FINARTEL CAPITAL AIFLNP V.C.I.C. LTD

PERSONAL DATA PROTECTION POLICY

VERSION 3

16.06.2020

Alkaios, 7, Alkaios Court, Flat/Office 103,
3090, Limassol, Cyprus

+357 25 057 150

hq@finartel.fund

CySec License Number: LPAIF114/2014

FINARTEL

Contents

1. POLICY STATEMENT 5
2. BACKGROUND 5
3. DEFINITIONS 5
4. INTRODUCTION 6
5. SCOPE AND LIMITATION 7
6. DATA PROTECTION RISKS 7
7. RESPONSIBILITIES 7
8. GENERAL EMPLOYEES' GUIDELINES 8
9. SUBJECT TO CONSENT 8
10. PROCESSING OF PERSONAL DATA 8
10.1. Collection 8
10.1.1. Collection of personal data of clients 9
10.1.2. Collection of personal data of employees 10
10.1.3. Collection of personal data of other individuals 10
10.2. Use 10
10.2.1. Use of personal data of clients 10
10.2.2. Use of personal data of employees 10
10.2.3. Use of personal data of other individuals 11
10.3. Storage of personal data 11
10.3.1. Personal Data kept physically/on Paper 11
10.3.2. Personal data stored electronically 11
10.4. Access 12
10.5. Disclosure 12
10.6. Transfer 12
10.7. Destruction 13
10.7.1. Hard copies 13
10.7.2. Electronically 13

11. FOR HOW LONG THE COMPANY KEEPS YOUR PERSONAL DATA 13
12. PROCESSING FOR OTHER REASON 14
13. SECURITY MEASURES AND POLICIES 14
13.1 Organizational Security Measures and Policies 14
13.1.1. Data Protection Officer 14
13.1.2. Trainings and Seminars 14
13.1.3. Conduct of Privacy Impact Assessment 15
13.1.4. Recording and documentation of processing activities carried out by the Company 15
13.1.5. Duty of Confidentiality 15
13.1.6. Review of Privacy Policy 16
13.2. Physical Security Measures 16
13.2.1. Security of the office 16
13.2.2. Format of data to be collected and stored 16
13.2.3. Paper-based/physical format 16
13.2.4. Digital/electronic format 16
13.2.5. Monitoring and limitation of access 16
13.2.6. Design of office space/work station 16
13.2.7. Responsibilities of the Persons involved in processing 17
13.2.8. Modes of transfer of personal data within the Company, to authorized recipients or to third parties via email or Fax technology 17
13.2.9. Disposal procedure 17
13.3. Technical Security Measures 17
13.3.1. Monitoring for security breaches 17
13.3.2. Security of the software/s and application/s used 17
14. DATA ACCURACY 18
15. DATA SUBJECTS RIGHTS 18
16. BREACH AND SECURITY INCIDENTS 19
16.1. Procedures in case of breach 19
16.2. Communication of the incident or breach to the Office of the Data Protection Commissioner 19
16.3. Communication of the incident or breach to the data subject 20

16.4. Measures to prevent and minimize occurrence of breach and security incidents 20
16.5. Recovery and restoration of personal data 20
16.6. Documentation of any personal data breach 21
17. INQUIRIES AND COMPLAINTS 21
17.1. Inquiries 21
17.2. Complaints 21
18. RECORDS 21
19. VALIDITY 22

1. POLICY STATEMENT

FINARTEL CAPITAL AIFLNP V.C.I.C. LTD ("Company", "We", "Our", "Us") intends to fully comply with all requirements of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, in so far as it affects is activities.

2. BACKGROUND

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

REGULATION (EU) 2016/679 protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

REGULATION (EU) 2016/679 applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

REGULATION (EU) 2016/679 applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

REGULATION (EU) 2016/679 applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behavior as far as their behavior takes place within the Union.

REGULATION (EU) 2016/679 applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

3. DEFINITIONS

Personal data: any information relating to an identified or identifiable natural person (**data subject**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring,

storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal data breach: 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.

4. INTRODUCTION

FINARTEL CAPITAL AIFLNP V.C.I.C. LTD needs to collect and use the personal data about its employees, clients and other individuals who come into contact with the Company. Specific, in relation to our clients and prospect clients, the Company processes their personal data in order to provide them with our services and for employees the Company processes their personal data in relation to the employment agreement.

In collecting and using this personal data, the Company is committed to protecting an individual's right to privacy with regard to the processing of personal data, therefore this Data Protection Policy ("Policy") is hereby adopted in compliance with REGULATION (EU) 2016/679 to support this commitment.

This Data Protection Policy ensures FINARTEL CAPITAL AIFLNP V.C.I.C. LTD:

- Complies with REGULATION (EU) 2016/679.
- Protects the rights of individuals related to the Company.
- Is open about how the Company collects, use, storage, access, discloses, transfers and destructs individual's data.
- Protects the Company from the risks of a data breach.

The Company respects and values your data privacy rights, and makes sure that all personal data collected from you are processed in adherence to the general principles of data protection as set out in the Regulation EU 2016/679. In accordance these principles, the personal data shall:

- Be processed lawfully, fairly and in a transparent manner;
- Be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Be accurate and, where necessary, kept up to date;
- Be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

- Be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

This Policy shall inform you of our organizational, physical and technical measures and procedures for data protection and may serve as your guide in exercising your rights under the REGULATION (EU) 2016/679.

5. SCOPE AND LIMITATION

All employees of the Company, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Policy.

This Policy applies to all data that the Company holds relating to identifiable individuals.

6. DATA PROTECTION RISKS

This Policy helps to minimize data security risks the Company is dealing with, including:

- Breach of confidentiality. For instance, accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
- Failing to comply with data subject' rights.
- Reputational damage. For instance, the Company could suffer if hackers successfully gained access to personal data.

7. RESPONSIBILITIES

In accordance the Regulation, the Company is the Controller of data subjects' personal data and responsible to implement the principles of the data protection and to demonstrate that processing is performed in accordance with the Regulation.

Everyone who works for or with the Company and processes personal data has some responsibility for ensuring that personal data is collected, handled and stored appropriately in accordance the Regulation.

However, the management of the Company is ultimately responsible for the oversight and implementation of this policy. In particular, the management has the following responsibilities:

- Review all data protection measures and procedures where necessary, when a processing activity is changed, when a new regulation for the protection of personal data has been issued and at least annually.

  Ensures that employees of the Company are aware of and abide by this policy.
- Arrange data protection training.
- Handling data protection questions from employees and anyone else covered by this Policy.
- Dealing with requests from individuals whom their personal data is under process by the Company, in accordance their rights as these are defined in REGULATION (EU) 2016/679.
- Checking and approving any contracts or agreements with third parties that may handle personal data processed by the Company.

- Ensure all systems and equipment used for storing data meet acceptable security standards.
- Ensures that the antivirus system is function properly.
- Approve any data protection statements attached to communications such as emails and letters.
- Ensure that any marketing activities abide by data protection principles.

8. GENERAL EMPLOYEES' GUIDELINES

Employees should keep all personal data secure, by taking sensible precautions. Employees should follow the policies and measures defined in this Policy and particular:

- Employees who will access data covered by this Policy should be those who need it for their work.
- All employees should attend training arranged by the Company to help them understand their responsibilities when process data.
- Should not disclose the personal data to unauthorized people, either within the Company or externally.
- Authorized employees should regularly review and update personal data the Company process, in accordance the Company's policy and legal obligations and should delete and destruct personal data that is no longer required, following the measures defined in this Policy.

9. SUBJECT TO CONSENT

The Company needs the consent of its clients to process their personal data in the case of:

- Processing the personal data of a client who is a child below the age of 14 years old therefore the consent is given or authorized by the holder of parental responsibility over the child.
- Processing of the personal data of a client related to special categories of personal data such as racial origin, political opinions, religious beliefs, genetic data, biometric data.
- Client's on-boarding is postponed
- A restriction has been obtained, under certain conditions, for the processing.
- A transfer of the personal data to a third country where the European Commission has not included this third country in the approved third countries or appropriate safeguards are not provided.

In such case that the processing is based on consent, the Company keeps evidences in order to be able to demonstrate that the processing is based on consent.

10. PROCESSING OF PERSONAL DATA

10.1. Collection

The lawfulness of collection and processing of personal data by the Company is based on:

The necessity to comply with its legal obligations,

- For the performance of a contract to which is a party or in order to take steps at the request of a prospective client prior to entering into a contract, and;
- For the Company's legitimate interests.

Where the Company intends to further process the personal data for a purpose other than that for which the personal data were collected, the Company will provide the data subject prior to that further processing with information on that other purpose and with any relevant further information.

10.1.1. Collection of personal data of clients

The Company collects sufficient evidences and information of clients and prospective clients for their identity verification process, subject to its legal obligations in accordance the Law L188(I)/2007 as amended and Directive D144-2007-08 of 2012, as amended, for the Prevention of Money Laundering and Terrorist Financing.

These evidences and information shall include:

- Telephone number, email address and fax number,
- Date and place of birth,
- Nationality,
- Certified and translated copy of passport or ID,
- Certified and translated copy of evidence for the full permanent, address, including postal code,
- Tax identification number,
- Profession reference,
- Bank account details,
- CV,
- Bank Reference,
- Information on profession or occupation,
- Name of employer,
- Information and evidences about his/her economic profile (Size of wealth, source of wealth, income source)
- Information and evidences about public positions the client and the prospective client holds or held in the last twelve months as well as whether the client and the prospective client is a close relative or associate of such individual.

Where the Company collects the personal data from the data subject, at the time of collection, the Company informs the client about:

a) the identity and the contact details of the Company;
b) the contact details of the data protection officer;
c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d) legitimate interests pursued by the Company or by a third party;
e) any recipients or categories of recipients of the personal data;
f) the possibility to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission;
g) the period for which the personal data will be stored;

h) the existence of the rights of data subject;
i) the right to lodge a complaint with a supervisory authority;
j) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
k) if exist automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The company will collect such information and evidences through the "Subscription Application Package". This Package shall:

- Be completed by customer physically - hard copy; or
- Be completed by customer electronically; or
- Be completed by an employee of the Company in communication with the customer.

In addition, the Company may collect additional personal data for its clients under its legal obligation, update personal data and other additional personal data under any new legal requirement the company is subject, as well as, personal data information not obtained from the data subject (e.g. open sources).

In case a prospective client has not become a client of the Company, the Company shall destroy any collected personal data. By derogation to this, in case a client's on-boarding is postponed, the Company shall keep client's personal data only when having client's prior consent.

10.1.2. Collection of personal data of employees

The Company collects personal data of its employees for the purpose of the employment in the Company. In this respect employees are responsible to keep the personal data accurate and up to date and inform the Company for any changes and for any errors in relation to the personal data they have provided.

10.1.3. Collection of personal data of other individuals

The Company may periodically collect personal data of other individuals such as from employment candidates. In such case, the process of the personal data shall be in accordance the Regulation and the principles of this Policy shall be implemented.

10.2. Use

The Company implements security measures as these are described in this Policy for the personal data in use.

10.2.1. Use of personal data of clients

Personal data collected shall be used by the company for potential client's identity verification process subject to its legal obligations under the Law L188(I)/2007 as amended and Directive DI144-2007-08 of 2012, as amended, and to decide for the start or not of a business relationship with the client.

The Company use the personal data of its clients in line its legal obligations.

10.2.2. Use of personal data of employees

The Company uses the personal data of employees only for the matter of employment.

10.2.3. Use of personal data of other individuals

The personal data collected from other individuals is in use by the Company for a specific purpose, such for example the use of personal data of employment candidates for the purpose of possible employment.

10.3. Storage of personal data

The Company ensures that personal data under its custody are protected against any accidental or

unlawful destruction, loss, alteration, unauthorized disclosure of, or access as well as against any other unlawful processing.

For the storage of personal data, the Company applies the physical security measures as these are described under the paragraph "12. SECURITY MEASURES AND POLICIES".

10.3.1. Personal Data kept physically/on Paper

Personal data kept on paper is stored in the office with 24/7 security alarm system and entrance video surveillance.

Employees handling personal data should make sure that printouts are not left unattended on the printer where unauthorized people could see them.

If personal data on paper is needed to be transported outside the Company's office, then it is transported in a locked car or by a messenger authorized by the client who is sending the personal data.

The Company does not create any unnecessary additional data sets.

If no longer needed, the Company uses a shredder to tear the personal data and related printouts and disposes them into a bin.

10.3.2. Personal data stored electronically

When personal data is stored electronically is protected from unauthorized access:

- By having in place passwords on each computer.
- From accidental deletion by having in place back up.
- From malicious hacking due to the fact that it is protected by antivirus programs.

Personal data is kept in files on computers of authorized persons and these files are protected by passwords.

In case personal data is needed to be kept on mobile devices (e.g. laptops), these mobile devices are protected through access only by the owners of the mobile devices with the use of passwords, codes and/or fingerprint. Files on mobile devices are secured by build-in antivirus tools.

If personal data is collected by email, this email is kept in a separate folder for each client accordingly, in order to be decided if the personal data to be kept or to be deleted. In case the Company decides to keep the personal data, then the personal data will be moved to files on the computers. In case the Company decides that the personal data is not needed, then it will be deleted. In any case the email containing personal data will be deleted after Company's relevant decision.

In case personal data is needed to be transferred through email, the relevant email is encrypted.

Personal data electronically stored is kept on G-Suite (cloud based suite of applications - Google). Access on G-Suite is secured by 2-step verification procedure. Data on G-suite is protected by Operational Security (Vulnerability Management, Malware Prevention, Monitoring & Incident Management).

The Company keeps a backup of the personal data that is in electronic format on G-Suite.

10.4. Access

Due to the sensitive and confidential nature of the personal data under the custody of the Company, only the data subject, the Company and the authorized recipients of the Company shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy or public order.

The reason of access personal data by the Company or its authorized recipients is for the normal business operations and the security measures and policies, as described in this Policy, are followed.

In relation to this Policy, authorized recipients includes any third party the Company has an agreement with in relation to the provision of the Company's services to Company's clients.

10.5. Disclosure

All employees, personnel and authorized recipients, shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations.

Personal data under the custody of the company shall be disclosed only pursuant to a lawful purpose and to authorized recipients of such data.

In case the Company will disclose your personal data, in the scope of Company's normal business operations, to a third party other than an authorized recipient, supervisory authority, for public policy or for public order, the Company will communicate with you through the email address you have provided to inform you for this fact, when the personal data will be first disclosed to the third party.

10.6. Transfer

Where the Company will transfer personal data to a third country or international organization, the Company will ensures that:

a) there is a decision by the Commission that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection; or
b) when there is an absence of a decision by the Commission as described above, the Company ensures that the transfer is take place on one of the following conditions:
    i. the data subject has been informed of the possible risks of such transfer and has explicitly consented to the proposed transfer,
    ii. the transfer is necessary for the performance of a contract between the data subject and the Company or the implementation of pre-contractual measures taken at the data subject's request,
    iii. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Company and another natural or legal person,
    iv. the transfer is necessary for important reasons of public interest,

v. the transfer is necessary for the establishment, exercise or defense of legal claims,
vi. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent,
vii. the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

In such case, the Company will keep documentation for the assessment of the condition applicable for the transfer.

10.7. Destruction

10.7.1. Hard copies

After the storage period, as defined below under the paragraph "10. FOR HOW LONG THE COMPANY KEEPS YOUR PERSONAL DATA", is ended, the Company uses a shredder to tear the personal data and related printouts and disposes them into a bin.

10.7.2. Electronically

Personal data kept on desktop, mobile devices files and G-Suite shall irretrievably be deleted along with any back up. "Recycle bin" is then cleared. Where mobile devices will not be used again, shall be physically destroyed.

11. FOR HOW LONG THE COMPANY KEEPS YOUR PERSONAL DATA

The Company will keep personal data for no longer that is necessary for the purposes for which the personal data are processed.

The Company will keep personal data of clients during the time of business relationship.

In accordance Company's legal obligations, at the time the business relationship of the Company with the Client terminates, the Company will keep client's personal data for a period of at least five (5) years, which is calculated after the termination of the business relationship. In case personal data is relevant to ongoing investigations by the Cyprus Unit for Combating Money Laundering (MOKAS), the personal data will be kept until MOKAS confirms that the investigation has been completed and the case has been closed.

The Company process personal data for the time period necessary to meet the purposes for which the personal data are processed, to comply with Company's legal obligations for the regulated services that provides, as well as, to comply with any tax issue purpose.

Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed following the procedures described under the paragraph "Destruction".

12. PROCESSING FOR OTHER REASON

The Company will ask to receive data subject's consent in any case will process data subject's personal data for a purpose other than that for which personal data have been collected.

13. SECURITY MEASURES AND POLICIES

When the personal data is accessed and used, it can be at a great risk of loss or theft, therefore the Company ensures the implementation of Organizational, Physical and Technical measures.

Organizational, Physical and Technical measures and policies within the organization shall be updated to remain consistent with current data privacy Regulation.

13.1 Organizational Security Measures and Policies

13.1.1. Data Protection Officer

The Company has designated the Data Protection Officer ("DPO") of the Company, as per the company structure.

Data subjects may contact the DPO at the email: compliance@finartel.fund in regards to all issues related to processing of their personal data and to the exercise of their rights.

The DPO is involved properly and in a timely manner, in all issues related to the protection of personal data which the Company processes.

The DPO has the necessary resources and access to personal data and processing operations in order to carry out her tasks.

The DPO is responsible to:

a) Keep the Company and employees of the Company who carry out processing, informed about their obligations pursuant to the Regulation and advise them accordingly,
b) To monitor the compliance of this Policy with the Regulation and other Union or Member State data protection provisions, as well as to assign responsibilities and train the employees involved in processing operations,
c) To provide advice where requested as regards the data protection impact assessment and monitor its performance,
d) To cooperate with the supervisory authority,
e) To act as the contact point for the supervisory authority on issues relating to processing of personal data.

13.1.2. Trainings and Seminars

For employees directly involved in the processing of personal data, Company ensures their attendance and participation in relevant trainings and orientations, as often as necessary.

13.1.3. Conduct of Privacy Impact Assessment

The Company shall conduct a Privacy Impact Assessment (PIA) (APPENDIX 1) relative to all activities, projects and systems involving the processing of personal data prior to a type of processing that in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of data subjects.

In such case, prior to the processing, the Company will carry out a PIA following the steps below:

a) Identify the need for the Data Protection Impact Assessment. In this step, the Company will determine whether the risks of the processing require undertaking a PIA.
b) Describe the information flow. In this step, the Company will describe how the information within this particular processing is collected, from whom it is obtained and to whom is disclosed, what information is used, who can access them, where to be stored, how to be deleted and any other necessary information.
c) Identify privacy and related risks. In this step, the Company will make a list of the range of threats, and their related vulnerabilities, to the rights and freedoms of individuals whose data is collected / processed. E.g. data breach and possible damage caused to the data subject, legal compliance risks and possible damages to the Company.
d) Identify and evaluate privacy solutions. In this step, the Company shall make a decision for each identified risk. E.g. whether to accept or reject the risk, whether to transfer it or take any other steps. The Company may accept some level of risk and the relative impact on the personal data privacy.
e) Make a conclusion and record the PIA outcomes. In this step, the Company shall summarize and keep a record of the outcomes of the above steps in a report. Report shall include also any steps to reduce the risks and any decisions taken. Where appropriate, the Company shall seek the views of data subjects.
f) Integrating the PIA outcomes back into the project processing plan. The Company will integrate in the project plan the findings and the actions of the assessment. The Company will apply this step by continually refer to the assessment in order to ensure that it is being followed and that its responses to the risks have been implemented effectively.

The Company will keep record of any Data Protection Impact Assessment taken for future processing projects.

13.1.4. Recording and documentation of processing activities carried out by the Company

The Company keeps records of processing activities for the personal data.

13.1.5. Duty of Confidentiality

All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

All employees of the Company signed an Employment Agreement that includes among others the clause "CONFIDENTIALITY".

Under this "CONFIDENTIALITY" clause, it is provided that during the term of an employee's employment with the Company, as well as, upon the termination of the employee's Employment Agreement, the employee shall keep in secret and shall not disclose to any third party, among others, data relevant to the client database of the Company.

13.1.6. Review of Privacy Policy

This Privacy Policy shall be reviewed, evaluated and updated where necessary and at least annually.

13.2. Physical Security Measures

13.2.1. Security of the office

The office is protected with 24/7 security alarm system and entrance video surveillance.

13.2.2. Format of data to be collected and stored

Personal data in the custody of this Company may be collected in paper-based/physical format and digital/electronic format.

13.2.3. Paper-based/physical format

Persona data collected in paper-based/physical format is kept in the office. The office is secured with 24/7 security alarm system and video surveillance.

In case the Company will transport personal data in paper-based/physical format, outside the Company's office, the personal data is transported in a locked car or by a messenger service authorized by the client or relevant third party.

13.2.4. Digital/electronic format

Devices in use to process personal data in digital/electronic format (pc, laptop, smartphone) are protected by antivirus systems. The antivirus systems in use are: for Windows the Bitdefender Antivirus, for MacBook Pro the Build-in anti-malware tool and for Smartphone the Build-in antivirus.

The owners of these devices have access only, with the use of passwords, codes and/or fingerprint.

Personal data kept on G-Suite is secured by 2-step verification procedure and protected by Operational Security (Vulnerability Management, Malware Prevention, Monitoring and Incident Management).

In case laptop devices will be used to transport personal data in digital/electronic format outside the Company's office, these devices are secured with passwords, codes and/or fingerprint and can only be accessed by the owners.

In case personal data in digital/electronic format will be transferred through files, these are transferred via G-Suite that is protected by operational security (Vulnerability Management, Malware Prevention, Monitoring & Incident Management).

In case personal data is sent through email, this email is encrypted.

13.2.5. Monitoring and limitation of access

Personal data is processed only by authorized persons, under the normal business operations.

13.2.6. Design of office space/work station

Computer screens are locked when left unattended.

Computer screens are placed in such way that cannot be viewed by other employees passing by.

No copies are left unattended on the desk or copy machine.

13.2.7. Responsibilities of the Persons involved in processing

Persons involved in processing shall always maintain confidentiality and integrity of personal data. These persons:

- Are not allowed to use their own gadgets or storage device when processing personal data.
- Shall ensure that screens of their computers are always locked when left unattended.
- In case they will send personal data in use by email, this email is encrypted in order to be viewed and be accessed only by the authorized receiver.
- Shall not disclose personal data to any other employee except with the authorisation of the management of the Company or in line with the Company's business operations.

13.2.8. Modes of transfer of personal data within the Company, to authorized recipients or to third parties via email or Fax technology

Transfers of personal data via email shall be done through an encrypted email including any or all attachments.

The Company does not use Fax machine to collect and/or send personal data.

13.2.9. Disposal procedure

The Company shall retain the personal data of a client for the period as defined under the paragraph "10. FOR HOW LONG THE COMPANY KEEPS YOUR PERSONAL DATA ". Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of in accordance the process described under the paragraph "Destruction".

13.3. Technical Security Measures

13.3.1. Monitoring for security breaches

Personal data is kept in electronic format and paper format, therefore the Company has implemented the following security measures to monitor for any breach.

a) For personal data kept in electronic format

For the security of personal data kept in electronic format, the Company uses the antivirus systems described under paragraph "12.2.4. Digital/electronic format" to monitor security breaches and alert the Company of any attempt to interrupt or disturb the system.

In case of an attempt of a breach, the antivirus system's alert appears on the screen of the device and a suspicious file is blocked from being opened or launched.

b) For personal data kept in paper format

For the security of personal data kept in paper format, the office of the Company is secured with 24/7 security alarm system and video surveillance.

13.3.2. Security of the software/s and application/s used

The Company first review and evaluate software applications before the installation thereof in computers and devices of the Company to ensure the compatibility of security features with overall operations.

14. DATA ACCURACY

The Regulation EU 2016/679 requires the Company to take reasonable steps to ensure personal data is kept accurate and up to date.

Employees who work with the personal data take reasonable steps to ensure it is kept as accurate and up to date as possible. Subject to our legal obligations we review the personal data we keep for each client.

The review is performed every one (1) year or four (4) years, in accordance the categorization of our clients. Evidence of the review is kept in the client's file.

Employees are responsible to inform the Company for any change of their personal data which the Company keeps in relation to their Employment status.

15. DATA SUBJECTS RIGHTS

All individuals who are the data subject of personal data held by the Company are entitled to the below rights as these are defined in Regulation EU 2016/679, unless these rights are subject to a restriction under the same Regulation:

- **Right of access.** You have the right to request a copy of your personal data which the Company holds about you. The Company will provide a copy of your personal data that is undergoing processing. For any further copies requested by you, the Company may charge a reasonable fee based on administrative costs.

You can send an email to compliance@finartel.fund asking for a copy (APPENDIX 2) of your personal data that is undergoing processing.

- **Right to rectification.** You have the right to request from the Company to rectify any inaccurate personal data concerning you.

You can send an email to compliance@finartel.fund asking for rectification. The Company will send you a supplementary form (APPENDIX 3) that you can fill and submit it.

- **Right to erasure.** You have the right, under certain circumstances as these are defined in the Regulation EU 2016/679, to obtain from the Company the erasure of your personal data.
- **Right to restriction of processing.** Where there is a dispute in relation to the accuracy or processing of your personal data, you have the right to request a restriction on further processing, in accordance GDPR Regulation EU 2016/679 provisions.

In case the processing of your personal data is restricted under the conditions defined in Regulation EU 2016/679, the Company, with the exception of storage, will only process your personal data under your consent or the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

The Company will inform you before the restriction will be lifted.

- **Right to data portability.** Where the processing is based on consent or on a contract and the processing is carried out by automated means, you have the right to receive the personal data and have the right to transmit those data to another controller.

- **Right to object.** Where applicable under the Regulation EU 2016/679, you have the right to object to the processing of your personal data.
- **Right not to be subject** to a decision based solely on automated processing, including profiling.

In case the Company will use automated processing, including profiling, for a decision concerning you, you have the right to obtain human intervention on the part of the Company, to express his or her point of view and to contest the decision.

- **Right to withdraw your consent.** Where the processing is based on your consent, you have the right to withdraw your consent at any time.

To withdraw your consent, send an email to compliance@finartel.fund asking to withdraw your consent.

- **Right to lodge a complaint** with the Personal Data Protection Commissioner's Office.

In such case, the Company asks the data subject in the first instance to contact FINARTEL CAPITAL AIFLNP V.C.I.C. LTD at the email compliance@finartel.fund. (APPENDIX 4)

For any type of inquiry or complaint, the Company may request the provision of additional information necessary to confirm the identity of the data subject who makes the request or complaint.

The Company shall provide information on action taken on a request of the data subjects in accordance their rights within one (1) month of receipt of the request. This period may be extended by two (2) further months where necessary, taking into account the complexity and number of the requests. The Company will inform the data subject of any such extension within one (1) month of receipt of the request, together with the reasons for the delay.

The Company will provide to the data subject the requested information by electronic means where possible.

The requested information will be provided free of charge. The company reserves the right to charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or refuse to act on the request, if in case your request is manifestly unfounded or excessive.

16. BREACH AND SECURITY INCIDENTS

Breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorized

disclosure of, or access to, personal data transmitted, stored or otherwise processed.

16.1. Procedures in case of breach

The Company is responsible for ensuring immediate action in the event of a security incident or personal data breach. The management shall asses the incident or breach in order to ascertain the nature and extent thereof.

16.2. Communication of the incident or breach to the Office of the Data Protection Commissioner

The Company shall assess the incident and if decide that personal data breach result in a risk to the rights and freedoms of natural persons, then shall notify the Office of the Data Protection Commissioner, (http://www.dataprotection.gov.cy) not later than 72 hours after having become aware of the breach. (APPENDIX 5)

If in case the Company is not able to send all the information included in the notification to the Commissioner at a first instance, then the company shall send the information in phases without undue delay.

16.3. Communication of the incident or breach to the data subject

The Company shall assess the incident and if decide that personal data breach result in a risk to the rights and freedoms of natural persons, then shall communicate the personal data breach to the data subject without undue delay. (APPENDIX 6)

During the assessing procedure of the incident, the Company may decide not to notify the data subject if any of the following conditions are met:

a) the company has applied appropriate technical and organizational protection measures to the personal data affected; (encryption)
b) the Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects affected from the breach is no longer likely to materialize;
c) the communication of the breach involve disproportionate effort. In such a case, the Company shall make a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

16.4. Measures to prevent and minimize occurrence of breach and security incidents

To minimize occurrence of breach and security incidents, the Company has in place technical security measures, as described in above paragraphs “12.3.1. Monitoring for security breaches”.

In case of an attempt of a breach, the antivirus system's alert appears on the screen of the device and a suspicious file is blocked from being opened or launched.

The office of the Company has a 24/7 security alarm system and entrance video surveillance.

16.5. Recovery and restoration of personal data

In some of the cases, personal data kept in paper format is also kept in electronic format.

In case of a breach incident concerning personal data in paper format, the Company may retrieve the affected personal data from the electronic files, where in the case that these personal data is also kept in electronic format.

The Company maintains a backup file on G-Suite for all personal data under its custody kept in electronic format.

In the event of a security incident or data breach, concerning personal data kept in electronic format, the Company shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

16.6. Documentation of any personal data breach

The Company prepares and keeps detailed documentation of every incident or breach encountered. The record that the Company keeps is a document comprising:

a) the facts relating to the personal data breach,
b) its effects, and;
c) the remedial action taken.

17. INQUIRIES AND COMPLAINTS

For any type of inquiry or complaint, the Company may request the provision of additional information necessary to confirm the identity of the data subject who makes the request or complaint.

The Company shall provide information in relation to the inquiry or complaint within one (1) month of receipt of the inquiry or complaint. That period may be extended by two (2) further months where necessary, taking into account the complexity and number of the inquiries or complaints. The Company shall inform the data subject of any such extension within one (1) month of receipt of the inquiry or complaint, together with the reasons for the delay.

The Company keeps records, in paper or electronic format, of requests and complaints and actions taken regarding the processing of data subjects' personal data, in the relevant data subject's file.

17.1. Inquiries

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the Company, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the Company at compliance@finartel.fund and briefly discuss the inquiry, together with their contact details for reference.

17.2. Complaints

In case of a complaint, the company asks the data subject in the first instance to contact FINARTEL CAPITAL AIFLNP V.C.I.C. LTD at the email compliance@finartel.fund. A complaint form will be sent to the data subject and asked to fill it.

The Company shall confirm to the complainant the receipt of the complaint form and the management of the Company shall examine the complaint form received and take the necessary actions within the time limits as described above.

18. RECORDS

The Company keeps records of processing activities for the personal data.

19. VALIDITY

The provisions of this Policy v.3.0. is considered as an ultimate part of Policy v.2.0. with immediate effect, until revoked or amended by the Company.

APPENDIX 1

Privacy Impact Assessment documentation

Data Protection Impact Assessment

FINARTEL CAPITAL AIFLNP V.C.I.C. LTD has decided, pursuant to Article 35(1) and 35(3) of the Regulation (EU) 2016/679 to carry, prior to the processing of ……., an assessment of the impact of the envisaged processing operations on the protection of personal data.

Privacy Impact Assessment (PIA) (in accordance Article 35(7) of the GDPR Regulation):

1) Description of the envisaged processing:

……

2) Purpose of the processing:

……

3) Does this specific processing require a PIA? (Reasons, Risks):

……

4) Legitimate interest of our Company:

……

5) Description of the information flow for the particular processing: (collection, from whom, to who will be disclosed, what kind of information, who can access them, where to be stored, how to be deleted and any other necessary information):

……

6) Necessity and proportionality of the processing operations in relation to the purposes:

……

7) Description of the risks to the rights and freedoms of data subjects affected (make a list of threats and vulnerabilities):

……

8) Description of the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned (decide whether to accept or reject the risk or any other steps to be taken):

……

Conclusion:

……

Decision taken or any steps to reduce the risks:

……

Integration (integration of the PIA outcomes into the project processing plan to ensure that it is being followed and that its responses to the risks have been implemented effectively):

……

APPENDIX 2

Form "Access to personal data"

Personal Data the FINARTEL CAPITAL AIFLNP V.C.I.C. LTD keeps for data subject

(Right to access)

Name:……..

Purpose of Processing	Categories of personal data	To whom these data is disclosed or will be disclosed	For how long will be kept	Source	Exist automated decision making

FINARTEL CAPITAL AIFLNP V.C.I.C. LTD ("Company") would like to inform you that keep the above data, for the purpose and time as defined above.

In accordance Article 15 of the Regulation (EU) 2016/679, you have the right to:

a) Request from the Company rectification or erasure of personal data or restriction of processing of personal data concerning you or to object to such processing.

b) Lodge a complaint with the competent supervisory authority.

Your rights are subject to restrictions as defined in Article 23 of the Regulation (EU) 2016/679.

APPENDIX 3

Supplementary Statement for the rectification of inaccurate data

Upon you request dated ..... received by ..... to rectify your personal data that FINARTEL CAPITAL AIFLNP V.C.I.C. LTD is processing and in accordance your right under the Article 16 of Regulation (EU) 2016/679, FINARTEL CAPITAL AIFLNP V.C.I.C. LTD asks you to inform us about your personal data your have requested to rectify.

Please fill the below boxes accordingly:

Current Personal Data	Personal Data to be changed to:

FINARTEL CAPITAL AIFLNP V.C.I.C. LTD would like to inform you that we will review your request, proceed accordingly subject to any restriction exist under the Article 23 of the Regulation (EU) 2016/679 and inform you the latest within one (1) month from the date of receipt your request (we will let you know in case we need more time).

For FINARTEL CAPITAL AIFLNP V.C.I.C. LTD

.....

Date

.....

APPENDIX 4

Complaint Form in relation to Personal Data

FINARTEL CAPITAL AIFLNP V.C.I.C. LTD ("Company") asks you to submit in details in the below box your complaint in regards the processing of your personal data: (please fill the box electronically and send it by email to compliance@finartel.fund)

Your name: .....

Date: .....

Complaint:
.....
.....
.....
.....

For Company use:

Action / Recommendation:

.....

.....

For FINARTEL CAPITAL AIFLNP V.C.I.C. LTD:

.....

Date:

.....

APPENDIX 5

Notification of a personal data breach to Cyprus Competent Authority

Notification of a personal data breach

Address to:

The Office of Data Protection Commissioner
Email: commissioner@dataprotection.gov.cy
Tel: 22818456, Fax: 22304565

FINARTEL CAPITAL AIFLNP V.C.I.C. LTD ("Company") informs you that on ..... the Company has suffered a breach concerning the personal data the Company process.

Please find below details of the breach:

1) The breach (description):

.....

2) Categories of personal data affected:

.....

3) Number of data subjects affected (or approximate number):

.....

4) Number of records affected (or approximate number):

.....

5) Company's Contact point:

.....

6) Consequences of the personal data breach:

.....

7) Measures taken or proposed to be taken:

.....

8) Reason for not submitting the notification within 72 hours of the incident:

.....

For FINARTEL CAPITAL AIFLNP V.C.I.C. LTD

.....

Date:

.....

APPENDIX 6

Notification of a personal data breach to a data subject

Notification of a personal data breach

Address to (Data Subject):
Name: .....
Email: .....
Tel: .....
Fax: .....

FINARTEL CAPITAL AIFLNP V.C.I.C. LTD ("Company") informs you that on ..... the Company has suffered a breach concerning the personal data the Company process. The breach has affected your personal data the Company process.

Please find below details of the breach:

1) Description of The breach:
.....

2) Company's Contact point:
.....

3) Consequences of the personal data breach:
.....

4) Measures taken or proposed to be taken:
.....

For FINARTEL CAPITAL AIFLNP V.C.I.C. LTD

.....

Date:

.....