PROFITTO

PRIVACY POLICY

1. INTRODUCTION

1.1. Profitto Ltd ("Company") incorporated in the Republic of St. Vincent and the Grenadines with registered Number 25659 BC 2019.

1.2. Profitto Limited ("Company") is committed to protecting your privacy and handling your data in an open and transparent manner. The personal data that we collect, and process depends on the product or service requested and agreed in each case.

2. GENERAL DATA PROTECTION REGULATION

2.1 Protecting the privacy and safeguarding the personal and financial information of Company clients and website visitors is one of our highest priorities. The following General Data Protection (the "GDP") Policy explains how we collect, store and protect your information.

2.2 This privacy statement:

a. gives a breakdown of how the Company collects and processes your personal information and in forms you about the rights you have under the local data protection law,
b. it applies only to natural persons who are either current or potential clients of the Company, or are authorized representatives/Introducing Brokers (IBs) or beneficial owners of legal entities or of natural persons which/who are current or potential clients of the Company,
c. it applies to natural persons who had such a business relationship with the Company in the past
d. contains information about how and why we share your personal data with other members of the Company and other third parties (for example, trusted service providers or suppliers).

2.3 Your data can be referred to as "personal information" or "personal data". We may also sometimes collectively refer to handling, collecting, protecting, and storing your personal data or any such action as "processing" such personal data.

2.4 For the purposes of this policy, personal data shall mean any information relating to you which identifies or may identify you and which includes, for example, your name, address, identification number.

3. WHAT PERSONAL DATA WE PROCESS AND WHERE WE COLLECT IT FROM

3.1 We collect and process different types of personal data which we receive from our clients (potential and current) via their representatives or via our alternative channels of communication such as our website or members area, in the context of our business relationship.

3.2 We may also collect and process personal data which we lawfully obtain not only from you but from other entities within the Company Group, or other third parties e.g., individuals, public authorities, companies that introduce you to us, companies that process card payments.

3.3 Additionally, we may also collect and process personal data from publicly available sources (e.g., the Department of Registrar of Companies and Official Receiver, commercial registers and media outlets) which we lawfully obtain, and we are permitted to process.

a. If you are a prospective client the relevant personal data which we collect may include:

- Name;
- ID-Passport;
- Address;
- Date of Birth;
- Education;
- Experience;
- Volume;
- Employment status;
- Gender;
- Estimate Net Worth;
- Source of Funds;
- If you hold/held a prominent public function (for PEPs);
- Authentication data (e.g. signature).;
- Death certificate;
- Marriage certificate; and
- Bank Details.

b. If you are a prospective Introducing broker/Affiliate the relevant personal data which we collect may include:

- Name;
- ID-Passport;
- Address;
- City/Town;
- Postal Code;
- State;
- Country;
- Gender; and
- Bank Details.

c. If you are a prospective business then we can provide a corporate account to you, the relevant personal data which we collect may include:

Company details:

- Name;
- Address;
- State;
- Country;

- Directors;
- Shareholders (which hold 10% or more shares); and
- Bank Details.

Primary contact details (Director)

- Name;
- Date of Birth;
- Address;
- State;
- Country;
- Gender;
- Phone number;
- Email;
- Licenses that company obtained;
- Regulatory bodies that company is member of; and
- Background/Experience of the Company Director/Shareholder.

4. DO YOU HAVE AN OBLIGATION TO PROVIDE US WITH YOUR PERSONAL DATA

4.1 In order that we may be able to proceed with a business relationship with you, you must provide your personal data to us which is necessary for the commencement, execution of a business relationship and the performance of our contractual obligations. We are furthermore obligated to collect such personal data given the provisions of the money laundering law which require that we verify your identity before we enter a contract or a business relationship with you (or the legal entity for which you are the authorized representative/ agent or beneficial owner). You must, therefore, provide us at least with your identity card/passport, your full name, place of birth (city and country), and your residential address so that we may comply with our statutory obligation as mentioned above.

5. WHY WE PROCESS YOUR PERSONAL DATA AND ON WHAT LEGAL BASIS

As mentioned earlier we are committed to protecting your privacy and handling your data in an open and transparent manner and as such we process your personal data in accordance with the GDPR and the local data protection law for one or more of the following reasons:

5.1 For the performance of a contract

a. We process personal data to offer you financial services. Therefore, we require you to fill appropriateness form with additional data, which will enable us to provide you with best suited product. Such information, which we are obligated to collect, is necessary for us to be able to provide you with our services.
b. The purpose of processing personal data depends on the requirements for each product or service our Client Agreement provides more details with regards to this matter.

5.2 For compliance with a legal obligation

a. There are several legal obligations emanating from the relevant laws to which we are subject as well as statutory requirements, e.g., the Money Laundering Law and various supervisory authorities whose laws and regulations we are subject to. Such obligations and requirements impose on us necessary personal data processing activities for identity verification, compliance with court orders, tax law or other reporting obligations and anti-money laundering controls.

5.3 For the purposes of safeguarding legitimate interests

a. We process personal data to safeguard the legitimate interests pursued by us or by a third party. A legitimate interest is when we have a business or commercial reason to use your information. But even then, it must not unfairly go against what is right and best for you, therefore, our objective is to process your data in fair, transparent and lawful manner. Examples of such processing activities include:

- Means and processes we undertake to provide for the Company's IT and system security, preventing potential crime, asset security, admittance controls and anti-trespassing measures;
- Setting up CCTV systems, e.g. at ATMs, for the prevention of crime or fraud;
- Measures to manage business and for further developing products and services.
- Sharing your personal data within the Company Group for the purpose of updating/verifying your personal data in accordance with the relevant anti-money laundering compliance framework; and
- Company Group risk management.

6. YOU HAVE PROVIDED YOUR CONSENT

6.1 Provided that you have given us your specific consent for processing (other than for the reasons set out herein above) then the lawfulness of such processing is based on that consent. You have the right to revoke consent at any time. However, any processing of personal data prior to the receipt of your revocation will not be affected.

7. WHO RECEIVES YOUR PERSONAL DATA

7.1 In the course of the performance of our contractual and statutory obligations your personal data may be provided to various departments within the Company but also to other companies of Company. Various service providers and suppliers/contractors may also receive your personal data so that we may perform our obligations. Such service providers and suppliers enter into contractual agreements with the Company by which they observe confidentiality and data protection according to the data protection law.

7.2 It must be noted that we may disclose data about you for any of the reasons set out herein above, or if we are legally required to do so, or if we are authorized under our contractual and statutory obligations or if you have given your consent.

7.3 Under the circumstances referred to above, recipients of personal data may be, for example:

a. Supervisory and other regulatory and public authorities, since a statutory obligation exists. Some examples are the St. Vincent and the Grenadines, the income tax authorities, criminal prosecution authorities;
b. Credit and financial institutions such as correspondent banks;
c. For our anti-money laundering process;
d. External legal consultants;
e. Auditors and accountants;
f. Marketing companies and market research companies;
g. Companies which help us to provide you with our services;
h. Card payment processing companies;
i. Fraud prevention agencies;
j. File storage companies, archiving and/or records management companies, cloud storage companies;
k. Compliance consultant companies;
l. Companies who assist us with the effective provision of our services to you by offering technological expertise, solutions and support and facilitating payments; and
m. Purchasing and procurement and website and advertising agencies.
n. Introducing Brokers and Affiliates with whom we have mutual relationship.

8. HOW WE TREAT YOUR PERSONAL DATA FOR MARKETING ACTIVITIES AND WHETHER PROFILING IS USED FOR SUCH ACTIVITIES

8.1 We may process your personal data to inform you about products, services and offers that may be of interest to you or your business.

8.2 The personal data that we process for this purpose consists of information you provide to us and data we collect and/or infer when you use our services, such as information on your transactions. We study all that information to form a view on what we think you may need or what may interest you. In some cases, profiling is used, i.e., we process your data automatically with the aim of evaluating certain personal aspects in order to provide you with targeted marketing information on products.

8.3 We can only use your personal data to promote our products and services to you if we have your explicit consent to do so or, in certain cases, if we consider that it is in our legitimate interest to do so. You have the right to object at any time to the processing of your personal data for marketing purposes, which includes profiling, by contacting at any time the Company in writing at sale@profittoltd.com.

9. HOW LONG WE KEEP YOUR PERSONAL INFORMATION FOR

9.1 We will keep your personal data for as long as we have a business relationship with you (as an individual or in respect of our dealings with a legal entity you are authorized to represent or are beneficial owner). Once our business relationship with you has ended, we may keep your data for up to ten (10) years. We may keep your data for longer than 10 years if we cannot delete it for legal, regulatory or technical reasons.

9.2 For prospective client personal data [or authorized representatives/agents or beneficial owners of a legal entity prospective client] we shall keep your personal data for 6 months from the date of notification of the rejection of your application for our services and/or facilities or from the date of withdrawal of such application.

10. YOUR DATA PROTECTION RIGHTS:

10.1 You have the following rights in terms of your personal data we hold about you:

a. Receive access to your personal data. This enables you to e.g., receive a copy of the personal data we hold about you and to check that we are lawfully processing it. In order to receive such a copy, you can complete our web form through the Company's website (https://www.profittoltd.com/contact-us/).

b. Request correction [rectification] of the personal data we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected.

c. Request erasure of your personal information. This enables you to ask us to erase your personal data (known as the 'right to be forgotten') where there is no good reason for us continuing to process it.

d. Object to processing of your personal data where we are relying on a legitimate interest and there is something about your situation which makes you want to object to processing on this ground. If you lodge an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights, and freedoms. You also have the right to object where we are processing your personal data, for direct marketing purposes. This also includes profiling in as much as it is related to direct marketing. If you object to processing for direct marketing purposes, then we shall stop the processing of your personal data for such purposes.

e. Request the restriction of processing of your personal data. This enables you to ask us to restrict the processing of your personal data, i.e., use it only for certain things, if:
   - it is not accurate;
   - it has been used unlawfully but you do not wish for us to delete it;
   - it is not relevant any more, but you want us to keep it for use in possible legal claims; and
   - you have already asked us to stop using your personal data but you are waiting us to confirm if we have legitimate grounds to use your data.

f. Request to receive a copy of the personal data concerning you in a format that is structured and commonly used and transmit such data to other organizations. You also have the right to have your personal data transmitted directly by us to other organizations you will name [known as the right to data portability].

g. Withdraw the consent that you gave us regarding the processing of your personal data at any time. Note that any withdrawal of consent shall not affect the lawfulness of processing based on consent before it was withdrawn or revoked by you.

10.2 To exercise any of your rights, or if you have any other questions about our use of your personal data, please contact your account manager or send a message to support@profittoltd.com

11. PERSONAL DATA BREACHES

11.1 A personal data breach is a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

11.2 A breach is therefore a type of security incident and there are three different types of breach that may occur:

a. Confidentiality breach: an accidental or unauthorized disclosure of, or access to, personal data.
b. Availability breach: an accidental or unauthorized loss of access to, or destruction of, personal data.
c. Integrity breach: an accidental or unauthorized alteration of personal data.
d. A breach can affair confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.

11.3 A personal data breach would, for example, include:

a. personal data being disclosed to an unauthorized person, e.g. an email containing personal data being sent to the wrong person.
b. an unauthorized person accessing personal data, e.g. an employee’s personnel file being inappropriately accessed by another member of staff due to a lack of appropriate internal restrictions.
c. a temporary or permanent loss of access to personal data, e.g. where a client’s or customer’s personal data is unavailable for a certain period of time due to a system shut down, power, hardware or software failure, infection by malware or viruses or denial of service attack, where personal data has been deleted either accidentally due to human error or by an unauthorized person or where the decryption key for securely encrypted data has been lost.

11.4 Notification to the Office of the Commissioner.

a. Not all personal data breaches are necessary to be notified to the Office of the Commissioner.
b. Every suspicion of a data breach has to be notified to the Data Protector Officer of the Company.
c. The DPO will gather all the necessary information as soon as possible and assess the level of risk to decide if the case needs to be communicated with the Office of the Commissioner.
d. The breach will only need to be notified if it is likely to result in a risk to the rights and freedoms of data subjects, and this needs to be assessed internally by the Company on a case- by-case basis. A breach is likely to result in a risk to the rights and freedoms of data subjects if, for example, it could result in:

- loss of control over their data
- limitation of their rights
- discrimination
- identity theft
- fraud
- damage to reputation

- financial loss
- unauthorized reversal of pseudonymization
- loss of confidentiality
- any other significant economic or social disadvantage.

11.5 Where a breach is reportable, the Company must notify the Office of the Commissioner without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If our report is submitted late, it must also set out the reasons for our delay. Our notification must at least include:

a. a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records
b. the name and contact details of the Company's CEO
c. a description of the likely consequences of the breach
d. a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

We can provide this information in phases, without undue further delay, if it cannot all be provided at the same time.

11.6 Awareness of the breach occurs when we have a reasonable degree of certainty that a breach has occurred. In some cases, it will be relatively clear from the outset that there has been a breach. However, where it is unclear whether or not a breach has occurred, we will have a short period of time to carry out an initial investigation and assessment after becoming aware about a potential breach in order to establish with a reasonable degree of certainty whether or not a breach has in fact occurred. If, after this short initial investigation, we establish that there is a reasonable degree of likelihood that a breach has occurred, the 72 hours starts to run from the moment of that discovery.

12. RIGHT TO LODGE A COMPLAINT

12.1 If you have exercised any or all of your data protection rights and still feel that your concerns about how we use your personal data have not been adequately addressed by us, you have the right to complain by contacting support (https://www.profittoltd.com/contact-us/).

12.2 We may modify or amend this privacy statement from time to time.

12.3 We will notify you appropriately when we make changes to this privacy statement, and we will amend the revision date at the top of this page. We do however encourage you to review this statement periodically so as to be always informed about how we are processing and protecting your personal information.

14. COMPANY'S CONTACT DETAILS

14.1 Clients shall communicate with the Company with the communication methods described within this policy and/or at the following address:

Correspondence Address: Suite 305, Griffith Corporate Centre, Beachmont P.O. Box 1510, Kingstown, St. Vincent and the Grenadines.

Customer Service E-mail: support@profittoltd.com