

DATA PROCESSING ANNEX

1. DEFINITIONS

Applicable Data Protection Laws: means:

(a) To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data.

(b) To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Supplier is subject, which relates to the protection of personal data.

Client Data: means any data, which may include confidential business data and personal data that the Client processes via the Service.

EU GDPR: the General Data Protection Regulation ((EU) 2016/679).

UK GDPR: has the meaning given to it in the Data Protection Act 2018.

2. DATA PROTECTION

2.1 For the purposes of this Annex, the terms **controller, processor, data subject, personal data, personal data breach** and **processing** shall have the meaning given to them in the UK GDPR. Any defined term not defined in this Annex shall have the meaning given to it under the Terms of Use.

2.2 Each party undertakes to comply with the provisions of the Applicable Data Protection Laws and any related legislation or replacement legislation in so far as the same relates to the provisions and obligations of this Agreement.

2.3 The Client shall own all right, title and interest in the Client Data. We agree that the Client can request for the Client Data to be returned in full, or irrecoverably erased at any time, and certainly at expiry or termination in line with the Terms of Use, and we will comply with such request in full and without delay.

2.4 The Client shall be the controller, and the parties acknowledge that we will be acting as processor in respect of data processing activities in relation to Client personal data that are carried out under this Agreement.

2.5 We shall follow comprehensive industry standard security measures and procedures, ISO 27001 or equivalent, in relation to the treatment and protection of Client Data.

2.6 We shall notify the Client in writing within 24 hours of becoming aware of any loss, damage or otherwise breach to the Client Data.

2.7 We shall process the Client Data only in accordance with these Terms of Use and the written instructions of the Client from time to time and to the extent, and in such a manner, as is reasonably necessary to supply the Services in accordance with this Agreement or as is required by any applicable law.

2.8 In respect of Client Data, which is in the possession or under our control, we shall implement appropriate technical and organisational measures to protect this Client Data against unauthorised or unlawful processing and accidental loss, destruction, alteration or disclosure.

2.9 We shall place any employees, contractors or sub-contractors who are authorised to process Client Data under appropriate confidentiality obligations.

2.10 We shall not (and shall ensure that our personnel do not) publish, disclose or divulge any Client Data to any third party, nor allow any third party to process Client Data on our behalf without the prior written consent of the Client.

2.11 We shall not transfer Client personal data outside the European Economic Area without the prior written consent of the Client and only provided adequate safeguards are in place to comply with Applicable Data Protection Law.

2.12 Subject to confidentiality obligations to which we are subject, we shall provide reasonable information and assistance to the Client to demonstrate compliance with this Data Processing Annex including, where necessary, documentation proving our ISO compliance and other reasonable evidence of compliance;

2.13 We shall use reasonable endeavours in:

(a) assisting the Client with any subject access request that the Client receives relating to Client personal data processed by us under this Agreement;

(b) dealing with data breaches (including informing the Client without undue delay if we become aware of a data breach); and

- (c) the completion of data protection impact assessments, taking into account the nature of processing and the information available to us.
- 2.14 We indemnify the Client, subject to the limitation in clause 9 of the Terms of Use, against any loss or damage suffered by the Client in relation to any breach by us of our obligations under this Data Processing Annex.
- 2.15. The Client generally authorises us to engage sub-processors for the purpose of carrying out its obligations under this agreement. When engaging a sub-processor, ThreatAware shall:
 - (a) notify the Client of the engagement of each sub-processor and shall give the Client the opportunity to object where it has evidence that the sub-processor is not compliant with Applicable Data Protection Laws. For the avoidance of doubt, the Client consents to sub-processors who are engaged as at the date of this agreement as notified to the Client within this Annex; and
 - (b) enter into a contract with each sub-processor which contains data protection provisions no less onerous than this Data Processing Annex
 - (c) be responsible and fully accountable for the actions (or inaction) their subcontractors take while fulfilling their role under this Agreement.
- 2.16 You consent to the processing by us of the Client Data to provide the Services under this agreement. This includes the processing activities set out in the table below. You shall ensure you have obtained all necessary consents for the processing of any Client personal data for these purposes.

<p>Subject matter and purpose of the processing:</p>	<p>The Client requires a technology solution to help aggregate and visualise event data from across its IT estate. This data is largely related to security and risk events generated by security software within the Clients IT systems and platforms, or through service providers that host/provide those platforms.</p> <p>The Client may also make use of task management systems to help track and rectify progress against certain risk events or operational activities.</p> <p>ThreatAware will provide the software and services, including but not limited to, securely hosting the Client Data (if necessary, through appropriate sub-processors) to deliver this solution.</p>
<p>Duration of the processing:</p>	<p>A rolling basis in line with the termination of the agreement Client owns and maintains all rights in the Client Data.</p> <p>ThreatAware warrants that it will not retain or otherwise process/share/sell the Client Data at any time, including post termination, unless expressly agreed in advance in writing by the Client, and in any case only on the basis that it will be in a completely anonymised form.</p>
<p>The nature of the processing:</p>	<p>Securely hosting the Client Data and associated event data equivalent to the ISO 27001 security standard.</p> <p>Aggregating and visualising the data in appropriate software dashboards.</p> <p>Generating events/alarms in relation to the risk data.</p>
<p>Type of personal data:</p>	<p>The scope of personal data contained within the event data could be broad but will largely relate to Name, IP address, IT access/usage/browsing or compliance data</p>
<p>Categories of data subjects:</p>	<p>Customer Employee</p>
<p>Sub-processors:</p>	<p>Amazon AWS – Cloud Infrastructure Hubspot CRM and Marketing Platform Mailchimp – Email and Marketing Automation</p>