CLIENT DATA PROTECTION POLICY

KEY PRINCIPLES

This policy applies in all instances of the Client's engagement with the Supplier in accordance with the Key Terms and the General Terms and Conditions.

1. DEFINITIONS

1.1 For the purposes of this Client Data Protection Policy, the following words and phrases will bear the following meanings:

"**Agreement**" means the agreement (including both the Key Terms and General Terms and Conditions), together with any schedules, annexes, policies, guidelines and procedures (as set out in the Key Terms and GTC) and amendments agreed in writing and executed by both parties from time to time. In the event of any conflict between the documents that comprise the Agreement, unless there is specifically a statement to the contrary in the General Terms and Conditions, the Key Terms shall prevail over the General Terms and Conditions which shall prevail over any schedules, annexes, policies guidelines and procedures. Any amendments agreed in writing and duly executed by the Parties shall expressly state which paragraphs and clauses in which document they vary;

"**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Process**", "**Processed**", "**Processing**", and "**Processor**" as set out in the Data Protection Legislation;

"**Data Protection Guidance**" means legally binding guidelines, recommendations, best practice, opinions, directions, decisions, codes of practice and codes of conduct issued, adopted or approved by the European Commission, the Article 29 Working Party, the European Data Protection Board, the UK's Information Commissioner's Office and/or any other supervisory authority or data protection authority from time to time in relation to the subject matter of the Data Protection Legislation;

"**Data Protection Legislation**" means the UK Data Protection Legislation and any applicable European Union legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the relevant data protection or supervisory authority and applicable to a Party;

"**Data Subject Request**" means a request by, or on behalf of, a Data Subject to exercise a Data Subject right under the Data Protection Legislation, including a data subject access request;

"**Personnel**" means the staff of the Supplier and the staff of any Subprocessors;

"**Subprocessor**" means a subcontractor appointed by the Supplier, which processes Personal Data;

"**Time and Materials Basis**" means a time and materials basis provided that such costs are reasonable;

"**UK Data Protection Legislation**" means all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**"), the Data Protection Act 2018, the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

1.2 Capitalised terms which are not defined above shall have the meanings set out elsewhere in the Agreement.

2. CONTROLLER AND PROCESSOR

2.1 The Parties agree that for the purposes of processing Personal Data in connection with the Agreement, the Client is the Data Controller and the Supplier is the Data Processor of such Personal Data.

3. WRITTEN INSTRUCTIONS

3.1 The Supplier will only process the Personal Data in accordance with the Client's written instructions and for the purposes of performing the Services. The Parties agree that the Agreement represents the written instructions of the Client.

3.2 The Supplier shall immediately inform the Client if, in its opinion, an instruction infringes the Data Protection Legislation.

4. WRITTEN DESCRIPTION OF PROCESSING

4.1 A description of the nature and purpose of the processing carried out by Supplier under the Agreement, and the type of Personal Data and categories of Data Subjects involved, is set out in Annex 1 to this Client Data Protection Policy. Both Parties shall keep this information up-to-date while the Agreement is in force.

5. SECURITY

5.1 The Supplier shall ensure that the Supplier Software is designed and managed in alignment with IT security standards that represent good industry practice. Supplier shall ensure that the Supplier Software complies with ISO 27001 standard.

5.2 The Parties agree that Supplier's compliance with the provisions of **paragraph 5.1 of this Client Data Protection Policy** shall constitute an effective discharge of the processor's obligation set out in Article 32 of the GDPR.

6. NO OFFSHORING

6.1 The Supplier shall not process Personal Data outside the UK or the European Economic Area without the Client's prior written consent, provided that such transfer or processing to Personnel in the USA will be permitted on the basis of the Supplier's then-current intra-group data sharing agreement ("**DSA**"), provided further that the DSA is at all relevant times consistent with and embodies the EU's Standard Contractual Clauses for international processor to subprocessor or controller-to-processor data transfers, as appropriate and

that Client has, prior to such transfer or processing, if required, executed such document in its capacity as data controller as may be necessary to give appropriate effect to such permitted transfer.

7. ICO REQUESTS

7.1 The Supplier shall co-operate with the Client to enable the Client to comply in good time with any enquiry made, or investigation or assessment of processing initiated by any regulator (including the Information Commissioner's Office). Supplier shall be entitled to charge on a Time and Material Basis for such cooperation.

8. DATA SUBJECT REQUESTS

8.1 The Supplier shall as soon as reasonably practicable (and in any event by the end of the fifth (5) working day following receipt of a Data Subject Request), inform the Client if it receives a Data Subject Request.

8.2 The Supplier shall be entitled to charge the Client on Time and Materials Basis in relation to work incurred in responding to Data Subject Requests.

9. SUBPROCESSORS

9.1 The Supplier shall ensure that any processing carried out by the Supplier's Subprocessors shall be carried out under a written contract imposing on the Subprocessor equivalent obligations as are imposed on the Supplier under this Agreement in respect of the processing, confidentiality and protection of Personal Data.

9.2 Subject to **paragraph 9.3 of this Client Data Protection Policy**, the Supplier shall not subcontract the processing of the Personal Data without the prior written consent of the Client, such consent not to be unreasonably withheld or delayed.

9.3 The Client consents to the Supplier subcontracting the specified elements of the Supplier's obligations to Amazon Web Services ("**AWS**") which the Supplier has specified as a Subprocessor, provided that the Client may only withdraw such consent if there is a genuine cause for concern that such sub-processing is not being undertaken in accordance with the terms of the Agreement.

9.4 The Supplier will give the Client not less than one (1) month prior notice (other than in the case of an emergency) of the proposed appointment of any new or replacement Subprocessor.

9.5 If the Client does not object to such appointment in writing (giving reasons for its objection) within thirty (30) days after receiving notice of the proposed appointment, then the Client shall have deemed to have given its written consent to such appointment.

9.6 If the Client does object to such appointment in writing (giving reasons for its objection) within thirty (30) days after receiving notice of the proposed appointment, then:

9.6.1 either Supplier shall withdraw the proposal, in which case no further action shall be taken, or

9.6.2 the Supplier shall not withdraw the proposal, and the Client shall be deemed to have given its prior written consent to the appointment of the Subprocessor for the purpose of paragraph 9.2 of this Client Data Protection Policy, and the Client shall be entitled to terminate the Agreement without penalty.

10. PERSONNEL

10.1 The Supplier shall take reasonable steps to ensure the reliability of any Personnel who have access to any Personal Data in connection with the Agreement, and ensure that such Personal Data shall only be accessible by Personnel:

10.1.1 to the extent necessary to properly perform their duties in relation to the Agreement;

10.1.2 who are informed of its confidential nature and the security procedures relating to it, and who are contractually bound to maintain its confidentiality; and

10.1.3 who are appropriately reliable, qualified and trained.

11. PERSONAL DATA BREACH

11.1 The Supplier shall without undue delay (and in any event within twenty-four (24) hours of becoming aware) notify the Client of any Personal Data Breach of which it becomes aware.

11.2 The Supplier shall take all steps as reasonably required by the Client, and provide all reasonable assistance to the Client, in order for the Client to deal with any Personal Data Breach notified in accordance with paragraph 11.1 of this Client Data Protection Policy including, where relevant, notification to the Information Commissioner's Office and notification to Data Subjects.

11.3 Where a Personal Data Breach results from a breach of the Supplier's obligations under the Agreement (including a breach by Supplier's Subprocessors), the Supplier shall bear its costs of complying with paragraphs 11.1 and 11.2 of this Client Data Protection Policy subject to the limitations and exclusions set out in clause 12 (Limits of Liability) of the GTC.

11.4 Where a Personal Data Breach does not form a breach of the Supplier's obligations under the Agreement, the Client shall pay Supplier's costs of complying with paragraphs 11.1 and 11.2 of this Client Data Protection Policy on a Time and Materials Basis.

12. ARTICLE 30 RECORDKEEPING

12.1 The Supplier shall maintain, and shall make available to the Client on request, a record of all categories of processing activities carried out on behalf of a controller, containing:

12.1.1 the name and contact details of the Client, and, where applicable, of the Client's representative, and the Client's data protection officer;

12.1.2 the name and contact details of the Supplier, and, where applicable, of the Supplier's representative, and the Supplier's data protection officer

12.1.3 the categories of processing carried out on behalf of the Client;

12.1.4 where applicable, transfers of personal data to a third country or an international organisation and the documentation of suitable safeguards; and

12.2 a general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR.

13. SERVICE OVERSIGHT

13.1 The Supplier shall provide the Client with such information about and oversight over the Supplier's processing of Personal Data as will allow the Client, acting reasonably, to comply with the accountability principle of the GDPR.

13.2 The Client shall be entitled (but not more than once every six (6) months, except in cases of Personal Data Breach) to have a meeting with the Supplier (whether in person or by video link, as is most convenient to both parties) to discuss and review the Supplier's processing of Personal Data.

13.3 Where the Client requires more information about and oversight over the Supplier's processing of Personal Data that it provided for in **paragraphs 13.1 and 13.2 of this Client Data Protection Policy**, it shall be entitled to purchase such additional information and oversight at the Time and Material Basis, subject to the reasonable availability of the Supplier's resources.

14. AUDIT BY THE CLIENT

14.1 The Client and/or its designee, who shall not be the Supplier's competitor, (or, upon the Client's request, any Client Regulator) shall have the right, upon at least fifteen (15) Business Days' notice (unless shorter notice is required by the Client Regulator) and during Business Hours, to inspect and audit relevant books and records, other relevant documentation, systems, technology as well as relevant facilities and business premises of the Supplier, to the extent required to ascertain the Supplier's compliance with the terms of the Agreement.

14.1.1 For the avoidance of doubt, prior notice per **paragraph 14.1 of this Client Data Protection Policy** shall be required in circumstances when an audit is required to investigate a breach of the Supplier's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data; and, when the Client reasonably believes that the Supplier is in material breach of this Client Data Protection Policy.

14.2 Without limiting the generality of the foregoing, the Supplier shall cooperate in good faith with the Client and/or its designee or the Client Regulator or a law enforcement body to facilitate

the Client's exercise of its rights under this **paragraph 14 of this Client Data Protection Policy** and shall provide the Client or its designee or the Client Regulator or a law enforcement body all reasonable assistance as they may request.

14.2.1 The Client will not be required to give prior notice of an audit if an audit is required by the Client Regulator or a law enforcement body and the Client Regulator and / or law enforcement body requires that prior notice should not be given.

14.3 The Client may only exercise its right to conduct audits set out in this **paragraph 14 of this Client Data Protection Policy** once in each rolling 12-month period, except if:

14.3.1 the Client reasonably believes that Supplier is in material breach of this Agreement or that there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data; or

14.3.2 otherwise required by a Client Regulator or a law enforcement body.

14.4 The Supplier shall bear all reasonable costs incurred in respect of any audit carried out under this **paragraph 14 of this Client Data Protection Policy**, unless the audit reveals that the Client is in material breach of the Agreement, in which case the reasonable costs shall be borne by the Client.

15. EXPIRY AND TERMINATION

15.1 Upon cancellation, expiry or termination of the Agreement, the Supplier shall, at the choice of the Client, either:

15.1.1 deliver up to the Client all Personal Data in its then current format; or

15.1.2 delete all Personal Data,

except that the Supplier shall be entitled to retain a copy of all or part of the Personal Data where, in the Supplier's reasonable opinion, the retention of such copy is advisable in the light of regulatory requirements or for the defence of legal claims.

ANNEX 1 — DESCRIPTION OF PROCESSING

Data Controller
The Client, as set out above. Data Protection Officer: as set out on the Client's website (if any).
Data Processor
The Supplier, as set out above. Data Protection Officer: as set out on the Supplier's website (if any).
The nature of the processing is:
Collecting and processing of the End User data for the purpose of processing payments. Reporting the such data as part of management information.
The purpose of the processing is:
Legitimate interest and performance of a contract.
The categories of Personal Data being processed are:
online identifiers including cookie identifiers, internet protocol addresses, device identifiers as well as further information as set out in the Key Terms and clause 2.4 of the GTC.
The categories of Data Subjects include:
the End Users which relate to the Services received by the Client.

Please see https://token.io/privacy for additional information on how the Supplier collects, uses and secures the Personal Data and the conditions in which the Supplier may disclose it to a third-party.

ANNEX 2 — JURISDICTIONAL SPECIAL TERMS

This Annex 2 to the Client Data Protection Policy sets out the jurisdictional specific terms where Supplier EEA is providing Services as set out in the Key Terms.

1. DEFINITIONS

1.1 The following definition in sub-paragraph 1.1 of the GTC shall be deleted and replaced with:

*""**Client Regulator**" means any public body having regulatory, enforcement and/or supervisory authority over the Client's receipt and use of the of the Services in accordance with the Agreement;"*

1.2 The following definition in sub-paragraph 1.1 of the GTC should be deleted and replaced with:

*""**Data Protection Guidance**" means legally binding guidelines, recommendations, best practice, opinions, directions, decisions, codes of practice and codes of conduct issued, adopted or approved by the European Commission, the Article 29 Working Party, the European Data Protection Board, Germany's Federal Data Protection Officer (Bundesdatenschutzbeauftragter), Germany's State Data Protection Officers (Landesdatenschutzbeauftragte) and / or any other supervisory authority or data protections authority from time to time in relations to the subject matter of the Data Protection Legislation;"*

1.3 The reference in sub-paragraph 1.1 of the GTC to "the UK Data Protection Legislation" in the definition "**Data Protections Legislation**" should be replaced by "the German Data Protection Legislation".

1.4 The definition in sub-paragraph 1.1 of the GTC "**UK Data Protection Legislation**" should be deleted and replaced with:

*""**German Data Protection Legislation**" means all applicable data protection and privacy legislation in force from time to time in Germany including the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**"), the Federal Data Protection Act (Bundesdatenschutzgesetz), the applicable State Data Protection Acts (Landesdatenschutzgesetze), the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended."*

1.5 The reference in sub-paragraph 11.2 of this Client Data Protection Policy to "the Information Commissioner's Office" shall by replaced by "the competent State Data Protection Officer (*Landesdatenschutzbeauftragter*)".