PRIVACY PROTECTIONS AND CONFIDENTIALITY POLICY

1. Commitment to Privacy

Blockchain Triangle ("**BCT**" or the "**Company**") respects individuals' rights to privacy and the protection of Personal Information / Personal Data. The scope of this Privacy Protections and Confidentiality Policy (the "**Privacy Policy**" or "**Policy**") is to explain and elaborate on how the Company collects, uses, process and store Personal Information / Personal Data in the course of its business.

The Company is committed to protecting the confidentiality of all personal information/personal data in accordance with the Personal Information Protection Act 2016 of Bermuda (the "**PIPA**") when concerning employees and clients whose residency is in Bermuda, as well as with the EU General Data Protection Regulation 2016/679 (the "**GDPR**") when concerning employees and clients whose residency is within the European Economic Area ("**EEA**").

This Policy is issued pursuant to and reflects compliance with the requirements and/or obligations and/or duties introduced by the PIPA and GDPR, as amended and replaced from time to time (collectively referred to as the "**Privacy Protection Laws**"), in regards with any and all Personal Information /Personal Data ("**Personal Information**" or "**Personal Data**" or "**Information**" or "**Data**") processing activities carried out by the Company. Personal Information / Personal Data means any information relating to an identified or identifiable natural person. The term Personal Information / Personal Data shall include all personal information/personal data including sensitive personal information and special categories of personal data, as those terms are defined in the PIPA and GDPR respectively.

This Policy applies to all BCT employees as well as service providers acting on BCT's behalf to support customer due diligence activities (collectively "**Covered Persons**") that use/process any Personal Information / Personal Data provided by a current, former, or prospective client and employee of BCT.

This Policy covers the clients and employees based in Bermuda and EEA and does not cover all other clients and employees residing outside of Bermuda and EEA. Should the Company decide to expand its services to clients outside Bermuda and the EEA and to employ persons residing outside Bermuda and the EEA, separate policies shall be prepared to abide by the relevant privacy regulations of each jurisdiction.

2. Collection and Use of Client Personal Information / Personal Data

BCT will seek to limit its collection of Personal Information / Personal Data to information from Clients that is reasonably necessary for the purposes and based on the legal basis set out in the Client Privacy Notice. BCT will also use the Personal Information / Personal Data collected from Clients in accordance with the Client Privacy Notice and as permitted or required by law, or as authorized by the Client. BCT will never sell any Personal Information / Personal Data of its Clients.

For the purposes of this Policy, "**Client**" shall mean the natural and legal persons who are using or wish to use the services and/or products and/or platforms of the Company.

BCT will strive to: (a) ensure the security and confidentiality of the Personal Information / Personal Data; (b) protect against anticipated threats and hazards to the security and integrity of the Personal Information / Personal Data; and (c) protect against unauthorized access to or improper use of the Personal Information / Personal Data.

The Privacy Officer (for the purposes of PIPA, or Data Protection Officer ("DPO") for the purposes of GDPR, depending on the residency of the person whose Information / Data is used/processed) is responsible for administering this Privacy Policy as well as the Client Privacy Notice. BCT employees are required to promptly notify the Privacy Officer / DPO of any threats to, or improper disclosure of, Information/Data.

The Client Privacy Notice which is attached as Appendix 1 to and forms an integral part of this Policy contains all the information on the collection and use/processing of the Clients' Personal Information / Personal Data by the Company as well as the Clients' rights.

2.1. Dissemination of Privacy Notices

It is BCT's policy to provide initial and annual privacy notices to all Clients. In addition, should BCT materially change its privacy policies or procedures, the Privacy Officer / DPO and/or his/her specified designee will ensure that all Clients receive a notice informing them of such changes. A copy of BCT's current Client Privacy Notice is posted on the BCT website and is also attached to this Policy as Appendix 1.

2.2. Disclosure of Personal Information / Personal Data

Personal Information / Personal Data may only be provided to third parties in the cases set out in Section 14 of the Client Privacy Notice, which is attached to and forms an integral part of this Policy.

Any Information / Data may be disclosed only on the above cases and to the extent required.

Employees should take reasonable precautions to confirm the identity of individuals requesting Personal Information / Personal Data. Employees must be careful to avoid disclosures to identity thieves who may use certain Information / Data to convince an employee to divulge additional information. Any contacts with suspected identity thieves must be promptly reported to the CISO and Privacy Officer / DPO.

To the extent practicable, employees will seek to remove nonessential Information / Data from information disclosed to third parties. Government agency identification numbers must never be included in widely distributed lists or reports.

Information / Data may be reviewed by BCT's outside service providers, such as accountants, lawyers, consultants and, where relevant, Fund administrators (in case of clients that are funds). BCT will review such service providers' privacy policies to ensure that Information / Data is not used or distributed inappropriately.

2.3. Safeguarding Information/Data and Sensitive Personal Information/Special categories of personal data of Clients

Information/Data and Sensitive Personal Information/Special categories of personal data should only be discussed or shared with those Covered Persons who need to know such information in connection with the performance of their job responsibilities with BCT (please refer to the Company's Access Control Policy). Covered Persons must not share Information/Data or Sensitive Personal Information/Special categories of personal data with anyone outside of BCT (including with relatives, spouses or other social contacts) other than on a need to know basis in connection with the conduct of BCT's business activities and subject to any related confidentiality obligations that apply to BCT (including, without limitation, any confidentiality obligations contained in any non-disclosure or similar agreement entered into by BCT). This obligation also continues following a Covered Person's separation from BCT for any reason.

Covered Persons must take steps to avoid inadvertent disclosure of Information/Data and Sensitive Personal Information/Special categories of personal data. Voice communications involving Information/Data and Sensitive Personal Information/Special categories of personal data must be kept to a minimum and performed in closed or secured locations. Information/Data and Sensitive Personal Information/Special categories of personal data should not be discussed in elevators and discretion must be exercised before discussing such information in public places where it might be overheard. All outgoing documents should be addressed to the appropriate person and marked "confidential" as appropriate. Furthermore, all Covered Persons must take care not to disclose Information/Data and Sensitive Personal Information/Special categories of personal data to reporters, researchers or analysts who may contact BCT.

3. Collection and Use of Employee Personal Information

The Company is transparent on how information is used and provides clear information to the employees about the procedure of collection and the way in which personal information will be used, both upon and during their employment.

3.1. Personal Information

The Company will request and hold the following, but not limited to the following, Personal Information for its employees:

- full name and title;
- home address;
- contact details (such as telephone number and email address);
- date of birth;
- gender;
- marital status;
- in cases of administration of medical cover, the Company shall request the information as stated below (provided that the relevant consent by the employee has been obtained):
    - name/surname/date of birth
    - address
    - ID/passport number
    - bank details (account number, IBAN, bank name)
    - gender
    - telephone number

In such cases the consent of the relevant family members will be required in advance, otherwise their details will not be processed. The employee is provided with a consent form under which the employee has the option to either contact directly the insurance provider or provide permission to the Company to process the insurance application on his/her behalf**. No copies or scanned copies of blood tests, other medical examinations, any of the details stated above necessary for the application for medical cover or the application itself are kept by the Company**;

- next of kin information and emergency contact information (consent of the relevant family members/persons will be required in order for their details to be processed. In the case of children under the age of 14, consent should be given by someone with parental responsibility for them);
- copies of identification documents;
- Curriculum Vitae (CV) and information provided in the employee's CV;
- education history, training and professional experience (including diplomas, certificates and professional registrations);
- current and past employment details (commencement and end dates, positions held, contact details etc.);
- immigration status and work permits (if applicable). Relevant immigration forms include details such as names, Passport number, previous and existing addresses, family details as well as copy of the passport of the applicant, criminal records, academic qualifications (diplomas etc), bank guarantee, medical insurance, rental agreement, employment agreement, medical exams and x-rays;
- references from previous employers (if required);
- languages spoken and level of proficiency (relevant certificates if applicable);
- performance records and appraisals of your employment with the Company;
- warning letters, resignation letters, redundancy information, notes/letters in relation to exit interviews;
- annual leaves/holiday records/ sick leaves and doctor notices/ maternity & paternity leaves;
- disciplinary and grievance records;
- remuneration information (including payroll information), National Insurance number, bank account details, payroll records and tax ID and tax status information;
- Bankruptcy information;
- Information relating to civil or criminal convictions or any legal or disciplinary proceedings or investigations related to misconduct or malpractice;
- recording of employee telephone lines (in justified cases);
- travel information in case tickets are booked for the employee by the Company;
- In cases where the employee is not registered with Social Insurance the following information is requested in relation to the employee's registration:
    - name, ID and Passport number, Nationality, Bermudian status condition, place of birth, residential address, telephone, fax, date and place of birth, gender, marital status & date of marriage if applicable, occupation, date of commencement of employment, if applicable name of spouse, Social insurance number of spouse; if applicable work permit/immigration spousal letter; and signature of the employee (Applicant).

  No copies or scanned copies are kept by the Company.

The Company will collect and use Personal Information for the purposes of:

- fulfilling its obligations under the employee's employment contract and therefore be able to comply with its legal obligations;
- being able to operate its business;
- processing salary payments, providing insurance covers, processing pension payments, adhering to Social insurance and tax obligations and other salary deductions;
- performance and appraisal procedures that help monitor the performance of the employees;
- compliance with its legal and regulatory obligations set by its regulator (the Bermuda Monetary Authority, "**BMA**") as well as for reasons related to the health and safety of its employees.

3.2. Sensitive Personal Information

The Company will usually also hold the following sensitive personal information:

- Racial or ethnic origin;
- data concerning information about an employee's physical or mental health (including any medical conditions, health and sickness records, details of sick leaves or where you end your employment due to health reasons);
- information about criminal convictions and offences.

The Company will use Sensitive Personal Information for the purposes of:

- carrying out the obligations in relation to the Company's employee's employment rights such as, monitoring equality of opportunity, assess suitability for particular jobs, to promote the health and safety of the employees (especially in cases where the Company will have to make adjustments to accommodate an Employee with a temporary or permanent disability), to make any necessary adjustments to accommodate an employee with a disability for his/her health and safety in the work environment, monitor sickness absence in relation to the administration/provision of benefits (maternity pay, sick pay, pensions and health insurance);
- to communicate with the insurance providers (with the employee's consent);
- to enable monitoring of sick leave, assessing an employee's working capacity for occupational health purposes;
- to defend or bring legal claims;
- for security purposes.

3.3. Collection of Personal Information

The Company collects employee Personal Information in the following manners:

- Directly from the employee;
- By third parties, i.e. recruitment agencies.

3.4. Legal Basis for collection and use of Personal Information

The legal basis for the collection and use of the employees' Personal Information is:

(a) Necessary for the performance of the employee's employment contract, i.e. in order for the Company to fulfil its obligations towards the employee under the terms of his/her employment contract, such as, payment of his/her salary, compliance with Employment and Social Insurance legislation.

(b) To comply with legal and regulatory obligations to which the Company is subject, i.e. Digital Asset Business Act 2018 ("**DABA**"), Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008, and Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008.

The Company will only use the employees' Personal Information for the purposes for which the Company collects it (as stated above), unless the Company needs to use it for another reason compatible with the original purpose and in such a case the employee will be informed in advance. In the event that the Company needs or is required to use the employee's Personal Information for another purpose the Company will notify the employee in advance and inform him/her accordingly of the legal basis to do so.

3.5. Disclosure of Personal Information to Third Parties

The Company may share the employee's information with:

- Insurance Providers;
- Governmental and regulatory authorities such as the BMA, the Ministry of Labour, Community Affairs and Sports, Department of Social Insurance, Office of the Tax Commissioner and other relevant governmental departments/agencies;
- Software provider(s) who can have access to employees' information stored electronically.

The Company may also disclose the employees' information to third parties for the following reasons:

- in the event of a sale or purchase of any business or assets, to the prospective seller or buyer of such business or assets;
- in the event that all or substantially all of the Company's assets are acquired by a third party, in which case personal information will be one of the transferred assets;
- a reference by a third party either during, or following the end of, an employee's employment. In such a case the Company will contact such employee and ask for his/her consent.

The Company shall ensure that the employees' information is safe and shall take all reasonable steps necessary to ensure that their information is treated securely and in accordance with this Policy and applicable law. Details regarding these safeguards in each case can be obtained from the Privacy Officer.

We will not sell an employee's personal information or disclose it to any third parties without he employee's consent.

3.6. Maintaining accurate information

In order for the Company to be able to comply with its obligations and maintain an accurate record of the employees' personal information, the employees should immediately notify in writing the Company or the Privacy Officer (at the contact details stated below) of any changes to their personal details such as, but not limited to:

- name, address, contact details
- marital status and next of kin status
- change in criminal record
- involvement in litigation
- bankruptcy, application for bankruptcy against the employee, receiving order against the employee
- disciplinary action taken against the employee by any regulatory/professional body
- nationality or immigration status
- changes in his/her insurance coverage

Where the employee has notified the Company or the Privacy Officer of any inaccuracies or changes in his/her information, the Company will immediately update his/her information.

The contact details of the Privacy Officer are stated below:

Name: John Tartaglia
Telephone number: (441) 505-5538
Email Address: dpo@blockchaintriangle.io
Office Address: 52 Reid Street, Hamilton HM 12, Bermuda

3.7. Policies and Procedures

This Policy, or any subsequent version, shall be communicated to each employee upon employment.

Any new or updated policies or procedures will be communicated to the employees, during their employment, as soon as practicable by appropriate means.

3.8. Security of Employees' Personal Information

3.8.1. Security of employees' Personal Information is a priority for the Company and the Company is committed to ensuring that employees' information is kept secure. The Company has in place appropriate security measures and procedures to prevent any accidental loss, destruction, unauthorised use or access, alteration or disclosure of employees' Personal Information. Employees' Personal Information is kept on the Company's servers in scanned copies and certain data are kept in hard copies in cabinets that require a key for access. The data is accessed by authorised personnel only and such access is carried out according to the Company's instructions and this Policy; the authorised personnel is subject to a duty of confidentiality.

3.8.2. In case an employee has provided data electronically the Company makes sure that such information is stored on the Company's servers. With reference to transmission of information via the internet, the Company uses strict procedures and security features to try and prevent the possibility of unauthorised access.

3.8.3. Where an employee has a password which enables him/her to access the Company's IT system, he/she is responsible for keeping this password confidential and he/she should not share his/her passwords with anyone.

3.8.4. The Company has in place procedures in relation to security breaches and it will notify the employee and the supervisory authority of a suspected or actual breach where the Company is legally required to do so as soon as possible.

3.8.5. In the event of a technical or physical incident the Company has in place procedures to restore the availability and access to data. The Company regularly tests and evaluates the technical and organisational measures it has in place in order to ensure the security of its data.

3.9. How long the Company keeps Employees' Personal Information

The Company will keep the employee's information as long as necessary to fulfil the purposes as stated in this Policy or in the terms of his/her employment contract, or as required by law for compliance with any legal, regulatory or reporting requirement. The Company will keep an employee's information for up to 6 years from the date of termination of his/her employment with the Company and will anonymise his/her personal information to ensure that the information cannot be associated with that particular employee.

Once the employee's personal information is no longer necessary, it will be deleted without undue delay.

3.10. Employees' Rights

3.10.1. **Right of Access**: Employees have the right to receive confirmation that their information is being used, they also have the right to access their personal information. The Company in case the employee requests access shall provide information such as the purpose, categories of personal information, copy of the personal information being used. In case the Company processes a large quantity of information in relation to an employee, it can request from the employee to specify the information or processing activity to which the request relates. Where possible, the Company may provide remote access to a secure system through which the employees will have direct access to their information.

3.10.2. **Right to rectification**: Employees have the right to request to correct their personal information if the information is inaccurate or incomplete. Information will be corrected without undue delay.

3.10.3. **Right to erasure**: Employees may request the deletion or removal of their personal information for certain reasons when there is no compelling reason to continue using the information (for instance in cases where the personal information is no longer necessary in relation to the purposes for which it was collected or the employee had objected to the use and there is no overriding ground for retention, or the information has been processed unlawfully. Information is deleted without undue delay.

The right of an employee to require the deletion of his/her personal information does not apply to the extent that retention is necessary:

- for compliance with a legal obligation that requires processing by the Company; or
- for the performance of their employment contract; or
- for the performance of a task carried out in the public interest; or
- for the establishment, exercise or defence of legal claims.

3.10.4. **Right to limitation of use**: The employee has the right to limit the use of his/her Personal Information under certain circumstances.

3.10.5. **Right to blocking**: The employees/candidates have the right to request the Company to cease, or not to begin, using their Personal Information where the use of that Personal Information is causing or is likely to cause substantial damage or substantial distress to them or to another individual.

3.11. Employee Requests – Company Obligations

In accordance with the employee's rights as stated above the Company shall:

- Respond to the employee, and provide the information requested by the employee, if requested, without undue delay and within 45 days of receipt of the request. The period may be extended by no more than 30 days, or for such longer period as the Privacy Commissioner of Bermuda may permit, depending on the complexity of the request as well as the number of requests. In such a case, the Company shall inform the employee of the extension as well as the reasons for delay and the time when a response from the Company can be expected the soonest possible but not later than the expiration of the 45 days of receipt of the request.
- Verify the identity of the employee. In the event the Company is not certain of the identity of the individual, additional information may be requested in order to confirm his/her identity.
- Not provide other information other than the information in relation to the requesting party.
- Provide the information free of charge.
- Where an employee request is manifestly unfounded or excessive, in particular because of its repetitive character, the Company may charge a reasonable fee taking into account administrative costs or refuse to act on the request. If this is the case the Company shall bear the burden of proving that the request was manifestly unfounded or excessive. Records are kept in relation to all requests.
- If no action is taken by the Company on a request of an employee, the Company shall inform the employee in writing of the reasons for the refusal and of his/her right to contact the Privacy Commissioner of Bermuda to make a complaint, at the latest within 45 days of receipt of the request.

3.12. Employee Obligations

The employees are obliged to treat all information that come to their knowledge during their employment, including Clients' personal information / personal data, as confidential and retain the confidential information in strict confidence in accordance with the policies of the Company, including this Policy, and to protect the security, integrity and confidentiality of such information. In this respect, the employees shall sign a Confidentiality Agreement along with their employment contract, upon their employment.

3.13. Complaints

If an employee is not satisfied with how the Company processes his/her Personal Information, he/she has the right to file a complaint to the Privacy Commissioner of Bermuda at the contact details in the Commissioner's website at: https://www.gov.bm/privacy.

3.14. Amendments to the Policy

This Policy may be amended from time to time by the Company at its sole and absolute discretion. Any changes which may be made to this Policy will be notified to the employees as soon as practicable by appropriate means.

4. Security Safeguards

The Company has put in place appropriate safeguards to protect Personal Information / Personal Data that it holds, including risks of (a) loss; (b) unauthorised access, destruction, use, modification or disclosure; or (c) any other misuse.

4.1. Requests from Outside Parties for BCT Regulatory Information

All requests by third parties to review any section of the policies of the Company, including this Policy, compliance testing results, correspondence between BCT and regulators and other compliance-related documents should be forwarded to the Privacy Officer / DPO. Covered Persons are not authorized to respond to such requests without the prior approval of the Privacy Officer / DPO.

4.2. Information Stored in Hard Copy Formats

BCT has implemented various policies and procedures to protect Information/Data and Sensitive Personal Information/Special categories of personal data stored in hard copy format systems. Further details on these policies and procedures are contained within the Access Control Policy.

4.3. Electronic Information Systems

BCT has implemented various policies and procedures to protect Information/Data and Sensitive Personal Information/Special categories of personal data stored on electronic systems. Further details on these policies and procedures are contained within the Access Control Policy.

4.4. Complaints and Security Breaches

Covered Persons must promptly inform the Privacy Officer / DPO of:

- Any complaints from a Client regarding their Personal Information / Personal Data; or
- Any suspected or actual identity theft involving a Client; or
- Any breach of security; or
- Any suspected or actual disclosure of Information/Data and Sensitive Personal Information/Special categories of personal data in violation of this Policy.

In case of a breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to personal information, which is likely to adversely affect an individual, the Company shall, without undue delay:

a. notify the Privacy Commissioner of Bermuda, if concerning a Bermuda client or employee, or the relevant EEA Commissioner, if concerning an EEA client, of the breach;
b. then notify any individual affected by the breach; and
c. notify the BMA of the breach.

The notification to the Privacy Commissioner of Bermuda / relevant EEA Commissioner / BMA shall describe:

a. the nature of the breach;
b. its likely consequences for that individual; and
c. the measures taken and to be taken by the organisation to address the breach,

so that the Privacy Commissioner of Bermuda / relevant EEA Commissioner /BMA can determine whether to order the Company to take further steps.

APPENDIX 1

CLIENT PRIVACY NOTICE

1. Introduction

As part of our business operations, we need to collect personal information/personal data from our clients and prospective clients in order to provide them with our products and services and ensure that we can meet their needs when providing these products and services, as well as when providing them with the respective information. Your privacy is of utmost importance to us and it is our policy to safeguard and respect the confidentiality of information and the privacy of individuals.

This Privacy Notice, as amended or otherwise changed from time to time (the "**Privacy Notice**" or "**Notice**") sets out the manner in which Blockchain Triangle (the "**Company**", "**BCT**", "**we**", "**us**", "**our**") collects, uses and manages your personal information we receive by you or a third party in connection with our provision of services and products to you or which we collect from your use of our services and products and/or our website http://www.bctriangle.com/ website (the "**Website**"). This Privacy Notice also informs you of your rights with respect to the using / processing of your personal information/personal data.

2. Scope and Objective of the Privacy Notice

The Company is committed to protecting the confidentiality of all personal information/personal data in accordance with the Personal Information Protection Act 2016 of Bermuda (the "**PIPA**") when concerning clients whose residency is in Bermuda, as well as with the EU General Data Protection Regulation 2016/679 ("**GDPR**") when concerning clients whose residency is within the European Economic Area ("**EEA**").

This Notice is issued pursuant to and reflects compliance with the requirements and/or obligations and/or duties introduced by the PIPA and GDPR, as amended and replaced from time to time (collectively referred to as the "**Privacy Protection Laws**"), in regards with any and all Personal Information or Personal Data ("**Personal Information**" or "**Personal Data**" or "**Information**" or "**Data**") using/processing activities carried out by the Company. Personal Information / Personal Data means any information relating to an identified or identifiable natural person. The term Personal Information / Personal Data shall include all personal information/personal data including sensitive personal information and special categories of personal data, as those terms are defined in the PIPA and GDPR respectively.

This Privacy Notice applies to all clients of BCT receiving its services and products and using BCT's platforms (the "**Clients**"). If your country of residence, as determined by your verified residential address, is (i) within Bermuda, you will be referred to in this Notice as "**Bermuda Client**"; or (ii) within the European Economic Area ("**EEA**"), you will be referred to in this Notice as an "**EEA Client**".

The Company collects, uses and process various categories of information/data at the start of, and for the duration of, its business relationship with the Clients. The Company will limit the collection and use/processing of information/data to the necessary information to meet the purpose and legal basis as described in Section 9 of this Privacy Notice.

3. Safeguarding the confidentiality of your Personal Information / Personal Data and protecting your privacy

The Company respects the privacy of any existing or prospective clients who use its services and products, and it is therefore committed to taking all reasonable steps to safeguard this.

The Company keeps any clients'/potential clients' Personal Information / Personal Data in accordance with the Privacy Protection Laws and applicable regulations.

We have put in place appropriate safeguards to protect Personal Information / Personal Data that we hold, including risks of (a) loss; (b) unauthorised access, destruction, use, modification or disclosure; or (c) any other misuse.

We have the necessary and appropriate technical and organisational measures and procedures in place to ensure that your information remains secure at all times. We regularly train and raise awareness to all of our employees on the importance of maintaining, safeguarding and respecting your personal information and privacy. We consider breaches of individuals' privacy very seriously and will impose appropriate disciplinary measures, including dismissal where necessary. We have also appointed a Privacy Officer / Data Protection Officer to ensure that our Company uses/processes your personal information in compliance with the Privacy Protection Laws and applicable regulations and in accordance with this Privacy Notice.

Transmission of information via the internet is not always completely secure but the Company endeavors to protect your personal information/data by taking serious precautions. Once we have received your information/data, we will apply procedures and security features to try to prevent unauthorised access.

4. EEA Clients

The following applies to EEA Clients only

For the purposes of the GDPR, BCT is the data controller of your Personal Data. We have appointed the following entity as our local representative in the EEA:

Local representative: Helena Wahlund
Postal Address: Gunnesbovägen 167, Lund 22654, Sweden
Contact: wahlund.helena@gmail.com

5. Personal Information we collect about you

We collect and use/process various categories of Personal Information / Personal Data at the start of, and for the duration of, your business relationship with us. The Company will limit the collection and processing of Personal Information / Personal Data to the necessary Information / Data to meet the purpose and legal basis as described in Section 9 of this Privacy Notice.

The information that the Company may collect from you includes:

- Basic Information / Data, including but not limited to full name, residential address, date of birth, contact details (e.g. email address, telephone number, etc.), place of birth, gender, citizenship, marital status, family and next of kin information, and contact details of such persons;
- Financial status information including but not limited to information about your income and wealth, including details about source of funds, assets and liabilities, bank account information, FATCA and CRS information and financial statements;
- Purpose and reason of your registration with us, your inquiries and our responses when registering and using our services and products;
- Education information including but not limited to field of study and level of study;
- Information on whether you hold a prominent public function (PEPs);
- Profession and employment details;
- Authentication data (e.g. signature);
- Verification information (including visual images), which includes information necessary to verify your identity such as a passport or ID or driver's license (examples also include background information we receive about you from public records or from other entities not affiliated with us); furthermore, we may collect other identifiable information such as identification numbers and/or Passport/Tax registration numbers;
- Online profile and social media information and activity based on your interaction with us, our websites and applications including but not limited to account profile, login information, Internet Protocol (IP) address, smart device information, location coordinates, mobile phone network information, searches and site visits;
- Bank account details including but not limited to IBAN number, SWIFT code, account number and Sort Code (where applicable);
- Any other similar information.

The Company may also process certain Sensitive Personal Information (for Bermuda Clients) and special categories of Personal Data (for EEA Clients) for specific and limited purposes and only on the basis of an explicit consent granted by you or on any other legal basis, as described in Section 9 of this Privacy Notice.

Please see Sections 6 and 7 for the information collected as Sensitive Personal Information and special categories of Personal Data.

When you open an account with us, a unique account number will be issued as well as a User ID and password. Only certain employees of the Company shall have access to your account number and User ID. However, please note that you are fully responsible for the secrecy of your account number, User ID and password. As a result, if you disclose your account number, User ID and/or password by any means, to any person, you shall be considered as fully responsible for such action and the Company shall not be liable for any consequences of such disclosure.

Information about criminal convictions or offences

Subject to the Privacy Protection Laws, the Company may process Personal Information / Personal Data about criminal convictions or offences and/or alleged offences for specific and limited activities and purposes including but not limited to perform checks to prevent and detect any unlawful or fraudulent

acts and comply with the relevant laws relating to anti-money laundering and terrorist financing, fraud, bribery, corruption and international sanctions. It may involve investigating and gathering intelligence on suspected financial crimes, fraud and threats and sharing Information/Data between credit or financial organisations, the Bermuda Monetary Authority ("**BMA**") and other competent or other authorities, including non-governmental authorities in any jurisdiction within or outside Bermuda or the EEA.

If you fail to provide Personal Information / Personal Data
Where we need to collect Personal Information / Personal Data by law, or under the terms of our business relationship (e.g. contract we have with you) and you fail to provide that information/data when requested, we may not be able to perform the contract we have, or are trying to enter into, with you. In this case, we may have to close your account and cease the provision of our services and products. We will notify you if this is the case at the time.

6. Sensitive Personal Information

This Section 6 applies to Bermuda Clients only

We may collect and use the following sensitive personal information only with your explicit consent and only for the purposes of the provision of services to you:

- Place of origin
- National origin
- Marital Status

In addition, the Company may use Sensitive Personal Information for the purpose of any criminal or civil proceedings.

In any case, we shall not use your sensitive personal information that may be collected from you to discriminate against you contrary to any provision of Part II of the Human Rights Act 1981.

7. Special Category of Data

This Section 7 applies to EEA Clients only

The Company may also process certain special categories of Personal Data for specific and limited purposes and only on the basis of an explicit consent granted by you or on any other legal basis, as described in Section 9 of this Privacy Notice.

These special categories of Personal Data include:

1. Physical or psychological health details or medical conditions;
2. Information about racial or ethnic origin;
3. Religious or philosophical beliefs;
4. Biometric information, relating to the physical, physiological or behavioural characteristics of a person, including but not limited to using voice recognition or similar technologies whatsoever to prevent fraud and/or money laundering activities.

The Data that may be collected, used, processed and stored under this category are the following: Biometric information including facial recognition technology to prevent fraud and/or money laundering activities.

Information about criminal convictions and offences.

Subject to the GDPR, the Company may process Personal Data about criminal convictions or offences and/or alleged offences for specific and limited activities and purposes including but not limited to perform checks to prevent and detect crime and comply with the law relating to anti-money laundering and terrorist financing, fraud, bribery, corruption and international sanctions. It may involve investigating and gathering intelligence on suspected financial crimes, fraud and threats and sharing Data between credit or financial organisations, the supervisory or other competent or other authorities including non-governmental authorities in any jurisdiction within or outside the EEA.

8. How we collect your Personal Information / Personal Data

We obtain your Personal Information / Personal Data in a number of ways:

a. From you, through your use of our services and products including through our website(s), apps, application forms, etc.;
b. From third parties – including third parties who provide services to you or us including but not limited to Identity Minds, Fundamental Interactions, Vouched, established or located within and/or outside Bermuda and the EEA;
c. Credit reference and fraud prevention agencies, banks or other financial institutions, authentication service providers and providers of public registers;
d. During our business relationship with you and the way you operate your account/s;
e. From the technology that you use to access our services including location data from your mobile phone, or an IP address or telephone number and how you use it;
f. From publicly available sources including the press, company registers and online search engines.

We may ask for other personal information/data voluntarily from time to time (for example, through market research or surveys).

If you choose not to provide the information/data which we need to fulfil your request for a specific product or service, we may not be able to provide you with the requested product or service.

It is your duty and responsibility to provide us with updates as to the Personal Information / Personal Data provided in order for such Information / Data to remain current, accurate and correct and you acknowledge that we rely on the Personal Information / Personal Data provided to us in carrying out our obligations, under the law and our business relationship with you.

Where you are a non-physical person providing to us Personal Information / Personal Data of any individual or where you are an individual providing us with Personal Information / Personal Data of any individual other than yourself, you hereby undertake and represent that such individual, whose Personal Information / Personal Data is collected, used/processed and stored in accordance with this Privacy Notice, has been fully informed of and clearly consented in writing to such collection, use, processing and store of his/her Personal Information / Personal Data under this Privacy Notice and that he/she has

been informed of his/her rights in relation to the Personal Information / Personal Data which is collected, used/processed and stored, in accordance with this Privacy Notice.

9. Purpose and Conditions / Legal Basis of collection and using/processing of your Personal Information / Personal Data

9.1. Purpose

We will only collect your Personal Information / Personal Data where it is necessary for us to carry out our lawful business activities and provide our services and/or products.

9.2. Legal Basis

We may use/process your Personal Information / Personal Data on the following bases and for the following purposes:

1. **Performance of a contract**

   We use/process Personal Information / Personal Data in order to provide our services and products, as well as information regarding our products and services based on the contractual relationship with our clients (i.e. so as to perform our contractual obligations). In addition, processing of personal information / personal data takes place to be able to complete our client acceptance procedures.

   In view of the above, we need to verify your identity in order to accept you as our client and we will need to use those details in order to effectively manage your business relationship with us to ensure that you are getting the best possible service from us. This may include third parties carrying out credit or identity checks on our behalf. The use of your personal information is necessary for us to know who you are as we have a legal obligation to comply with certain 'Know Your Customer' and 'Customer Due Diligence' regulatory obligations.

2. **Compliance with a legal and regulatory obligation**

   There are a number of legal obligations emanating from the relevant laws to which we are subject as well as statutory requirements and laws and regulations of various supervisory authorities we are subject to. Such obligations and requirements impose on us necessary personal information/data using/processing activities for credit checks, identity verification, compliance with court orders, tax law or other reporting obligations and anti-money laundering controls, for the prevention, detection or investigation of crimes.

3. **Publicly available information**

We may use/process personal information /personal data that is publicly available information. Such information / data will be used only for a purpose that is consistent with the purpose of its public availability.

4. **You have provided your consent**

For sensitive personal information, special category of data as well as for research, statistical or marketing purposes, we may collect, use/process, and store Personal Information / Personal Data where an explicit consent has been granted.

In addition to the above, and with respect to *Bermuda Clients only,* Personal Information may be collected, used and stored, with your explicit consent pursuant to the Company's Terms of Use Policy and without prejudicing your interests or fundamental rights and freedoms, for the following purposes:

- initiating legal claims and preparing our defence in litigation procedures;
- to investigate issues and/or settle disputes with you in a timely and efficient manner;
- to ensure network and information security, including but not limited to monitoring authorised users' access to our information technology for the purpose of preventing cyber-attacks, unauthorised use of our telecommunications, other systems and websites, prevention or detection of crime and protection of your Personal Information;
- measures to manage business and for further developing products and services;
- to help us improve our products and services, including customer services, and develop and market new products and services
  We may from time to time use personal information provided by you through your use of the services and/or through client surveys to help us improve our products and services. In this way, we ensure the highest standards when providing you with our products and services and we continue to be a market leader in the financial services industry.
- updating/verifying your personal information in accordance with the relevant anti-money laundering compliance framework;
- to monitor, maintain and improve internal business processes, information and data, technology and communications solutions and services;
- to ensure business continuity and disaster recovery responding to information technology and business emergencies;
- to provide assurance on the management of the Company's material risks;
- to perform general, financial and regulatory accounting and reporting;
- to protect our legal rights and interests;
- to send you surveys as part of our customer feedback process in order to ensure that we provide our services/products at the highest standards;
- to send you marketing communications by email or phone or other agreed forms to ensure that you are always kept up to date with our latest products and services;
- for internal business and research purposes as well as for record keeping purposes, that may include any communications that we have with you in relation to the services and products we provide to you and our relationship with you.

5. **For the purposes of safeguarding legitimate interests**

This Section 5 applies to EEA Clients only.

We may collect, process, use and store your Personal Data so as to safeguard the legitimate interests pursued by us or by a third party and without prejudicing your interests or fundamental rights and freedoms. A legitimate interest is when we have a business or commercial reason to use your information. Examples of such processing activities include:

- initiating legal claims and preparing our defence in litigation procedures;
- to investigate issues and/or settle disputes with you in a timely and efficient manner;
- en sure network and information security, including but not limited to monitoring authorised users' access to our information technology for the purpose of preventing cyber-attacks, unauthorised use of our telecommunications, other systems and websites, prevention or detection of crime and protection of your Personal Data;
- measures to manage business and for further developing products and services;
- to help us improve our products and services, including customer services, and develop and market new products and services;

We may from time to time use personal data provided by you through your use of the services and/or through client surveys to help us improve our products and services. It is in our legitimate interests to use your personal information in this way to ensure the highest standards when providing you with our products and services and to continue to be a market leader in the financial services industry;

- updating/verifying your personal data in accordance with the relevant anti-money laundering compliance framework;
- to monitor, maintain and improve internal business processes, information and data, technology and communications solutions and services;
- ensure business continuity and disaster recovery responding to information technology and business emergencies;
- provide assurance on the management of the Company's material risks;
- perform general, financial and regulatory accounting and reporting;
- protect our legal rights and interests;
- to send you surveys as part of our customer feedback process in order to ensure that we provide our services/products at the highest standards;
- to send you marketing communications by email or phone or other agreed forms to ensure that you are always kept up to date with our latest products and services;
- for internal business and research purposes as well as for record keeping purposes, that may include any communications that we have with you in relation to the services and products we provide to you and our relationship with you.

10. How we use your Personal Information / Personal Data

We shall use your Personal Information / Personal Data only for the specific purposes for which this is collected under Section 9 or for purposes that are related to those specific purposes.

11. How we share your Personal Information / Personal Data

We will not share your Personal Information / Personal Data to a third party, except:

- where necessary to disclose your information / data to law enforcement agencies, regulators, government/public officials, or other relevant third parties in the course of

our business and for the provision of our services and products to you, i.e. the BMA, the Registrar of Companies of Bermuda, etc, depending on the services and products provided to you;

- where we have your explicit consent;
- where necessary to disclose your information / data to law enforcement agencies, regulators, government/public officials, or other relevant third parties to comply with any law, subpoenas, court orders, or government request, defend against claims, investigate or bring legal action against illegal or suspected illegal activities, enforce our terms, or to protect the rights, safety, and security of the Company, our users, or the public.
- to third party service providers (such as Identity Minds, Fundamental Interactions, and Vouched) to provide you with the services and products that we offer you through our Website; to conduct quality assurance testing; to provide technical support; to verify your identity. Provided that such third-party service providers shall be informed about the confidentiality nature of such Information / Data and commit to not use your Personal Information / Personal Data other than to provide the services requested by us;
- to the Company's professional advisors provided that in each case the relevant professional shall be informed about the confidential nature of such Information / Data and commit to the confidentiality obligations herein as well;
- to third parties (e.g. the purchaser or new owner) in connection with or during negotiation of any merger, financing, acquisition or dissolution transaction or proceeding involving sale, transfer, divestiture, or disclosure of all or a portion of our business or assets. In the event of an insolvency, bankruptcy, or receivership, Personal Information / Personal Data may also be transferred as a business asset. If another company acquires our company, business, or assets, that company will possess the Personal Information / Personal Data collected by us and will assume the rights and obligations regarding your Personal Information / Personal Data as described in this Privacy Notice.

We may provide links to third-party websites which are regulated by their own privacy policies. We are not responsible for the privacy policies of these third-party websites even if they were accessed using the links from our website.

Other than as stated in this Privacy Statement, we do not disclose any of your personal information / personal data to third parties unless required to do so by law enforcement, court order, or in compliance with legal reporting obligations.

12. Storage of your Personal Information / Personal Data and retention period

We will hold your Personal Information / Personal Data, for as long as we have a business relationship with you, in a combination of secure computer storage facilities and paper-based files and other records and we take the necessary measures to protect the personal information we hold from misuse, loss, unauthorised access, modification or disclosure.

When we consider that Personal Information / Personal Data is no longer necessary for the purpose for which it was collected, we will remove any details that will identify you or we will securely destroy the records. However, we may need to maintain records for a significant period of time if a legal or

regulatory provision provides for such an obligation. For example, we are subject to certain anti-money laundering laws which require us to retain the following:

- a copy of the documents we used in order to comply with our customer due diligence obligations;
- records of the services and products used during your relationship with us.

Where you have opted out of receiving marketing communications, we will hold your details on our suppression list so that we know you do not want to receive these communications.
We may keep your data for longer than 6 years if we cannot delete it for legal, regulatory or technical reasons.

13. Children's Personal Information / Personal Data

We do not generally accept Children as our clients and do not collect, use/process and store Information / Data of Children. However, we may collect Information / Data of children only when our services concern trusts that have children as their beneficiaries.

In such cases, the Information / Data collected include:

- Full name;
- Date of Birth;
- Verification information (including visual images), which includes information necessary to verify their identity such as a passport or id (examples also include background information we receive about them from public records or from other entities not affiliated with us); furthermore, we may collect other identifiable information such as identification numbers and/or Passport numbers.

The Company shall obtain, use/process and store Personal Information / Personal Data of Children only if the consent by the holder of parental responsibility over the child is given or authorised.

For the purposes of this Notice, "child" means an individual under the age of 14 for the purposes of PIPA and an individual under the age of 16 for the purposes of GDPR.

14. Transfers Outside of Bermuda and the EEA

We may transfer your personal information outside Bermuda (in case of Bermuda Clients) and the European Economic Area (in case of EEA Clients) to our service providers and affiliates as part of our service delivery to you and where needed in compliance with any regulatory requirement. To the extent we transfer your information/data outside Bermuda/the EEA, we will ensure that the transfer is lawful and that the overseas third-parties / parties in third countries are obligated to comply with PIPA / GDPR (as the case may be) standards and to provide appropriate safeguards in relation to the transfer of your data in accordance with PIPA / GDPR.

The below applies to Bermuda clients only.

Your Personal Information may be used by staff operating outside of Bermuda who work for us or for one of our service providers. Such staff may be, among others, engaged in the fulfilment of your requests, the processing of your payment details and the provision of support services. By submitting your personal information, you agree to this transfer and use. The Company will take all steps reasonably necessary to ensure that your information is treated securely and in accordance with this Privacy Notice.

The below applies to EEA clients only.

If you are an EEA client, whenever we transfer your Personal Data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your Personal Data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.
- We may use specific contracts approved by the European Commission which give Personal Data the same protection it has in Europe.
- In respect of transfers to entities in the US, we may transfer Personal Data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between Europe and the US.

In view of the above, your Personal Data may be processed by staff operating in Bermuda who work for us or for one of our processors. Such staff may be, among others, engaged in the fulfilment of your requests, the processing of your payment details and the provision of support services. By submitting your personal data, you agree to this transfer, storing and processing. The Company will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Notice.

15. Your legal rights

Under certain circumstances, you have rights under the Privacy Protection Laws in relation to your Personal Information / Personal Data:

Request access	You have the right to get access to the Personal Information / Personal Data, including the records of any and all telephone conversations, email and/or text message correspondence, between you and the Company, held by the Company for you. **Please note:** If you require additional copies, we may need to charge a reasonable administration fee.
Request rectification	You have a right to rectification of inaccurate Personal Information / Personal Data and to update incomplete Personal Information/ Personal Data. In case you believe that any of the Personal Information / Personal Data held by the Company is inaccurate, you are entitled to request correction of that Personal Information / Personal Data and rectify the inaccuracies.

	If you need to add or change any information, you can do so by logging in to your account profile and directly amending entries. Such amendments may be subject to review.
Request erasure	You have a right to request to delete your Personal Information/ Personal Data. You may request to delete your Personal Information/ Personal Data in case you believe that: ● the Company no longer needs to process your Personal Information/ Personal Data for the purposes for which it was provided; ● the Company requested your consent to process your Personal Information/ Personal Data but you withdraw your consent; ● the Company is not using your Personal Information/ Personal Data in a lawful manner. **Please note:** If you request us to delete your Personal Information/ Personal Data we may have to suspend the services and/or products provided to you. **Please note:** Your right of deletion would not apply for various reasons including if we need to retain your Personal Information/ Personal Data in order to comply with a legal obligation or to establish or defend a legal claim. Where we are unable to comply with your request of deletion, we will notify you at the time of your request also informing you of the reason we cannot comply with your deletion request.
Request limitation of use/restriction of processing	You have a right to request us to restrict the processing of your Personal Information/ Personal Data. You may request us to restrict processing your Personal Information/ Personal Data in case you believe that:

	● any of your Personal Information/ Personal Data held by the Company is inaccurate; ● the Company no longer needs to process your Personal Information/ Personal Data for the purposes for which it was provided, but you require such Information / Data to establish, exercise or defend legal proceedings; ● the Company is not using your Information / Data in a lawful manner; ● you have objected to our use of your information / data but we need to verify whether we have overriding legitimate grounds to use it. **Please note:** If you request us to restrict processing your Personal Information/ Personal Data we may have to suspend the services, accounts, and/or products provided to you. In the event of account suspension, your use of the Company's services may be affected.
Portability Right **This right applies to EEA clients only.*	If you ask us, we will provide you or a third party you have chosen, your Personal Information / Personal Data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you. **Please note:** In case you request us to provide your Personal Information / Personal Data to a third party, the Company shall not be responsible for any such third parties' use of your Personal Data, which will be governed by their agreement with you and any privacy statement they provide to you.
Blocking **This right applies to Bermuda clients only.*	You may request us to cease, or not to begin, using your Personal Information where the use of that Personal Information is causing or is likely to cause substantial damage or substantial distress to you or to another individual.

Object to Processing **This right applies to EEA clients only.*	You have the right to object to the processing of your Personal Data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your interests and fundamental rights and freedoms. You also have the right to object where we are processing your Personal Data for direct marketing purposes. In some cases, we may demonstrate compelling and legitimate grounds for the processing, which may override your own interests, rights and freedoms, or where we need to process your Personal Data to investigate and protect us or others from legal proceedings.
Marketing	You have a right to object at any time to collect, use, process or store your Personal Information / Personal Data for direct marketing purposes, including profiling you for the purposes of direct marketing.
Withdraw consent	In case in which the Company relies on your permission to process your Personal Information / Personal Data, you have a right to withdraw your consent at any time by sending a written request to us. **Please note:** If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.
Raise a complaint	If you wish to make a complaint, you can contact our Privacy Officer / DPO who will investigate the matter. You may also raise a complaint directly to the supervisory authority for data protection issues: ● If you are based in Bermuda, you have the right to make a complaint at any time to the Privacy Commissioner (the "**Bermuda Commissioner**"), the

	Bermuda supervisory authority for data protection issues (https://www.gov.bm/privacy). ● If you are based in EEA, you have the right to make a complaint at any time to The Swedish Data Protection Authority (Datainspektionen) , the Swedish supervisory authority for data protection issues (https://www.datainspektionen.se/other-lang/in-english/). We would, however, appreciate the chance to deal with your concerns before you approach the relevant supervisory authority, so please contact us in the first instance.

If you wish to exercise any of the rights set out above, please contact our Privacy Officer / DPO.

16. Changes to this Privacy Notice

We may change this Notice from time to time to reflect changes in law, our Personal Information / Personal Data collection and use/processing practices, the features on the Website, or advances in technology. When material changes are made to this Notice, we will send you a notification or post a notice on our Website. If you ever have any questions about changes made to the Privacy Notice, please contact our Privacy Officer / DPO.

17. Your duty to inform us of changes

It is important that the Personal Information / Personal Data we hold about you is accurate and current. If you need to add or change any information, you should email dpo@blockchaintriangle.io and outline the required changes. We may contact you to verify that you have requested the changes and authenticate the new information provided.

18. Cookies

We collect web browser information, through the use of cookies, in order to enhance your experience on our Website and track how the services and products are being used. Cookies are small pieces of data that are stored on your device (computer or mobile device).

We use cookies to provide you with a better user experience. The information collected can include, but is not limited to, your IP address, referral URLs, the type of device you use, your operating system, the type of browser you use, geographic location, and other session data.

You may opt to deactivate your cookies, but it is important to note that you may not be able to access or use some features of our site.

19. Contact Details of Privacy Officer / DPO

Email: dpo@blockchaintriangle.io
Telephone no.: (441) 505-5538
Office Address: 52 Reid Street, Hamilton, HM 12, Bermuda