CLIENT DATA PROTECTION POLICY

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

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, rectification, erasure, objection, restriction, and portability 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.

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 or itself a Processor on behalf of third party Controllers and the Supplier is the Data Processor or where the Client is a Processor on behalf of third party Controllers, Supplier a sub-processor of such Personal Data.

2.2 In the event that Token is the regulated entity under the agreement, and will be carrying out the KYB requirements, Token shall be the Data Controller as outlined in the Privacy Policy published on Token's website.

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. Client is authorised to transmit instructions on behalf of its customers to Supplier for the purpose of Supplier providing services pursuant to the Agreement.

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 will implement and maintain all appropriate technical and organizational security measures to protect from a Personal Data Breach and to preserve the security, integrity and confidentiality of Personal Data. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Supplier shall ensure that the Supplier Software complies with ISO 27001 standard.

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

6.2 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.

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 only charge at cost and 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), forward such Data Subject Request to the Client.

8.2 The Supplier shall be entitled to only charge the Client at cost and on a Time and Materials Basis for such cooperation.

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. Supplier remains fully liable for any breach of this DPA or the Agreement that is caused by an act, error or omission of such Subprocessor. Client may request that Supplier audit a Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist in obtaining a third-party audit report concerning Subprocessor's operations) to ensure compliance with its obligations imposed by Supplier in conformity with this DPA. Such third-party audit reports include, but are not limited to: SSAE18 (SOC 1/SOC 2/SOC 3) audit reports, penetration test summaries, business continuity plans, PCI DSS AOC, ISO27k Certificates, and NIST certificates.

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

1.1.3 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. Such notification shall include written details of the Personal Data Breach as soon as it becomes known or available to Supplier, including: (a) a description of the nature of the incident, including the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned; (b) a description of the likely consequences of the incident; and (c) a description of the measures taken or proposed by Supplier to address the incident, including measures to mitigate its possible adverse effects. Furthermore, in the event of a Personal Data Breach, Supplier shall provide timely information and cooperation as Client may require to fulfil Client's contractual obligations and data breach reporting obligations under applicable Data Protection Legislation and take such measures and actions as are appropriate to remedy or mitigate the effects of the Personal Data Breach and keep Client up-to-date about all developments in connection with the Personal Data Breach.

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. The content and provision of any notification, public/regulatory communication or press release concerning the Personal Data Breach directly impacting Personal Data Controlled by the Client shall be solely at Client's discretion, except as otherwise required by applicable law.

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 the 'Limits of Liability' section 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
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. Examples of the documents referenced in paragraph 14.1 of this Policy include, but are not limited to: SSAE18 (SOC 1/SOC 2/SOC 3) audit reports, penetration test summaries, business continuity plans, PCI DSS AOC, certificates of insurance, ISO27001 Certificates, NIST certificates, and any other documents related to Supplier's information security program.

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.

14.1.2 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.

14.2.2 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:

- 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
- otherwise required by a Client Regulator or a law enforcement body.
- 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 on a Time and Materials Basis.

15. EXPIRY AND TERMINATION

15.1 Upon cancellation, expiry or termination of the Agreement, the Supplier shall:

15.1.1 deliver up to the Client all Personal Data in its then current format; and
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. The obligations placed upon Supplier under this Policy shall survive so long as Supplier and/or its Subprocessors process Personal Data on behalf of Client.

Annex 1 – Details of Processing

A. List of Parties

Data exporter:

Name: The Customer, as defined in the Token Customer Terms of Service (on behalf of itself and Permitted Affiliates)

Address: The Customer's address, as set out in the Order Form

Contact person's name, position and contact details: The Customer's contact details, as set out in the Order Form and/or as set out in the Customer's Token Account

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Token Services under the Token Customer Terms of Service

Role (controller/processor): Controller

Data importer:

Name: Token.io Ltd.,
a company registered in England and Wales under number 10143662 (VAT number: GB 360 4047 27)

Correspondence Address: 70 St Mary Axe, 4th Floor, London EC3A 8BE, United Kingdom

Contact person's name, position and contact details:
Privasee Group Ltd, External DPO, Privacy@token.io

Activities relevant to the data transferred under these Clauses:
Processing of Personal Data in connection with Customer's use of the Token Services under the Token Customer Terms of Service

Role (controller/processor): Processor

B. Description of Transfer

Categories of Data Subjects whose Personal Data is Transferred

You may submit Personal Data in the course of using the Token Service, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Your Contacts and other end users including your employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to your end users.

Categories of Personal Data Transferred

You may submit Personal Data to the Token Services, the extent of which is determined and controlled by you in your sole discretion, and which may include but is not limited to the following categories of Personal Data:

1. Contact Information (as defined in the General Terms).
2. Any other Personal Data submitted by, sent to, or received by you, or your end users, via the Token Service.
3. Sensitive Data transferred and applied restrictions or safeguards
4. 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 parties do not anticipate the transfer of sensitive data.

Frequency of the transfer

Continuous

Nature of the Processing

Personal Data will be Processed in accordance with the Agreement (including the DPA) and may be subject to the following Processing activities:
1. Storage and other Processing necessary to provide, maintain and improve the Token Services provided to you; and/or
2. Disclosure in accordance with the Agreement (including the DPA) and/or as compelled by applicable laws.

Purpose of the transfer and further processing

We will Process Personal Data as necessary to provide the Token Services pursuant to the Agreement and as further instructed by you in your use of the Token Services.

Period for which Personal Data will be retained

Subject to the 'Expiry and Termination' section of this policy, we will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

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

- 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;"
- 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;"
- 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".
- 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."
- 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)".