STRIFOR

POLITICAL EXPOSED PERSONS POLICY

WWW.STRIFOR.ORG

STRIFOR

1. **GENERAL PROVISIONS**

1.1. This Regulation on the Processing and Protection of Personal Data regarding the handling of Personal Data (hereinafter referred to as the “Regulation”) determines the policy of 7 Lucky Trading (Mauritius) Ltd, a company registered under the laws of Republic of Mauritius, having Investment Dealer (Full Service Dealer, excluding Underwriting) License №GB23202670 and regulated by Financial Services Commission of Mauritius, having registered address at: 1/F River Court, 6 St Denis Street, Port Louis, 11328, Mauritius regarding the Processing of Personal Data of all Subjects whose Personal Data is processed by the Company, including the collection procedure , storage, use, transfer and Protection of Personal Data.

1.2. The Regulations have been developed in accordance with the current legislation of Saint Vincent and the Grenadines.

1.3. The provisions of the Regulation apply to the Processing of Personal Data received both before and after its approval.

1.4. In everything that is not regulated by the Regulations, but relates to its subject, it is necessary to be guided by the current legislation of Saint Vincent and the Grenadine.

1.5. For the purposes of the Regulations, the following basic concepts are used:

Website of the Company – website of the Company on the Internet, located at www.strifor.biz.

Personal data – any information relating to an identified individual or an identifiable individual.

Subject of Personal Data is an individual in respect of whom the Processing of Personal Data is carried out.

An identifiable natural person is an individual who can be directly or indirectly identified, in particular through his surname, first name, patronymic, date of birth, identification number or through one or more signs characteristic of his physical, psychological, mental , economic, cultural or social identity.

Processing of Personal Data – any action or set of actions performed with Personal Data, including collection, systematization, storage, modification, use, depersonalization, blocking, Distribution, Provision, deletion of Personal Data.

Protection of Personal Data is a set of legal, organizational and technical measures aimed at preventing unauthorized or accidental access to Personal Data, their modification, blocking, copying, distribution, provision, deletion, as well as other unlawful actions in relation to Personal Data.

Authorized person is a government body, a legal entity of Saint Vincent and the Grenadines, another organization or individual carrying out the Processing of Personal Data on behalf of or in the interests of the Company on the basis of an agreement with it or in accordance with an act of legislation.

Dissemination of Personal Data – actions aimed at familiarizing an indefinite number of persons with Personal Data.

Providing Personal Data – actions aimed at becoming familiar with the Personal Data of a certain person or group of persons;

User – any visitor to the resources that are part of the Company's Trading System, incl. a client, a participant in CFD trading, both who is and who is not a client of the Company.

Trading system – an information system within which the acceptance, control and registration of applications for the purchase and (or) sale of CFDs are carried out; carrying out transactions for the purchase and sale of CFDs; determining prices for CFDs; determining the requirements and obligations of the parties based on the results of transactions with CFDs, as well as ensuring the execution of these transactions; preparation and generation of reporting documents based on the results of transactions with CFDs; storage, processing and disclosure of information necessary for making and executing transactions with CFDs; performing other functions necessary for organizing trading in CFDs, carried out in accordance with the legislation of Saint Vincent and the Grenadines.

Account – account created by the Client in the Trading system and used including for the Client to carry out transactions within the Trading system, accounting for funds, electronic money and CFDs of the Client held by the Company .

Personal Account is a functional technical module of the Trading System, used for registration, identification, verification, opening and closing accounts, access to an electronic wallet and accounts, depositing and withdrawing funds, exchanging cryptocurrency at the current rate established by the Company, and performing other actions within the framework of the Trading System.

Electronic wallet is an integral part of the account (account), used for recording and storing funds transferred by the Client to the Company and reflected by the Company on the Client's Electronic wallet in the personal account, allowing the Client to carry out transactions for the acquisition (alienation, exchange) of CFDs in the Trading system, including including replenishing (transferring funds) to accounts within the Trading Platform, withdrawing funds from the Trading System.

Blocking Personal Data – termination of access to Personal Data without deleting it.

Depersonalization of Personal Data – actions as a result of which it becomes impossible to determine the ownership of Personal Data to a specific Personal Data Subject without the use of additional information.

Responsible person is a person responsible for implementing internal control over the Processing of Personal Data.

Deputy responsible person - a person performing the functions of a responsible person during his absence.

Applicants are citizens or legal entities who have submitted (are submitting) an application to the Company.

Counterparties are individuals, individual entrepreneurs and (or) employees of individual entrepreneurs, representatives and (or) employees of legal entities who are one of the parties to civil contracts concluded with the Company.

Client - an individual (including an individual entrepreneur) or a legal entity (including a foreign organization) who has entered into an appropriate civil law agreement with the Company and has undergone the Verification procedure with whom the Company carries out, or who has applied to the Company for the following transactions (operations):

alienation, acquisition of CFD;

other transactions (operations) allowed to be carried out within the Trading System in accordance with the legislation of Saint Vincent and the Grenadines

NCPD – National Center for Personal Data Protection of Saint Vincent and the Grenadines

EPK – expert verification commission. The “EPC” mark indicated in the List in relation to the storage periods of specific types of documents means that the storage period of such documents after an examination of their value can be extended, including such documents may have historical, scientific, social, economic, political or cultural value and are subject to transfer for permanent storage to state archives.

2. PRINCIPLES FOR PROCESSING PERSONAL DATA

2.1. With regard to the Processing of Personal Data of all Personal Data Subjects whose Personal Data is processed by the Company, the Company is guided by the following principles:

2.1.1. The Company processes Personal Data in accordance with local legal acts of the Company and the requirements of the legislation of Saint Vincent and the Grenadines

2.1.2. at all stages of Personal Data Processing, the Company ensures that the Processing is proportionate to the stated goals and a fair balance of interests of all interested parties;

2.1.3. in each case, the Company has a legal basis for Processing Personal Data: consent of the Personal Data Subject or other basis provided for by the Law or other act of legislation of Saint Vincent and the Grenadines

2.1.4. if the legal basis for the relevant Processing of Personal Data is consent, the Company ensures that the Personal Data Subject consents to the Processing of his Personal Data in accordance with the procedure provided for in Chapter 5 of the Regulations;

2.1.5. in the event of a change in the initially stated purposes of Processing Personal Data, the Company re-requests the consent of the Personal Data Subject to the Processing of his Personal Data in accordance with the changed purposes of Processing in the absence of other grounds for such Processing provided for by the legislative acts of Saint Vincent and the Grenadines

2.1.6. The processing of Personal Data is limited to the achievement of specific, pre-declared legitimate purposes;

2.1.7. The Company ensures that the content and volume of processed Personal Data correspond to the stated purposes of Processing at all stages of Processing and are not redundant;

2.1.8. The Company takes measures to ensure the accuracy of the Personal Data processed and, if necessary, updates them;

2.1.9. The Company stores Personal Data in a form that allows identification of the Personal Data Subject for no longer than required by the stated purposes of Personal Data Processing;

2.1.10. The Company ensures the transparent nature of the Processing of Personal Data by informing Personal Data Subjects about the Personal Data Processing processes existing in the Company through the Regulations, other local legal acts of the Company regarding the Processing of Personal Data, providing

other information about the Processing of Personal Data, including at the request of the Personal Data Subject .

3. CATEGORIES OF PERSONAL DATA SUBJECTS

3.1. The Company processes Personal Data of the following categories of Subjects:

- employees of the Company;
- relatives (family members) of employees;
- persons applying for employment in the Company;
- relatives (family members) of persons applying for employment in the Company;
- candidate;
- counterparties;
- Users of the Company's Website;
- applicants;
- trainees.

4. OBTAINING CONSENT TO PROCESSING

4.1. The Company ensures that consent to the Processing of Personal Data is obtained for purposes for which the legal basis is the consent of the Personal Data Subject, before such Processing begins.

4.2. The Company ensures that consent to Processing received from Personal Data Subjects meets the criteria of free, unambiguous and informed consent.

4.3. Consent is not required when there is another legal basis for the Processing of Personal Data for the relevant purpose, established by Art. 6 of the Law (for cases of Processing of Personal Data that are not special) or Art. 8 of the Law (for cases of Processing of special Personal Data).

Accordingly, in cases where the Processing of Personal Data may be carried out on another basis (for example, paragraph 16 of Article 6 of the Law, paragraph 19 of Article 6 of the Law) and such a basis is received/applicable for the relevant purpose, the Company does not request consent to Processing for this purpose.

Consent is obtained by the Company in writing, in the form of an electronic document or in another electronic form through:

- indication (selection) by the Personal Data Subject of certain information (code) after receiving SMS message or message to an email address; or
- putting the corresponding mark on the Internet resource by the Personal Data Subject; or
- other methods to establish the fact of obtaining the consent of the Personal Data Subject.

5. ORDER OF PROCESSING AND CROSS-BORDER TRANSFER

5.1. If the Company, as an Operator, entrusts the Processing of Personal Data to an Authorized Person on the basis of an agreement concluded with this person, such an agreement must contain at least the following conditions:

1. purposes of Processing Personal Data;

2. a list of actions that will be performed with Personal Data by the Authorized Person;

3. obligations to maintain the confidentiality of Personal Data;

4. measures to ensure the Protection of Personal Data in accordance with Art. 17 of the Law.

5.2. An employee who is directly involved in negotiations with an Authorized Person to conclude an agreement with the Company must

notify the responsible person (or deputy responsible person) about the possibility of concluding such an agreement before the start of negotiations.

5.3. The responsible person (or deputy responsible person) assesses the risks of engaging an Authorized Person.

5.4. As part of the risk assessment, the responsible person (or deputy responsible person) analyzes the measures taken by the Authorized Person to Protect Personal Data (in particular, studies the Authorized Person's policy regarding the Processing of Personal Data), if necessary, asks the Authorized Person questions regarding the Processing of Personal Data by him, analyzes information in the public domain (articles in the media, other sources about leaks of Personal Data that occurred with the Authorized Person, other negative facts that may affect the Protection of the Company's Personal Data).

5.5. Based on the results of the assessment, the responsible person (or deputy responsible person) informs the relevant employee about the possibility or impossibility of involving such an Authorized Person

5.6. The Responsible Person is involved in agreeing the terms of each agreement with each Authorized Person.

5.7. If the Company intends to carry out a cross-border transfer of Personal Data to the territory of foreign countries that do not provide an adequate level of Protection of the rights of Personal Data Subjects, the responsible person (or deputy responsible person) is obliged to conduct an analysis of the risks associated with such transfer before such transfer.

5.8. The list of foreign states on whose territory the appropriate level of Protection of the rights of Personal Data Subjects is ensured includes foreign states that are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on January 28, 1981.

5.9. Cross-border transfer of Personal Data is possible only in cases where the responsible person has come to the conclusion that it is

possible to ensure the safety of Personal Data after such transfer, and if there are legal grounds.

5.10. The appropriate legal basis for the transfer by the Company of Personal Data to states in whose territory the appropriate level of Protection of the rights of Personal Data Subjects is not ensured is:

1. consent of the Personal Data Subject, provided that the Personal Data Subject is informed of the risks arising from the lack of an adequate level of their Protection;

2. transfer of Personal Data to perform actions established by the agreement concluded (to be concluded) with the Personal Data Subject, on the basis of which they were obtained
Personal Information;

3. transfer of Personal Data in cases where Personal Data can be obtained by any person by sending a request in cases and in the manner prescribed by law;

4. the need to transfer Personal Data to Protect the life, health or other vital interests of the Personal Data Subject or other persons, if obtaining the consent of the Personal Data Subject is impossible;

5. permission of the authorized body for the Protection of the rights of Personal Data Subjects.

5.11. If, before carrying out a cross-border transfer, the Company must take certain actions (for example, obtain the consent of the Personal Data Subject or provide another legal basis for a cross-border transfer), the responsible person will organize a process for carrying out such actions.

5.12. The list of Authorized Persons to whom the Company entrusts the Processing of Personal Data is specified in the Appendix to the Regulations.

5.13. The Company may transfer Personal Data to third parties without following the procedure described above in cases where the

Company is obliged to transfer such Personal Data to a certain third party due to legal requirements.

6. CHANGING PROCESSING PROCESSES

6.1. If a decision is made to change existing Personal Data Processing processes (for example, changing the initially stated purposes of Personal Data Processing, attracting a new Authorized Person, changing the established storage periods for Personal Data, etc.), the employee who initiated such a change must agree on it before implementing such a change with the responsible person (or deputy responsible person).

6.2. The Company, represented by the responsible person (or deputy responsible person), before implementing any change in the Personal Data Processing processes, must conduct an analysis of the compliance of the change in question with the requirements of current legislation. In particular, the responsible person (or deputy responsible person) must ensure that the new Processing of Personal Data will comply with the rules set out in the Regulations.

If necessary, the responsible person involves third-party consultants in such analysis.

6.3. If the responsible person (or deputy responsible person) has come to the conclusion that the change under consideration complies with the requirements of the law, the responsible person (deputy responsible person) creates a list of actions that must be taken before implementing such a change.

6.4. The scope of actions may include introducing changes to the Regulations, other Company policies regarding the Processing of Personal Data, concluding an agreement with a new Authorized Person, ensuring an appropriate legal basis for a new purpose of Processing, developing a draft consent of the Personal Data Subject and organizing the receipt of such consent, preparing instructions for

employees Companies for obtaining proper consent of the Personal Data Subject and others.

6.5. Changes to the Personal Data Processing processes come into force only after all planned actions have been completed or on another date at the discretion of the responsible person (or deputy responsible person).

7. STORING AND DELETION OF PERSONAL DATA

7.1. The Company stores Personal Data in a form that allows identification of the Personal Data Subject for no longer than required by the stated purposes of Personal Data Processing.

7.2. Upon achieving the goals of Processing, as well as after the expiration of the period provided for by the legislation on Personal Data, the agreement on the basis of which the Personal Data was obtained, or the consent of the Personal Data Subject to the Processing of his Personal Data, the Company ceases Processing of Personal Data.

7.3. The Company also terminates the Processing of Personal Data earlier if it receives an application from the Personal Data Subject to terminate the Processing of his Personal Data and (or) delete his Personal Data or withdraw the consent of the Personal Data Subject.

7.4. The Company has the right to continue Processing Personal Data (in particular, to refuse the Personal Data Subject to execute his application) if the Company has other grounds for such Processing provided for by law. For example, the Company may refuse to fulfill an employee's request to terminate the Processing of his Personal Data and (or) delete his Personal Data if the Company is obliged to store such Personal Data for the period established by law.

7.5. When storing Personal Data, the Company ensures compliance with the conditions ensuring the safety of Personal Data.

7.6. Paper documents containing Personal Data are located in specially designated areas with limited access under conditions that ensure

their protection from unauthorized access. The list of places for storing documents is determined by the Company.

7.7. Personal data stored electronically is protected from unauthorized access using special technical and software protection tools.

7.8. The destruction or depersonalization of Personal Data is carried out in a manner that precludes further Processing of this Personal Data.

7.9. If it is necessary to destroy or block part of the Personal Data, the material medium is destroyed or blocked with preliminary copying of information that is not subject to destruction or blocking, in a manner that precludes simultaneous copying of Personal Data subject to destruction or blocking.

7.10. If it is necessary to destroy or block part of the Personal Data, the material medium is destroyed or blocked with preliminary copying of information that is not subject to destruction or blocking, in a manner that precludes simultaneous copying of Personal Data subject to destruction or blocking.

8. RIGHTS OF PERSONAL DATA SUBJECTS

8.1. In accordance with the provisions of the Law, Personal Data Subjects may send requests to the Company for the exercise of the following rights:

1. the right to receive information regarding the Processing of Personal Data:

The subject has the right to receive information regarding the Processing of his Personal Data, containing:

- name and location of the Company,
- confirmation of the fact of Processing of Personal Data by the Company,
- Personal data of the Subject and the source of its receipt,
- legal grounds and purposes of Personal Data Processing,

- the period for which the Subject's consent is given,
- name and location of the Authorized Person,
- other information required by law.

2. the right to receive information about the provision of Personal Data to third parties:

The subject of Personal Data has the right to receive from the Company information about the Provision of his Personal Data to third parties once a calendar year, unless otherwise provided by the Law and other legislative acts. Information is provided free of charge.

3. the right to make changes to your Personal Data:

The subject of Personal Data has the right to demand that the Company make changes to his Personal Data if it is incomplete, outdated or inaccurate.

4. the right to demand termination of the Processing of Personal Data and (or) its deletion:

The subject of Personal Data has the right to demand from the operator a free termination of the Processing of his Personal Data, including its deletion, if there are no grounds for the Processing of Personal Data.

5. Right to withdraw consent of the Personal Data Subject:

The Personal Data Subject has the right to withdraw his consent to the Processing of Personal Data at any time without giving reasons.

6. Subjects of Personal Data also have the right to appeal actions (inaction) and decisions of the Company to the authorized body for the Protection of the Rights of Subjects of Personal Data.

8.2. To exercise one or more rights specified in paragraphs. 1-5 clause 8.1 of these Regulations The subject may send the Company a corresponding application in writing or in the form of an electronic document. Right to withdraw consent - the Personal Data Subject

may implement by sending a corresponding application in writing, or in the form of an electronic document, or in another form through which consent was obtained.

- The Subject's application must contain:
- surname, first name, patronymic (if any) of the Personal Data Subject;
- address of residence (place of stay) of the Subject Personal data;
- date of birth of the Personal Data Subject;
- the essence of the requirements;
- identification number of the Personal Data Subject, in the absence of such a number - the number of the identity document of the Personal Data Subject, in cases where this information was indicated by the Personal Data Subject when giving his consent or Processing of Personal Data is carried out without the consent of the Personal Data Subject;
- personal signature or electronic digital signature of the Personal Data Subject

8.3. The procedure for the Company's response to requests received from Personal Data Subjects to exercise their rights is described below:

1. right to receive information.

Upon receipt of a request from a Personal Data Subject to exercise his right to receive information regarding the Processing of Personal Data, the Company, within 5 working days after receiving an application from the Personal Data Subject, provides the requested information or notifies the Personal Data Subject of the reasons for refusal to provide it.

- The information requested may include:
- name and location of the Company;
- confirmation of the fact of Processing of Personal Data by the Company (Authorized Person);
- Personal data and the source of its receipt;
- legal grounds and purposes of Personal Data Processing;

- the period for which his consent is given;
- name and location of the Authorized Person, which is a government body, a legal entity of Saint Vincent and the Grenadines, or another organization, if the Processing of Personal Data is entrusted to such a person;
- other information required by law.

The requested information is not provided if Personal data can be obtained by any person by sending a request in the manner prescribed by law, or by accessing an information resource (system) on the global computer network Internet, as well as in other cases provided for by law.

Such information is provided to the Personal Data Subject free of charge, except for cases provided for by legislative acts.

2. the right to receive information about the Provision of Personal Data to third parties.

Upon receipt of a request from the Personal Data Subject to exercise his right to receive information about the Provision of Personal Data to third parties, the Company, within 15 calendar days after receiving an application from the Personal Data Subject, provides the Personal Data Subject with information about what Personal Data of this Subject was provided and to whom it was provided during the year preceding the date of submission of the application, or notifies the Personal Data Subject of the reasons for refusal to provide it.

The requested information is not provided if Personal data can be obtained by any person by sending a request in the manner prescribed by law, or by accessing an information resource (system) on the global computer network Internet, as well as in other cases provided for by law.

3. the right to change Personal Data.

Upon receipt of a request from a Personal Data Subject to exercise his right to change Personal Data, the Company, within 15 calendar days after

receiving an application from the Personal Data Subject, makes appropriate changes to his Personal Data and notifies the Personal Data Subject about this or notifies the Personal Data Subject of the reasons refusal to make such changes.

When sending such a request, the Personal Data Subject attaches the relevant documents and (or) their duly certified copies confirming the need to make changes to personal Information.

Changes to Personal Data during their Processing without the use of automation tools are carried out by the Company by recording on the same material medium information about changes made to them or by producing a new material medium with the changed Personal Data. The old material medium of Personal Data is destroyed.

4. the right to terminate the Processing of Personal Data and/or their removal.

Upon receipt of a request from the Personal Data Subject to exercise his right to terminate the Processing of Personal Data and (or) its deletion, the Company within up to 15 calendar days after receiving an application from the Personal Data Subject stops the Processing of Personal Data and deletes it (ensures the termination of the Processing of Personal Data , as well as their removal by the Authorized Person) and notifies the Personal Data Subject about this. If it is not technically possible to delete Personal Data, the Company is obliged to take measures to prevent further Processing of Personal Data, including blocking it, and notify the Personal Data Subject about this within the same period.

The Company has the right to refuse to satisfy the Personal Data Subject's request to terminate the Processing of his Personal Data and (or) delete it if there are grounds for the Processing of Personal Data provided for by the legislation of the Saint Vincent and the Grenadines, including if they are necessary for the stated purposes of their Processing, with notification of this

Personal Data Subject within 15 calendar days after receiving an application from the Personal Data Subject.

5. right to withdraw consent

Upon receipt of a request from the Personal Data Subject to exercise his right to withdraw consent, the Company, within 15 calendar days after receiving the application from the Personal Data Subject, stops Processing Personal Data, deletes it and notifies the Personal Data Subject about this, except in cases where the Company has the right to continue Processing Personal Data if there are grounds established by the legislation of Saint Vincent and the Grenadines. If it is not technically possible to delete Personal Data, the Company is obliged to take measures to prevent further Processing of Personal Data, including blocking it, and notify the Personal Data Subject about this within the same period.

8.4. In the event that the provision by the Company of services in accordance with the agreement for participation in trading in CFDs is impossible without the use of Personal Data, the termination of Processing and (or) deletion of which is requested by the Client (data necessary for identification and verification, etc.), the Company has the right terminate the provision of services unilaterally. At the same time, the Company limits the Client's ability to conduct transactions solely by returning the Client's funds and CFDs to other Client accounts outside the Trading system, after which the Client is deprived of the right to access his personal account, conduct transactions and carry out other actions in the Trading system, and the corresponding civil law the agreement with the Company and the Client is considered terminated.

8.5. For assistance in exercising the rights, the Personal Data Subject may also contact the person responsible for internal control over the Processing of Personal Data in the Company by sending a message to the Company's email address.

STRIFOR

9. PERSONAL DATA PROTECTION MEASURES

9.1. Personal data must be processed in a manner that prevents its loss or misuse.

9.2. Personal data, as well as paper and electronic media containing Personal data, are subject to protection.

9.3. Measures to ensure the Protection of Personal Data taken by the Company include:

1. appointment of a person responsible for internal control over the Processing of Personal Data;

2. publication of documents defining the policy regarding the Processing of Personal Data;

3. familiarization of employees and other persons directly involved in the Processing of Personal Data with the provisions of the legislation on Personal Data, including requirements for the Protection of Personal Data, documents defining the policy regarding the Processing of Personal Data;

4. training of employees and other persons directly involved in the Processing of Personal Data on issues of working with Personal Data;

5. establishing the procedure for access to Personal Data, including those processed in the information resource (system);

6. implementation of technical and cryptographic Protection of Personal Data in accordance with the classification of information resources (systems) containing Personal Data.

9.4. To ensure internal Protection of Personal Data, all employees who have access to Personal Data, within the scope of their powers, are required to comply with the following measures:

1. delete Personal Data, including those stored on a computer, in correspondence, etc., that are no longer necessary for Processing, taking into account the purpose for which they were collected;

2. do not disclose Personal Data to third parties;

3. ensure storage of information and media containing Personal Data, excluding access to it by third parties;

4. do not use Personal Data for personal purposes outside the scope of work duties;

5. ensure the safety and immutability of Personal Data if the task being performed does not involve their correction or addition;

6. not to disclose codes, passwords, access keys, decryption tools and other similar information related to the Protection of Personal Data that have become known to the employee;

7. do not send Personal Data or media containing Personal Data through personal messengers, personal mail, or unsecured communication channels;

8. inform the responsible person in case of violation of Personal Data Protection systems within 1 hour from the moment when the employee it became known;

9. inform the responsible person about any other emergency situations related to the Processing of Personal Data within 1 hour from the moment the employee became aware of it;

10. if an employee identifies violations during the Processing of Personal Data by another person, if possible, prevent the commission of such a violation;

11. maintain confidentiality when posting information in the media, as well as when conducting interviews;

12. fulfill other obligations for the Protection of Personal Data assigned to the employee by local legal acts of the Company and current legislation.

9.5. If an employee identifies violations of the above measures on the part of another person, the employee is obliged, if possible, to stop the commission of such a violation, as well as to report the violation to the person in charge or his deputy, or to the director of the Company or his immediate supervisor.

9.6. The general organization of Personal Data Protection is carried out by the responsible person (or his deputy), who ensures:

1. familiarization of employees, against signature, with the Regulations and other local legal acts, as well as the requirements of the legislation of Saint Vincent and the Grenadines governing Processing and Protection Personal data;

2. conducting training for employees on Personal Data Protection;

3. general control over employees' compliance with Personal Data Protection measures.

10. PERSON RESPONSIBLE

10.1. In order to ensure compliance with the requirements of current legislation during the Processing of Personal Data, the Company has appointed a person responsible for internal control over the Processing of Personal Data, as well as a person replacing him.

10.2. For all questions arising in connection with these Regulations, other documents defining the Operator's policy regarding the Processing of Personal Data, as well as Processing issues, you can contact the responsible person or deputy responsible person.

11. RESPONSE TO SECURITY SYSTEMS VIOLATIONS

11.1. A violation of Personal Data Protection systems for the purposes of the Regulations is considered to be accidental or illegal destruction,

loss, modification of Personal Data, unauthorized Distribution or Provision of Personal Data.

11.2. If an employee of the Company has reason to believe that a violation of the Personal Data Protection systems has occurred, he must inform the person in charge (or his deputy) about this within 1 hour from the moment the employee has the corresponding suspicions. In his notice, the employee must clearly indicate that there is a suspicion of a violation of the Personal Data Protection systems.

11.3. The employee must ensure that the person in charge (or his/her deputy) has confirmed receipt of the information by phone, email, instant messenger or physically.

11.4. An employee should not attempt to investigate this matter on his own if such an investigation could delay the Company's response time or harm the situation.

11.5. The responsible person (or deputy responsible person) must inform the director of the Company within 1 hour of receiving the information.

11.6. The Director of the Company together with the responsible person (or his deputy) must immediately develop a plan

actions to investigate a possible violation of Personal Data Protection systems.

11.7. The Company informs the Personal Data Subject of cases of violation of the law and rules for handling his Personal Data when handling his Personal Data, if the level of risk that such violations may lead to a violation of the rights and legitimate interests of the Personal Data Subject is high.

11.8. The Company electronically maintains a log of cases of violation of the law and rules for handling Users' Personal Data when handling Users' Personal Data.

11.9. The Company electronically maintains a log of actions constituting the handling of Users' Personal Data.

11.10. If a violation of the Personal Data Protection systems is confirmed, the person in charge (or his deputy) notifies the NCPPD about violations of the systems immediately, but no later than 3 business

days after the Company becomes aware of such violations, except in cases provided for by the NCPPD.

12. ACCESS RESTRICTION

12.1. The list of persons who have access to Personal data processed by the Company is approved by the director of the Company.

12.2. Access to Personal Data is provided only to those employees of the Company whose job duties involve working with Personal Data, and only for the period necessary to work with the relevant data. The list of such persons is determined by the Company.

12.3. If it becomes necessary to provide access to Personal Data to employees who are not included in the list of persons with access to Personal Data, they may be provided with temporary access to a limited range of Personal Data by order of the Director of the Company or another person authorized by the Director of the Company. Relevant employees must be familiarized with all local legal acts of the Company in the field of Personal Data.

12.4. Employees of the Company who do not have a properly issued permit are prohibited from accessing Personal Data.

13. PROVIDING ACCESS TO THE STATEMENT

13.1. In order to ensure the transparent nature of the Processing of Personal Data, the responsible person (or his deputy), at the request of the Personal Data Subject, provides such person with access to this Regulation, as well as other information about the Processing of Personal Data of the Company.

13.2. At the same time, the responsible person (deputy responsible person) may exclude from the provided version of the Regulations norms that are confidential in cases where failure to provide such information does not contradict the law.

STRIFOR

14. **RESPONSIBILITY**

14.1. Persons guilty of violating the rules governing the Processing and Protection of Personal Data bear disciplinary, administrative, civil or criminal liability in accordance with the current legislation of Saint Vincent and the Grenadines