Introduction

The parties agree that this Data Protection Agreement ("**DPA**") sets forth each party's rights and obligations with respect to the processing and security of Customer Personal Data in connection with the Software and Services provided by Supplier. The DPA is incorporated by reference into the Commercial Terms (the "**Commercial Terms**"). The parties also agree that, unless a separate DPA signed by the parties exists, this DPA governs the processing and security of Customer Personal Data.

The provisions outlined in the Terms of this DPA pertain to Supplier acting as Processor of Customer Personal Data in the delivery of the Software and Services ("**Subject Matter**"). The DPA Terms supersede any conflicting provisions of the MetaCompliance Group Privacy Policy as they relate to the Subject Matter. For clarity, consistent with the 2021 Standard Contractual Clauses defined below, when the 2021 Standard Contractual Clauses are applicable, the 2021 Standard Contractual Clauses prevail over any other term of the Data Processing Agreement.

DATA PROCESSING AGREEMENT EFFECTIVE FROM 26th JANUARY 2026

1. Parties

1.1 The Customer is as defined in the Commercial Terms (the "**Customer**"); and

1.2 The Supplier is as defined in the Commercial Terms (the "**Supplier**").

2. Background

2.1 The Customer and the Supplier have entered into a Contract that shall require the Supplier to process Personal Data on behalf of the Customer.

2.2 This Data Processing Agreement ("**DPA**") sets out the additional terms, requirements and conditions on which the Supplier will process Personal Data when providing Services under the Contract and the Customer's obligations in respect of such Personal Data, as well as certain other Personal Data it may receive from the Supplier under the Contract. This DPA contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679 (and the Data Protection Acts 1988 to 2018, as amended) for contracts between controllers and processors.

2.3 This DPA is subject to the terms of the Contract and is incorporated into the Contract. The terms used in this DPA shall have the meanings set out in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Commercial Terms of the Contract.

2.4 The Annexes form part of this DPA and will have effect as if set out in full in this DPA. Any reference to this DPA includes Annexes.

2.5 In the event of a conflict between any provision of this DPA and any other term(s) of the Contract, with respect of the Subject Matter of this DPA, the provisions of this DPA shall prevail.

3. Definitions

The following terms in this DPA shall have the following meaning:

"Data Protection Laws"	means all applicable laws and regulations relating to the Processing of Personal Data at any time during the term of this DPA, which may include, as applicable: (1) the General

	Data Protection Regulation EU 2016/679 ("**GDPR**"); (2) the Data Protection Acts 1988 to 2018, as amended; (3) the UK Data Protection Act 2018 (**DPA2018**); (4) the UK GDPR, as defined in the DPA2018; (5) the Privacy and Electronic Communications (EC Directive) Regulations 2003; and/or (6) the ePrivacy Directive 2002/58/EC as implemented by EU member states, and any successor legislation and any other regulations, guides and codes of practice relating to data protection and privacy, in each case as amended, updated or replaced from time to time.
"Customer Personal Data"	means Personal Data Processed by the Supplier solely for the purposes of the provision of Services and as directed by the Customer expressly, by entering into the Contract and/or by configuring and interacting with any software made available as part of the Services.
"Standard Contractual Clauses"	means the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2021/914/EU as of 4th June 2021 and adopted under the UK Addendum as of 21st March 2022.
"Adequacy Decision"	means the European Commission's Adequacy Decision in respect of the transfer of Personal Data to the United Kingdom, adopted on 28 June 2021.
"Sub-processor"	means a third-party subcontractor engaged by the Supplier which, as part of the subcontractor's role in delivering the Services, will Process Personal Data on behalf of the Customer.
"Controller", "Data Subject", "Processor", "Process" or "Processing", "Personal Data", "Personal Data Breach"	shall have the meanings given to them in GDPR.

4. Processing of Personal Data

4.1 The parties acknowledge and agree that, for the purpose of the Data Protection Laws and with regard to the Processing of Customer Personal Data for the provision of Services, the Supplier is the Processor and the Customer is the Controller.

4.2 The Customer warrants and represents: (i) the transfer of Customer Personal Data to Supplier complies in all respects with Data Protection Laws (including without limitation in terms of its collection and use); and (ii) fair processing and all other appropriate notices have been provided to the Data Subjects of the Customer Personal Data (and all necessary consents from such Data Subjects have been obtained and at all times maintained and may be demonstrated to the Supplier on request) to the extent required by Data Protection Laws in connection with all processing activities which may be undertaken by the Supplier and its Sub-processors in accordance with this DPA and the Contract.

4.3 In providing the Services, the Supplier shall Process Customer Personal Data: (i) as needed to provide the Services; (ii) in accordance with written instructions from the Customer; and (iii) in accordance with the requirements of the Data Protection Laws.

4.4 The Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of the Data Protection Laws. The Customer shall ensure that any instructions to the Supplier in relation to the Processing of Customer Personal Data comply with the Data Protection Laws.

4.5 In respect of Customer Personal Data, the Customer's instructions to the Supplier regarding the Subject Matter and duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are described in **Annex A**. For the avoidance of doubt, the parties acknowledge and agree that subject to clause 5 and in addition the Processing instructions set out in this DPA and Annex A, the Customer may also issue instructions for Processing Customer Personal Data through the Services by its direct interaction with and configuration of the Services.

4.6 The Supplier shall immediately notify the Customer if, in the Supplier's reasonable opinion, any instruction given by the Customer is likely to infringe the Data Protection Laws.

4.7 Regarding the Subject Matter, the Supplier shall not process, transfer, modify, amend or alter the Customer Personal Data or disclose or permit to disclose the Customer Personal Data to any third party outside of the instructions detailed within this DPA.

4.8 The Supplier's personnel engaged in the Processing of Customer Personal Data shall be informed of the confidential nature of the Customer Personal Data and will receive appropriate training on their responsibilities. Such personnel shall be subject to appropriate confidentiality undertakings.

4.9 Taking into account the nature of Processing of Personal data in the Services provided, the Supplier shall as required by GDPR Article 32, maintain appropriate technical and organisational measures, to ensure the security of Processing, including protection against unauthorised or unlawful Processing, and against accidental or unlawful destruction, loss or alteration or damage, unauthorised disclosure of, or access to, Customer Personal Data. The parties acknowledge and agree that the security measures specified in this DPA and more specifically in **Annex B** constitute appropriate technical and organisational security measures to ensure a level of security appropriate to the risk.

4.10 The Supplier shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible and taking into account the nature of the Processing of the Customer Personal Data, in fulfilling the Customer's compliance obligations under the Data Protection Laws, including in relation to Data Subject's rights, data protection impact assessments (related to Customer's use of MetaCompliance Services) and reporting to and consulting with supervisory authorities (in connection with a data protection impact assessment related to the MetaCompliance Services).

4.11 In regard to the Subject Matter if Data Subjects, competent authorities or any other third parties request information from the Supplier regarding the Processing of Customer Personal Data, the Supplier shall refer such request to the Customer unless required otherwise to comply with the Data Protection Laws, in which case the Supplier shall provide prior notice to the Customer of such legal requirement, unless that law prohibits this disclosure on important grounds of public interest.

4.12 The Customer acknowledges that it shall receive Personal Data from the Supplier under and in connection with the Contract (including, without limitation, regarding personnel engaged by the

Supplier and its subcontractors and suppliers, as well as data subjects identifiable by images and voice recordings accessible as default options through certain of the Supplier's services). The Customer confirms that it shall Process such Personal Data as an independent Controller and in compliance with the Data Protection Laws.

5. Sub-processors

5.1 The Customer acknowledges and agrees that the Supplier may, in connection with the provision of Services, engage Sub-Processors that may be affiliates of the Supplier and/or third parties as more specifically described in **Annex A and Annex C**. Supplier's engagement of such parties shall be subject to a written (including in electronic form) contract consistent with the terms of this DPA, in relation to the required processing of Personal Data.

5.2 The Customer acknowledges that the Supplier is given general authorization to engage the Sub-Processors listed in Annex C and add (or remove) new Sub-Processors without obtaining any further written, specific authorization from the Customer. This is subject to the Processor notifying the Customer in writing of any new Sub-Processor's identity, 30 days in advance of processing Customer Personal Data (the "**Notice Period**").

5.3 If the Customer wishes to object to the relevant Sub-Processor, the Customer shall give notice hereof in writing within the Notice Period. Such notice shall include details of the alleged security risks or risk associated with the new Sub-Processor. Absence of any objections from the Customer on such grounds and within the Notice Period shall be deemed consent to use the relevant Sub-Processor.

5.4 In the event the Customer objects to a new Sub-processor, the Supplier will use reasonable efforts to address the concerns, make available to the Customer a change in Services or recommend a commercially reasonable change in Services to avoid Processing of the Customer Personal Data by the relevant new Sub-processor. If no alternative is possible, each party shall have a right to terminate the Contract between them on immediate notice and without liability or requirement for repayment of any sums by the Supplier.

5.5 The Supplier's notification of a new Sub-Processor to the Customer shall include the provision of an updated Annex C. The Supplier shall keep Annex C up-to-date on the following web-page MetaCompliance Sub-Processors | MetaCompliance.

5.6 The Supplier shall remain liable to the Customer for the performance of the Sub-processors' obligations.

6. Data Transfers

6.1 In accordance GDPR Article 28(3)(a), the Supplier shall not, and shall not permit any Sub-processor to, transfer any Customer Personal Data outside the EEA or the UK (as applicable) other than as provided in this Agreement. For the avoidance of doubt, the Customer hereby consents to the transfer and processing of the Personal Data as specified in **Annex A and C,** as they apply.

6.2 The Supplier acknowledges that in accordance with GDPR, adequate protection for the Personal Data must exist prior to any transfer outside the UK or EEA (either directly or via a Sub-processor's onward transfer) and shall enter into an appropriate agreement with the Customer and/or any sub-processor to govern such a transfer. This will include the applicable Standard Contractual Clauses, or will be reliant upon the Adequacy Decision, unless another adequacy or valid mechanism for the transfer exists.

7. Personal Data Breach

7.1 In the event of any Personal Data Breach involving the Customer Personal Data the Supplier shall:

7.1.1 Notify the Customer without undue delay (within a maximum of 48 hours) to enable Customer to comply GDPR reporting obligations and to provide reasonable assistance to the Customer when it is required to communicate a Personal Data Breach to a Data Subject.

7.1.2 Use reasonable efforts to identify the cause of such Personal Data Breach and take those steps as the Supplier deems reasonably practicable in order to remediate the cause of such Personal Data Breach.

7.1.3 Subject to the terms of this DPA, provide reasonable assistance and cooperation as requested by the Customer, in the furtherance of any correction or remediation of any Personal Data Breach.

8. Records of Processing

8.1 To the extent applicable to the Supplier's Processing for the Customer, the Supplier shall maintain all records required by Article 30(2) GDPR and shall make them available to the Customer upon request.

9. Audit Rights

9.1 The Supplier shall, and shall procure that its Sub-Processors, make available to the Customer on request reasonable information necessary to demonstrate compliance with its data protection obligations under this DPA and shall allow for and contribute to audits, including inspection at its premises, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data, provided that any such auditor is not a competitor to the Supplier.

10. Term

10.1 This DPA shall remain in full force and effect so long as:

10.1.1 The Contract remains in effect; or

10.1.2 The Supplier retains any Customer Personal Data in its possession or control.

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Contract in order to protect Customer Personal Data will remain in full force and effect.

11. Data Return and Destruction

11.1 Unless already deleted in accordance with the terms of the Contract, the Supplier shall, at the Customer's discretion and with any such request being provided by the Customer in writing, delete or return all the Customer Personal Data to the Customer after the end of the provision of Services relating to Processing, and delete existing copies unless applicable EEA or Member State law requires storage of the Customer Personal Data. If no written request is received from the Customer, the Supplier shall delete Customer Personal Data 90 days after the termination of the Contract.

11.2 On request by the Customer, the Supplier shall provide a written notice of the measures taken regarding the Customer Personal Data.

12. Indemnification

12.1 To the extent required by Article 82 of the GDPR and subject to clause 12.2 of this DPA, the Supplier agrees to indemnify the Customer against all direct costs, claims, damages or expenses incurred by the Customer due to any failure by the Supplier or its employees, sub-processors, subcontractors or agents to comply with any of its obligations under this DPA or the Data Protection Laws.

12.2 Notwithstanding anything to the contrary in this DPA or in the Contract (including, without limitation, either party's indemnification obligations), neither party will be responsible for any fines issued or levied under the Data Protection Laws against the other party by a regulatory authority or governmental body in connection with such other party's violation of the Data Protection Laws.

12.3 The Customer agrees to indemnify the Supplier against all direct costs, claims, damages or expenses incurred or received by the Supplier due to any failure by the Customer to comply with any of its obligations under the Data Protection Laws or this DPA (including, without limitation, its breach of any requirement under clause 4.2 of this DPA).

12.4 To the extent permitted by Data Protection Laws and subject to the exclusions detailed in clause 12.2 of this DPA, the total liability of each party under or in connection with this DPA howsoever caused shall be subject to the exclusions and limitations of liability set out in the Contract.

Annex A

Personal Data Processing Purposes and Details

Subject matter of processing	Details	Applies to:
Purpose	System access System administration Support Customer usage of the Software Delivery of system content according to modules subscribed to. See below:	All Customers
	Policies, Knowledge Assessments	Customers subscribing to Policy modules (PolicyLite, MetaEngage and MetaPolicy)
	eLearning, other Media	Customers subscribing to Elearning modules (MetaLearning Fusion)
	Privacy Surveys	Customers subscribing to MetaPrivacy module
	Incident Reviews	Customers subscribing to MetaIncident module
	Simulated Phishing Campaigns	Customers subscribing to MetaPhish
	SCORM transfer to Customer LMS	Customers subscribing to SCORM transfer
	Transform static PDF documents into an effective training experience	Customers subscribing to Content to Course
	Transform Customer scripts into a short AI generated video	Customers subscribing to Virtual Presenter Video
Types of Personal Data	First Name, Last Name, E-mail Address, IP Address, Department, Training Record, operating system, browser version and country	All Customers
	Active Directory Organisation Unit (OU)	Customers using Azure AD or on premise AD
	LMS ID	Customers with subscriptions to SCORM transfer
	Personal Data that Customer has included in Customer Data.	All Customers
Use of AI	AI generated Phish email creation	Customers with Premium Plus Security Awareness packages (including Multi-Language offering) using the Phish Generator.
	AI course creator	Customers who subscribe to the Content to Course Add-on.

Subject matter of processing	Details	Applies to:
	AI generated personalised videos	Customers who have availed of Virtual Presenter Add-on
Categories of Data Subjects	Customer Employees, Contractors, Suppliers, Partners and/or Affiliates.	All Customers in accordance with the Data Subject data provided to Supplier. Customer can limit this depending on their intended use of the Services.
Processing operations	Processing and storage of Customer Personal Data in order to set up, support and maintain Authorised Users accounts on the MyCompliance platform. Distribution of various notification emails initiated by the MetaCompliance MyCompliance system.	All Customers
	Distribution of simulated phishing emails specified initiated by the Customer via the MetaCompliance MyCompliance platform.	Customers subscribing to MetaPhish module
	Storage of Personal Data where it is input by the customer via the MetaCompliance MetaPrivacy module.	Customers subscribing to MetaPrivacy module
	To communicate with Customer LMS and evaluate licence count	Customers subscribing to SCORM transfer
	To utilise AI capabilities	Customers subscribing to Phish Generator, Content to Course and Virtual Presenter Software.
	To utilise translation services	Customers with multi-language features enabled.
Location of Processing operations	Processing locations within MetaCompliance Group are as set out in Annex C	All Customers.

Subject matter of processing	Details	Applies to:
	Microsoft Azure Default data centre (DC) locations are as set out in Annex C.	All Customers. There are default locations outlined herein, however, Customer can dictate changes in advance of initial tenant set-up at onboarding stage. Should Customer wish to change tenant locations mid-Contract, they should contact the support team for assistance.
	Amazon Web Services data centre (DC) locations are as set out in Annex C.	All Customers. There are default locations outlined herein, however, Customer can dictate changes in advance of initial tenant set-up at onboarding stage. Should Customer wish to change tenant locations mid-Contract, they should contact the support team for assistance.
	Userpilot, Inc., location is as set out in Annex C.	All Customers.
	Processing location in the use of AI functionality is as outlined in Annex C.	Applies to Customers who subscribe to Phish Generator, Content to Course and Virtual Presenter Video.
	Processing in the use of translation services as outlined in Annex C.	Applies to Customer with multi-language features enabled.
Retention requirements	Specific deletion timelines are as explained in the "AI at MetaCompliance" document as relevant to the Services requested by the Customer.	Customers who have requested Services which contain or use AI
	When a Customer subscription has expired or is terminated, all associated Customer Personal Data, which has not previously been deleted, is held for 90 days before it is actually deleted in order to recover from accidental subscription cancellation.	All Customers

Annex B

Security Arrangements

The Supplier shall, in order to assist the Customer to fulfil its legal obligations including but not limited to; security measures and privacy risk assessments, be obliged to take appropriate technical and organisational measures to protect the Customer Personal Data which is Processed. The measures shall at least result in a level of security which is appropriate taking into consideration:

(a) existing technical possibilities;

(b) the costs for carrying out the measures;

(c) the particular risks associated with the Processing of Customer Personal Data; and

(d) the sensitivity of the Customer Personal Data which is Processed.

The Supplier shall maintain adequate security for the Customer Personal Data. The Supplier shall protect the Customer Personal Data against destruction, modification, unlawful dissemination, or unlawful access. The Customer Personal Data shall also be protected against all other forms of unlawful Processing. Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the technical and organisational measures to be implemented by Supplier shall include as appropriate:

(a) the pseudonymisation and encryption of Customer Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services Processing Customer Personal Data;

(c) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

Further to the technical and organisational measures mentioned above, the Supplier shall implement the following measures:

(a) physical access protection whereby computer equipment and removable data containing Customer Personal Data at the Supplier's premises shall be locked up when not under supervision in order to protect against unauthorised use, impact and theft.

(b) a process for testing read back after Customer Personal Data has been restored from backup copies.

(c) authorisation control whereby the Supplier's access to the Customer Personal Data is managed through a technical system from authorisation control. Authorisation shall be restricted to those who need the Customer Personal Data for their work. User IDs and passwords shall be personal and may not be transferred to anyone else. There shall be procedures for allocating and removing authorisations.

(d) keep records of who has access to the Customer Personal Data.

(e) secure communication whereby external data communication connections shall be protected using technical functions ensuring that the connection is authorised as well

as content encryption for data in transit in communication channels outside systems controlled by the Supplier.

(f) a process for ensuring secure data destruction when fixed or removable storage media shall no longer be used for their purpose.

(g) routines for entering into confidentiality agreements with suppliers providing repair and service of equipment used to store Customer Personal Data.

(h) routines for supervising the service performed by suppliers at the premises of the Supplier. Storage media containing the Customer Personal Data shall be removed if supervision is not possible.

Annex C

I. APPROVED SUB-PROCESSORS:

1. Sub-processors required for delivery of all Services:

Sub-Processor	Purpose	Location	Sub-Processors
Microsoft Azure (contracted via Microsoft Operations Ireland Ltd)	Hosts the Services in the Cloud	Microsoft Azure Default data centre (DC) locations: United Kingdom Customers: DC in U.K. Canadian Customers: DC in Canada. American Customers: DC in United States of America. German Customers: DC in Germany European Customers outside of Germany: DC in Netherlands and Ireland	Further sub-processors available here
Amazon Web Services (contracted with "AWS Europe")	Transactional email provider	Amazon Web Services data centre (DC) locations: United Kingdom Customers: DC in U.K. Canadian Customers: DC in Canada. American Customers: DC in United States of America German Customers: DC in Germany European Customers outside of Germany: DC in Ireland	Further sub-processors available here
Userpilot, Inc.	Support customer usage of the platform	France	Amazon Web Services, France.
MetaCompliance Group entities (MetaCompliance Limited, MetaCompliance GmbH, Moch A/S, Metacompliance Ireland Ltd, MetaCompliance	Customer account services and support services	United Kingdom Germany Denmark Ireland Portugal France Norway Sweden The Netherlands	

Ireland Ltd Sucursal Portugal, MetaCompliance France, Junglemap AS, Junglemap AB, Junglemap Benelux B.V.		(as applicable and in line with each entity's place of incorporation)	

2. Translation Services for Customers with Multi-Language Subscriptions.

Sub-Processor	Personal Data Processed	Processing locations	Retention/Deletion
Weglot SAS	Name, email address, IP address and any Personal Data included in Customer Data/Content translated by Weglot SAS.	Frankfurt, Germany Weglot Sub-processors as provided for here: Trust Center - Weglot	Retained for the duration of the Subscription Term and deleted 30 days thereafter.

3. Additional Processing and Sub-Processors for use of Content To Course

A) Open AI

Metacompliance DC / Region	Home / Azure DC Location	Deployment	Personal Data Processed	Retention
IRE	West Europe (NL)	Data Zone (EU)	Other than Personal Data entered by Customers (e.g. in response to a prompt or Personal Data included in the content provided to create the course) no Customer Personal Data will be processed by this sub-processor.	No prompts or generations are stored in the model. Additionally, prompts and generations are not used to train, retrain, or improve the base models.
DACH	Germany West Central	Data Zone (EU)	As per above.	As per above.
NL	West Europe (NL)	Data Zone (EU)	As per above.	As per above.

CAN	Canada East	Standard (Canada East)	As per above.	As per above.
UK	UK South	Standard (UK South)	As per above.	As per above.
US	North Central US	Standard (North Central US)	As per above.	As per above.

B) Microsoft Document Intelligence and Azure Translator Services

Metacompliance DC / Region	Home / Azure DC Location	Processing	Personal Data Processed	Storage (temp 24 hours)
IRE	North Europe (Ire)	North Europe (Ire)	Other than Personal Data included in the content provided to create the course, no Customer Personal Data will be processed by this sub-processor.	North Europe (Ire)
DACH	Germany West Central	Germany West Central	As per above.	Germany West Central
NL	West Europe (NL)	West Europe (NL)	As per above.	West Europe (NL)
CAN	Canada Central	Canada Central	As per above.	Canada Central
UK	UK South	UK South	As per above.	UK South
US	North Central US	North Central US	As per above.	North Central US

4. Additional Processing and Sub-Processors for use of Phish Generator

Sub-Processors	Personal Data Processed	Region	Retention/Storage
Service: ChatGPT	Other than Personal Data entered by Customers (e.g. in response to a prompt **or**	Deployed : West Europe Processing : Global Standard (any region)	No prompts or generations are stored in the model.

	Personal Data included in the content provided to create the course) no Customer Personal Data will be processed by this sub-processor.		Additionally, prompts and generations are not used to train, retrain, or improve the base models.
Service: Text embedding	As per above.	As per above.	As per above.

5. Additional Processing and Sub-Processors for use of Virtual Presenter

Sub-Processor	Personal Data Processed	Region	Retention/Storage
Colossyan Inc.	Free text containing personal data (if any) provided in Customer Materials through scripts or other content. Customer confirms that no sensitive data will be transferred to the Processor.	Processing in United States, United Kingdom and Hungary (these are Colossyan and Colossyan affiliate locations). See Colossyan sub-processors detailed below	24 hours. Hard delete within 48 hours.

UTILISING AI FUNCTIONALITY

In utilising the AI functionality described above, all AI environments are closed at MetaCompliance level. Customer prompts (inputs) and completions (outputs), Customer embeddings, and Customer training data:

- are NOT available to other customers.
- are NOT available to Azure OpenAI.
- are NOT used to improve Azure OpenAI models.
- are NOT used to train, retrain, or improve Azure OpenAI Service foundation models.
- are NOT used to improve any Microsoft or 3rd party products or services without your permission or instruction.

II. APPROVED SERVICE PROVIDER

Service Provider	Service Provided	Location
Superlative Enterprises Pty Ltd	Breach Detection	United States

The above named Service Provider is included here for the purposes of transparency.

Archived Data Processing Agreement are available HERE