



DATA PROCESSING TERMS**1 DATA PROTECTION**

1.1 The purpose of these Data Processing Terms is to describe each party's rights and obligations with respect to the processing of the Customer's Personal Data by the Supplier in connection with the Platform Services.

1.2 In these Data Processing Terms, the following words and phrases shall have their respective meanings given below:

"Authorised User(s)"	has the meaning given in the General Terms and Conditions for Platform Services.
"Customer's Personal Data"	all Personal Data that is: 1. controlled by the Customer; and 2. collected, generated, or otherwise Processed by the Supplier in connection with the provision of the Platform Services.
"Data Protection Act 2018"	the UK Data Protection Act 2018.
"Data Protection Laws"	as applicable to the Customer's Personal Data: 1. GDPR; 2. the: (i) Data Protection Act 2018; and (ii) UK GDPR; 3. the Privacy and Electronic Communications (EC Directive) Regulations 2000; and 4. any applicable replacement or supplementary legislation governing the use and security of the Customer's Personal Data.
"Data Processing Activities"	the following Processing activities carried out: for and on behalf of; or under the instruction of, the Customer: 1. hosting and infrastructure management including with respect to the Customer's Personal Data hosted in the Platform; 2. support and maintenance with respect to the Customer's Personal Data hosted in the Platform; 3. troubleshooting with respect to the Customer's Personal Data hosted in the Platform; and 4. such other activities where the Supplier Processes the Customer's Personal Data on behalf of the Customer as the Customer's Processor.
"Data Processing Audit"	an audit (including inspection) to confirm the Supplier's compliance with its obligations under paragraph 6.1.
"Data Subject Request" or "DSR"	a request made by a Data Subject whose Personal Data is Processed by the Supplier under and/or in connection with the Agreement or the Platform Services, which relates to the exercising of their data protection rights granted under Articles 12 to 22 of GDPR and/or UK GDPR.
"EEA"	the European Economic Area.
"Fair Processing Notice"	has the meaning given in the General Terms and Conditions for Platform Services.
"GDPR"	the EU General Data Protection Regulation (2016/679).

- | | |
|------------------------------------|---|
| “Lawful Transfer Mechanism” | <p>a data transfer agreement designed to ensure that the Processing of the Customer's Personal Data in a Third Country is compliant with Data Protection Laws, for example:</p> <ol style="list-style-type: none"> 1. the EU Standard Contractual Clauses in the form annexed to the European Commission's decision of 4 June 2021 (the “EU SCCs”); and/or 2. the UK International Data Transfer Agreement for the transfer of Personal Data to persons established in Third Countries or International Data Transfer Addendum to the EU SCCs. |
| “Legislation” | has the meaning given in the General Terms and Conditions for Platform Services. |
| “Regulator” | <p>as applicable to the supervision of the Processing of the Customer's Personal Data:</p> <ol style="list-style-type: none"> 1. the UK Information Commissioner's Office; and 2. the Supervisory Authority Concerned. |
| “Security Controls” | the “ <i>Security Controls</i> ” document located on the Trust Site documenting the technical and organisational security measures applied to the Platform. |
| “Sub-processor” | a third-party subcontractor or service provider to the Supplier that has been appointed by the Supplier to Process the Customer's Personal Data in connection with the provision of the Platform Services. |
| “Sub-processor List” | a list of the Sub-processors (as may be updated from time to time in accordance with these Data Processing Terms). |
| “Subscription Period” | has the meaning given in the General Terms and Conditions for Platform Services. |
| “Third Country” | <p>a territory that:</p> <ol style="list-style-type: none"> 1. is outside of the UK or EEA; and 2. does not, at the time of the Processing, require specific authorisation because of an adequacy decision under GDPR / UK GDPR Article 45. |
| “UK” | the United Kingdom of Great Britain and Northern Ireland. |
| “UK GDPR” | the UK retained version of GDPR (as defined in section 3(10) and supplemented by section 205(4) of the Data Protection Act 2018). |
- 1.3 The words “**Controller**”, “**Data Subject**”, “**Personal Data**”, “**Personal Data Breach**”, “**Process**” (and its derivatives), and “**Supervisory Authority Concerned**” shall each have their respective meanings given in GDPR or UK GDPR as applicable to the Customer's Personal Data.
- 2 RELATIONSHIP TO THE AGREEMENT**
- 2.1 The rights and obligations contained in these Data Processing Terms apply in addition to the other provisions of the Agreement that may concern the use and/or protection of the Customer's Personal Data.
- 3 GDPR / UK GDPR ARTICLE 28(3)**
- 3.1 The parties agree that the:
- (a) **subject matter, nature and purpose** of the Processing of Customer's Personal Data by the Supplier is the performance of the Platform Services under the Agreement;

- (b) **types of Personal Data** comprise the Customer's Personal Data as made available to the Supplier by the Customer or an Authorised User (including, for example, names, e-mail addresses, and user identifiers);
- (c) **categories of Data Subjects** are the Authorised Users; and
- (d) **duration of the Processing** will be the relevant Subscription Period.

4 CLASSIFICATION

- 4.1 As between the parties, and for the purpose of construing the Data Protection Laws and these Data Processing Terms, if and to the extent the Supplier carries out Data Processing Activities:
- (a) the Customer will be the Controller of the Customer's Personal Data; and
 - (b) the Supplier will be:
 - (i) the Processor; or
 - (ii) where the Customer is itself a Processor to its customer, a sub-Processor.
- 4.2 Where the Supplier is not carrying out Data Processing Activities, the Supplier shall Process such Customer's Personal Data as an independent Controller in accordance with the Agreement (including the Supplier's Fair Processing Notice).

5 CUSTOMER'S OBLIGATIONS

- 5.1 The Customer warrants, represents, and undertakes to the Supplier that:
- (a) the Customer's Personal Data is, and shall be, provided and/or made available in accordance with the Data Protection Laws; and
 - (b) all instructions given to the Supplier in respect of the Customer's Personal Data are lawful.

6 SUPPLIER'S OBLIGATIONS

- 6.1 The Supplier shall, in respect of (and in connection with) the Data Processor Activities comply with its obligations described in this paragraph 6.

Compliance with Data Protection Laws

- 6.2 The Supplier shall:
- (a) comply with its mandatory obligations under the applicable Data Protection Laws; and
 - (b) not Process the Customer's Personal Data in a manner that it knows (or reasonably ought to have known) will result in the Customer breaching its obligations under the Data Protection Laws.

Compliance with the Customer's instructions

- 6.3 The Supplier shall:
- (a) Process the Customer's Personal Data in accordance with the Customer's documented instructions which are to Process the Customer's Personal Data:
 - (i) to the extent, and in such manner as is reasonably necessary for, the Supplier to discharge its obligations under the Agreement; and
 - (ii) as required by the Data Protection Laws; and
 - (b) inform the Customer if, in its reasonable opinion, an instruction given by the Customer is in breach of Data Protection Laws.

Data Subject Requests

- 6.4 The Supplier shall with respect to Data Subject Requests:
- (a) promptly notify the Customer if it receives a Data Subject Request (except if and to the extent prevented by applicable Legislation); and
 - (b) thereafter provide, at the Customer's reasonable cost and expense, such commercially reasonable assistance as the Customer may reasonably request to help the Customer to respond to such Data Subject Request.

Supplier's personnel

- 6.5 The Supplier shall ensure that its personnel who are, as part of the Platform Services, required to Process the Customer's Personal Data are:
- (a) only granted access to such Customer's Personal Data as strictly necessary for the performance of that person's duties;
 - (b) made aware that the Customer's Personal Data is the confidential information of the Customer;
 - (c) appropriately vetted in accordance with applicable Legislation;
 - (d) adequately trained in connection with the Data Protection Laws; and
 - (e) the subject of written obligations of confidence that survive termination of their engagement.

Appointment of Sub-processors

- 6.6 The Supplier shall be permitted to engage Sub-processors to Process the Customer's Personal Data and, in respect of such Sub-processors:
- (a) the Supplier shall ensure that any contract with such Sub-processor imposes obligations that are equivalent to the obligations that the Supplier is subject to under this paragraph 6;
 - (b) the Supplier shall remain responsible for the acts and omissions of such Sub-processors as if such acts and omissions were the Supplier's own;
 - (c) the Supplier shall maintain a Sub-processor List;
 - (d) make the Sub-processor List available to the Customer promptly following a request;
 - (e) the Supplier shall, where possible, give the Customer reasonable advance notice of its intention to appoint a new Sub-processor to the Sub-processor List (a "New Sub-processor") in order to give the Customer an opportunity to object to the appointment;
 - (f) the Customer shall be given ten (10) days from the day on which it receives the Supplier's notice above to object to the Supplier's use of a New Sub-processor provided that such objection is on the grounds that the New Sub-processor will not, in all material respects, be able to comply with the terms of this paragraph 6;
 - (g) the Customer's failure to notify the Supplier of an objection to a New Sub-processor shall constitute the Customer's irrevocable consent to the appointment of the New Sub-processor;
 - (h) where the Customer reasonably objects to the appointment of a New Sub-processor in accordance with paragraph 6.6(f) then the parties shall use their respective reasonable endeavours to resolve the objection by seeking to agree (where practicably possible):
 - (i) an alternative to the New Sub-processor;
 - (ii) additional terms concerning the appointment of the New Sub-processor; or
 - (iii) early termination of the Agreement and a pro-rated refund for Platform Services not received.

Security Controls

- 6.7 The Supplier apply the Security Controls to the extent applicable to the Processing of the Customer's Personal Data (which the Customer agrees to be adequate).

Personal Data Breaches

- 6.8 The Supplier shall promptly notify the Customer upon becoming aware of a Personal Data Breach and provide the Customer with the following information as it becomes available:
- (a) a description of the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects concerned;
 - (b) the name and contact details of the Supplier representative from whom more information can be obtained; and
 - (c) a description of the measures taken, or proposed to be taken, to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Information provision

- 6.9 The Supplier shall:
- (a) provide such information as is reasonably requested by the Customer in respect of the Data Processing Activities (provided that such information shall be construed as the Supplier's confidential information)

- (b) comply with any obligation to carry out a data impact assessment or consult with a Regulator; and
- (c) on termination of the Agreement for whatever reason, or upon written request from the Customer at any time (subject to: applicable laws and backup retention cycles; and the necessity of Processing for the continued provision of the Platform Services) return or destroy (by putting Customer's Personal Data beyond use) the Customer's Personal Data in accordance with the General Terms and Conditions for Platform Services.

Processing of Customer's Personal Data in Third Countries

- 6.10 The Supplier shall not Process the Customer's Personal Data in a Third Country otherwise than in compliance with Data Protection Laws (including by putting in place a Lawful Transfer Mechanism).

Audit

- 6.11 The Supplier shall, subject to paragraph 6.12, allow for, and give such reasonable assistance as is requested by the Customer in connection with, the conduct of a Data Processing Audit.
- 6.12 In respect of a Data Processing Audit, the parties agree that:
- (a) to request a Data Processing Audit, the Customer shall submit a detailed audit plan to the Supplier at least sixty (60) days in advance of the proposed date for the Data Processing Audit;
 - (b) the Customer shall ensure that the audit plan describes the proposed scope, duration, and start date of the Data Processing Audit (which scope shall not include an audit of any third-party Cloud provider's premises, systems or environment);
 - (c) the Supplier will review the audit plan and shall inform the Customer of any concerns or questions (for example, concerns that the proposed scope could compromise: (i) the Supplier's confidentiality obligations to third parties; or (ii) the security of the Platform);
 - (d) the parties shall use their respective reasonable endeavours to cooperate and agree a final audit plan for the Data Processing Audit provided that all Data Processing Audits must:
 - (i) be conducted during the Supplier's normal office hours;
 - (ii) have reasonable consideration to the Supplier's internal policies applicable to its premises (including with respect to health and safety and on-premise security); and
 - (iii) not unreasonably interfere with the Supplier's business activities;
 - (e) audit reports prepared during or as a result of the Data Processing Audit shall constitute confidential information under the Agreement and shall only be used by the Customer for the purposes of meeting its audit requirements under the Data Protection Laws;
 - (f) the Customer may only perform a Data Processing Audit (under all Order Forms) once in each successive period of twelve (12) calendar months except: (i) where an additional Data Processing Audit is required by Data Protection Laws or a Regulator applicable to the Customer; or (ii) in the event that the Supplier suffers a Personal Data Breach impacting the Customer's Personal Data;
 - (g) the Customer (or an independent third-party auditor (approved by the Supplier)) will comply with the confidentiality obligations set out in the Agreement;
 - (h) if the proposed scope of the Data Processing Audit has been adequately addressed in an audit report:
 - (i) commissioned by the Supplier in the twelve (12) months prior to the proposed Data Processing Audit; and
 - (ii) prepared by a qualified third-party auditor,
- and, in respect of such report, the Supplier confirms there are no known material changes in the controls audited, then the Customer shall accept the findings in the Supplier-commissioned report in lieu of requesting a Data Processing Audit of the controls covered by such report;
- (i) all Data Processing Audits shall be conducted at the Customer's sole cost and expense; and
 - (j) any request for the Supplier's assistance in connection with a Data Processing Audit requiring the use of resources different from or in addition to those required for the provision of the Platform Services will be considered an additional service which reasonable additional Fees and expenses may be charged.