016/679.
- (d) The Parties shall set out in Annex II the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 8 Notification of personal data breach

In the event of a personal data breach, we shall cooperate with and assist you to comply with your obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to us.

8.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by you, we shall assist you:

- (a) 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); (b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679 shall be stated in your notification, and must at least include:
- (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (2) the likely consequences of the personal data breach;
 - (3) the measures taken or proposed to be taken by you to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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.

- (c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679 with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

8.2 Data breach concerning data processed by the processor

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:

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

exclaimer

- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

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.

The Parties shall set out in Annex II all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III FINAL PROVISIONS

Clause 9 Non-compliance with the Clauses and termination


- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that we are in breach of our obligations under these Clauses, you may instruct us to suspend the processing of personal data until we comply with these Clauses or the contract is terminated. We shall promptly inform you in case we are unable to comply with these Clauses, for whatever reason.
- (b) You shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - (1) the processing of personal data by us has been suspended by you pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - (2) We are in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - (3) we fail to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) We shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed you that your instructions infringe applicable legal requirements in accordance with Clause 6.1 (b), you insist on compliance with the instructions.
- (d) Following termination of the contract, 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 Union or Member State law requires storage of the personal data. Until the data is deleted or returned, we shall continue to ensure compliance with these Clauses.

SIGNATURE PAGE FOLLOWS:

SIGNED

EXCLAIMER EUROPE B.V.

MENTOR IT A/S

<p>DocuSigned by:  Signature 5536623642D440A...</p>	<p> Signature</p>
--	--



Print Name Daniel Richardson	Print Name: Jesper Ungermann Christensen
Title CTO	Title: Quality Assurance & Compliance Manager
Date 05 October 2022 1:15 PM BST	Date 30/09-2022



Annex 1 Processing Services

SCOPE AND PURPOSE OF PROCESSING	<p>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 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.</p> <p>We will process the Personal Data for the duration of the period in which we provide Services to you.</p>
CATEGORIES OF DATA SUBJECTS AND PERSONAL DATA PROCESSED	<p>Personal Data provided by you to us or collected by us in order to manage your account. This includes the following:</p> <ul style="list-style-type: none"> • Customer name. • Customer email address. • Customer business address. • Customer telephone number. • Customer credit card or direct debit information. • Debit/Credit card name. • Debit/Credit card type. • Debit/Credit card expiry date. • Debit/Credit card number. <p>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 (with your express permission having been granted), we will have access to any Personal Data set out in that email. 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:</p> <ul style="list-style-type: none"> • 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. <p>No sensitive data is processed by us unless you include it in the Content of emails.</p>
NATURE OF PROCESSING	<p>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.</p> <p>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.</p>
SUBPROCESSORS	<p>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</p>



DURATION AND FREQUENCY OF PROCESSING	Only for the duration of your subscription to the Service and frequency is determined by the number of emails/surveys sent by you through our data centre.
CONTACT	dpo@exclaimer.com or write to us at FAO: The DPO, Exclaimer Europe B.V., Bollenmarkt 8 E, 1681 PJ Zwaagdijk-Oost, The Netherlands

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.	<p>Card access control system with documentation of key holders.</p> <p>Security patrolled business park.</p> <p>Physical security service inside building.</p> <p>Monitored alarm system.</p> <p>CCTV.</p> <p>Locked server room with authorized personnel access only.</p>
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.	<p>Individual user log-in to corporate network.</p> <p>All development, staging, production systems are located within secure Data Centres.</p> <p>Access to production level infrastructure per tenancy is limited to secure certificate endpoint.</p> <p>Processors Password policy procedures are regulated by Password Policy.</p> <p>Automatic password-protected blocking of computer after a certain period of time without user activity.</p>
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.	<p>Encrypted access via TLS</p> <p>Hard drive encryption of all processor employee machines used to facilitate business performance protected by Bitlocker.</p> <p>Locked server room at Processor's premises with authorized personnel access only.</p>
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.	<p>Access rights.</p> <p>Functional responsibilities.</p>
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.	<p>Training of all Processor's representatives involved in Personal Data Processing for technical and organizational security measures. Follow-up training at regular intervals.</p> <p>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.</p> <p>Appointment of contact person in charge of data protection (dpo@exclaimer.com).</p>
Availability control measures Importer applies to ensure that Personal Data are protected from accidental destruction or loss.	<p>Replication/Back-up processes.</p> <p>Active/Active and regional Data Centres.</p> <p>Centralized virus protection and firewall at Processor's infrastructure Air conditioning for work and server/network environment.</p> <p>Fire alarm system.</p> <p>Monitored alarm system.</p> <p>CCTV.</p> <p>Contingency plans.</p>
Measures of pseudonymisation and encryption of personal data	<p>All data at rest is encrypted.</p> <p>Data in transit encrypted via TLS between user end-points and core services.</p> <p>Pseudonymisation techniques assigned to all data sat within queues or at rest.</p>
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	<p>Data Protection Officer, CTO and Director of Technical Services meet regularly to review current processes and risk register.</p> <p>Regular Penetration tests carried out on infrastructure and application (service and code level).</p> <p>3rd party IDS and Cloud Native security products built into solution.</p>



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	<i>Multiple data centres operate in an active/active configuration. All personal data is aggregated across all per-geo data centres.</i>
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	<i>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.</i>
Measures for user identification and authorisation	<i>MFA coupled with Zero trust.</i>
Measures for the protection of data during transmission	<i>TLS Encryption at all points of transmission, including between internal services.</i>
Measures for the protection of data during storage	<i>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.</i>
Measures for ensuring physical security of locations at which personal data are processed	<i>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.</i>
Measures for ensuring events logging	<i>3rd party tooling to ensure all external events are logged. In product logging of all key events.</i>
Measures for ensuring system configuration, including default configuration	<i>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.</i>
Measures for internal IT and IT security governance and management	<i>Accredited to ISO27001 & 27018. Robust process, policies and tooling to ensure compliance.</i>
Measures for certification/assurance of processes and products	<i>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.</i>
Measures for ensuring data minimisation	<i>Independent audit and product peer review of all data collected.</i>
Measures for ensuring data quality	<i>Independent teams assess multiple streams of data, with a focus on quality. Any quality issues are fed back into the process and resolved promptly.</i>
Measures for ensuring limited data retention	<i>All data storage retention timeframes are regularly reviewed and assessed. Audits of data storage are conducted by independent teams to ensure adherence to policies.</i>
Measures for ensuring accountability	<i>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.</i>
Measures for allowing data portability and ensuring erasure	<i>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.</i>

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.	Socketlabs	n/a	SocketLabs Acquisition, LLC 700 Turner Industrial Way, Suite 100 Aston, PA 19014 USA	Email delivery services (for Feedback Power Up only)
8.	Cloudflare	n/a	101 Townsend Street San Francisco, CA 94107 USA	Content delivery network and DDoS mitigation services (for Feedback Power Up only)