

# Introduction

The parties agree that this Data Protection Agreement (“DPA”) sets forth each parties rights and obligations with respect to the processing and security of Customer Personal Data in connection with the Software and Services provided by MetaCompliance Ltd. The DPA is incorporated by reference into the Commercial Terms (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 of the DPA Terms supersede any conflicting provisions of the MetaCompliance Privacy Statement that otherwise may apply to processing of Customer Personal Data. 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 6<sup>th</sup> July 2023

### 1. Parties

- 1.1 The Customer is as defined in the Commercial Terms (the “**Customer**”) and
- 1.2 **MetaCompliance Limited** incorporated and registered in Northern Ireland with company number NI049166 whose registered office is at Third Floor Old City Factory 100 Patrick Street, Londonderry BT48 7EL (the “**Supplier**”).

### 2. Background

- 2.1 The Customer and the Supplier have entered into a Contract that may 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. This DPA contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679 and UK GDPR legislation) 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 term(s) of the Contract, with respect of the subject matter of this Agreement, the provisions of this DPA shall prevail.

### 3. Definitions

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

“ <b>Data Protection Laws</b> ”	means all applicable laws and regulations relating to the Processing of Personal Data at any time during the term of this DPA,
---------------------------------	--

	including (1) the General Data Protection Regulation (GDPR, EU 2016/679); (2) the UK General Data Protection Regulation (UK GDPR) as tailored by the Data Protection Act 2018; (3) 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.
<b>“Customer Personal Data”</b>	means Personal Data Processed by MetaCompliance solely for the purposes of the provision of Services and as directed by the Customer.
<b>“Standard Contractual Clauses”</b>	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 4 <sup>th</sup> June 2021 and adopted under the UK Addendum as of 21 <sup>st</sup> March 2022.
<b>“Sub-processor”</b>	means a third-party subcontractor engaged by the Supplier which, as part of the subcontractor’s role of delivering the services, will Process Personal Data on behalf of the Customer.
<b>“Controller”, “Data Subject”, “Processor”, “Process or Processing”, “Personal Data”, “Personal Data Breach”</b>	shall have the meanings given to them in the UK and EU 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, 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 obtained and at all times maintained) 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 Agreement;
- 4.3 The Supplier undertakes to Process Customer Personal Data only: (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 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, the Processing instructions set out in this DPA and Annex A constitute the complete set of instructions from the Customer to the Supplier as they apply.
- 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 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 UK and EU 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 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.

## **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 C**.
- 5.2 The Customer acknowledges that the Supplier is given general authorization to engage 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.

- 5.3 If the Customer wishes to object to the relevant Sub-Processor, the Customer shall give notice hereof in writing within ten (10) business days from receiving the notification from the Supplier. Absence of any objections from the Customer 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 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, the parties have a right to terminate the Contract between them.
- 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.
- 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 with UK and EU 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**, as it applies.
- 6.2 The Supplier acknowledges that in accordance with the UK and EU GDPR, adequate protection for the Personal Data must exist after 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 unless another adequacy 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 with UK and EU 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) of the UK and EU 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 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 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 in accordance with Article 82 of UK and EU GDPR.

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 GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

12.3 Subject to the obligations at law outlined in clause 12.1 and the limitations detailed in clause 12.2, the liability of each party under this DPA shall be subject to the exclusions and limitations of liability set out in the Contract. Any reference to any "limitation of liability" of a party in the Contract shall be interpreted to mean the aggregate liability of a party and all of its Subsidiaries and Affiliates under the Agreement and this DPA.

## Annex A

### Personal Data Processing Purposes and Details

Subject matter of processing	Details	Applies to:
<b>Purpose</b> Specify all purposes for which the Personal Data will be processed by the Supplier	System access System administration 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
<b>Types of Personal Data</b> Specify the Personal Data that will be processed by the Supplier	First Name, Last Name, E-mail Address, Department, Training Record	All Customers
	Active Directory Organisation Unit (OU)	Customers using Azure AD or on premise AD
	LMS ID	Customers with subscriptions to SCORM transfer
<b>Categories of Data Subjects</b> Specify the categories of Data Subjects whose Personal Data will be Processed by the Supplier	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.
<b>Processing operations</b> Specify all Processing activities to be conducted by Supplier	Processing and storage of Customer Personal Data in order to set up 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

Subject matter of processing	Details	Applies to:
<b>Location of Processing operations</b> Specify all locations where the Personal Data will be processed by the Supplier	United Kingdom (MetaCompliance Group ALSO by Microsoft Azure and Amazon Web Services as applicable in Annex C) Denmark (MetaCompliance Group) Portugal (MetaCompliance Group) Ireland (MetaCompliance Group ALSO by Microsoft Azure and Amazon Web Services as applicable in Annex C). Holland (Microsoft Azure as applicable in Annex C) Canada (Microsoft Azure and Amazon Web Services as applicable in Annex C)	All Customers as applicable. Please refer to Annex C for further details.
<b>Retention requirements</b> When applicable, specify the retention time of Customer Personal Data stored by the Supplier.	When a Customer subscription has expired or is terminated, all associated Customer Personal Data 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

**Approved Sub-Processors All new Customers after 5<sup>th</sup> July 2023 can opt to amend the default application of Sub-Processors and data centre locations at onboarding via a confirmation email to MetaCompliance Ltd. The defaults that apply are:**

Sub-Processor	Location	Applies to:
Microsoft Azure (Hosts the Services in the Cloud)	Holland Dublin United Kingdom (UK) Canada	<b>Location applied in accordance with the below for new Customers after 5th July 2023::</b> <ol style="list-style-type: none"> <li>1. UK Customers will default to UK only Data Centres for Microsoft Azure.</li> <li>2. Canadian Customers will default to Canadian only Data Centres for Microsoft Azure.</li> <li>3. EEA &amp; Switzerland based Customers will default to EU based Data Centres for Microsoft Azure.</li> </ol>
Amazon Web Services (contracted with “AWS Europe”, as transactional email provider)	Dublin United Kingdom Canada	<b>Location applied in accordance with the below for new Customers after 5th July 2023:</b>

		<ol style="list-style-type: none"> <li>1. UK Customers will default to for UK only Data Centres for AWS Europe.</li> <li>2. Canadian Customers will default to the Canadian only Data Centres for AWS Europe.</li> <li>3. EEA &amp; Switzerland based Customers will default to EU based Data Centres for AWS Europe.</li> </ol>
--	--	--

**For Customers who contracted on or prior to 5<sup>th</sup> July 2023 please see detail below regarding use of Sub-Processors:**

1. Customers with a separate DPA – that document (as amended) takes precedence and outlines Sub-Processors in use.
2. Customers who were part of the group switch on 15th July 2023 to utilise AWS Europe for phish simulation notifications will use the below (unless specifically directed otherwise in writing):
  - Microsoft Azure – Dublin and Amsterdam data centres (cloud host)
  - Amazon Web Services – Dublin (transactional email provider for phish simulation notifications only)
  - Twilio for Sendgrid Services – U.S.A (transactional email provider for all other notifications from the platform).