FINARTEL CAPITAL VCIC LTD

ПОЛИТИКА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

РЕДАКЦИЯ 2

ОКТЯБРЬ 2019 ГОДА

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

+357 25 057 150

hq@finartel.fund

Номер лицензии, выданной Кипрской комиссией по ценным бумагам и биржам: LPAIF114/2014

FINARTEL

Содержание

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

+357 25 057 150

hq@finartel.fund

FINARTEL

1. ДЕКЛАРАЦИЯ

FINARTEL CAPITAL VCIC LTD (далее — «Компания», «мы», «нас», «нам», «нами», «наш») настоящим выражает намерение в полной мере соблюдать все требования РЕГЛАМЕНТА (ЕС) 2016/679 ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА ЕВРОПЕЙСКОГО СОЮЗА от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных в той мере, в которой действие указанного регламента распространяется на деятельность Компании.

2. ОБЩИЕ СВЕДЕНИЯ

В РЕГЛАМЕНТЕ (ЕС) 2016/679 ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА ЕВРОПЕЙСКОГО СОЮЗА от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных устанавливаются правила защиты физических лиц при обработке персональных данных, а также правила свободного перемещения персональных данных.

РЕГЛАМЕНТОМ (ЕС) 2016/679 предусматривается защита фундаментальных прав и свобод физических лиц, в частности их права на защиту персональных данных.

РЕГЛАМЕНТ (ЕС) 2016/679 применяется к обработке персональных данных, осуществляемой полностью или частично с использованием автоматизированных средств, а также к неавтоматизированной обработке персональных данных, являющихся частью системы регистрации и хранения документов либо предназначенных для того, чтобы стать частью системы регистрации и хранения документов.

РЕГЛАМЕНТ (ЕС) 2016/679 распространяется на обработку персональных данных при условии организации в ЕС деятельности контролера или лица, осуществляющего обработку данных, независимо от того, производится ли обработка данных непосредственно на территории ЕС.

РЕГЛАМЕНТ (ЕС) 2016/679 применяется в отношении обработки персональных данных субъектов данных, находящихся в ЕС, контролером или лицом, осуществляющим обработку данных, не имеющим присутствия в ЕС, если процессы обработки данных касаются:

(a) предложения товаров и услуг субъектам данных, находящимся в ЕС, независимо от того, требуется ли от них оплата; или

(b) мониторинга поведения субъектов данных в случаях, когда действия совершаются ими в ЕС.

РЕГЛАМЕНТ (ЕС) 2016/679 применяется в отношении обработки персональных данных, осуществляемой контролером, не имеющим присутствия в ЕС, а в юрисдикции, где согласно международному публичному праву действует право государств-членов ЕС.

3. ОПРЕДЕЛЕНИЯ

Персональные данные — любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (далее — «**Субъект данных**»); идентифицируемое физическое лицо — это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством таких идентификаторов, как имя, идентификационный номер, сведения о местонахождении, сетевой идентификатор в режиме онлайн, или через один или несколько признаков, характерных для физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности такого физического лица.

Обработка — любая операция или набор операций, осуществляемых с персональными данными или наборами персональных данных с применением автоматизированных средств или без таковых, включая сбор, запись, организацию, структурирование, хранение, модификацию или изменение, извлечение, просмотр, использование, раскрытие посредством передачи, распространение или предоставление иным способом, упорядочение или комбинирование, ограничение, стирание или уничтожение.

Контролер — физическое или юридическое лицо, орган государственной власти, учреждение или другой орган, который самостоятельно или совместно с другими лицами определяет цели и способы обработки персональных данных; контролер или определенные критерии для его назначения могут быть установлены законодательством ЕС или Государства-члена ЕС в случаях, когда цели и способы указанной обработки определены законодательством ЕС или Государства-члена ЕС.

Согласие субъекта данных — добровольное, конкретное, информированное и однозначное волеизъявление, посредством которого субъект данных в форме заявления или четкого утвердительного действия дает согласие на обработку относящихся к нему персональных данных.

Утечка персональных данных — нарушение безопасности, ведущее к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию персональных данных, являющихся объектом передачи, хранения или обработки иным способом, или к несанкционированному доступу к таким данным.

4. ВСТУПЛЕНИЕ

В рамках своей деятельности FINARTEL CAPITAL VCIC LTD признает необходимость сбора и использования персональных данных своих сотрудников, клиентов и прочих физических лиц, обращающихся в Компанию. В частности, в отношении клиентов и потенциальных клиентов Компания обрабатывает персональные данные с целью оказания им услуг, а в отношении сотрудников Компания обрабатывает персональные данные в связи с заключением трудового договора.

При сборе и использовании указанных персональных данных Компания обязуется защищать право физического лица на неприкосновенность частной жизни в связи с обработкой персональных данных, и с учетом такого обязательства принимается настоящая Политика защиты данных (далее — «Политика») в соответствии с требованиями РЕГЛАМЕНТА (ЕС) 2016/679.

Настоящая Политика защиты данных призвана обеспечить со стороны FINARTEL CAPITAL VCIC LTD:

- соблюдение РЕГЛАМЕНТА (ЕС) 2016/679;
- защиту прав физических лиц, связанных с Компанией;
- прозрачность сбора, использования, хранения, предоставления доступа, раскрытия, передачи и уничтожения Компанией данных физических лиц;
- защиту Компании от рисков нарушения безопасности персональных данных.

Компания уважает и ценит права физических лиц на конфиденциальность данных, а также обеспечивает обработку всех полученных персональных данных в соответствии с общими принципами защиты данных, изложенными в Регламенте ЕС 2016/679. В соответствии с указанными принципами персональные данные должны:

- обрабатываться законным, справедливым и прозрачным образом;
- собираться для четко указанных, конкретных и законных целей и не подвергаться дальнейшей обработке не совместимым с этими целями способом;
- соответствовать заявленным целям обработки, учитывать и включать только те сведения, которые необходимы для таких целей;
- являться точными и при необходимости поддерживаться в актуальном состоянии;
- храниться в форме, которая позволяет идентифицировать субъектов данных не дольше, чем того требуют цели обработки персональных данных;

- обрабатываться способом, обеспечивающим соответствующую безопасность персональных данных, включая защиту от несанкционированной или незаконной обработки, а также от случайной потери, уничтожения или повреждения.

Настоящая Политика предназначена для информирования о наших организационных, физических и технических мерах, а также процедурах защиты данных и может служить руководством при осуществлении прав физических лиц в соответствии с РЕГЛАМЕНТОМ (ЕС) 2016/679.

5. СФЕРА ПРИМЕНЕНИЯ И ОГРАНИЧЕНИЯ

Независимо от вида трудовой деятельности или типа договорных отношений с Компанией все сотрудники Компании обязаны соблюдать положения настоящей Политики.

Действие настоящей Политики распространяется на все данные, которые получены Компанией в отношении идентифицируемых физических лиц.

6. РИСКИ В ОБЛАСТИ ЗАЩИТЫ ДАННЫХ

Настоящая Политика позволяет минимизировать риски в области безопасности данных, с которыми сталкивается Компания, в том числе:

- нарушение конфиденциальности, например, случайное или незаконное уничтожение, потеря, изменение, несанкционированное раскрытие персональных данных, являющихся объектом передачи, хранения или обработки иным способом, или несанкционированный доступ к таким данным;
- несоблюдение прав субъекта данных;
- ущерб деловой репутации. Например, репутация Компании может пострадать, если злоумышленникам удастся получить доступ к персональным данным.

7. ОБЯЗАННОСТИ

В соответствии с Регламентом Компания является Контролером персональных данных субъектов данных и отвечает за реализацию принципов защиты данных, а также за подтверждение того, что обработка осуществляется в соответствии с Регламентом.

Каждое лицо, работающее в Компании или сотрудничающее с ней, которое осуществляет обработку персональных данных, несет определенную ответственность за организацию надлежащего процесса сбора, обработки и хранения персональных данных в соответствии с Регламентом.

Однако в конечном счете ответственность за контроль и реализацию настоящей Политики несет руководство Компании. В частности, обязанности руководства состоят в следующем:

- пересмотр (при необходимости) всех мер и процедур защиты персональных данных в случае изменения принципов деятельности по обработке или издания нового регламента защиты персональных данных, но в любом случае не реже одного раза в год;

  организация процесса информирования сотрудников Компании о настоящей Политике, а также обеспечение соблюдения ими настоящей Политики;
- проведение обучения в области защиты данных;
- решение вопросов защиты данных, возникающих у сотрудников и любых других лиц, подпадающих под действие настоящей Политики;
- работа с запросами физических лиц, чьи персональные данные обрабатываются Компанией, в соответствии с их правами, определенными РЕГЛАМЕНТОМ (ЕС) 2016/679;
- проверка и утверждение любых договоров или соглашений с третьими лицами, которые могут производить какие-либо действия с персональными данными, обрабатываемыми Компанией;

- обеспечение соответствия всех систем и оборудования, используемых для хранения данных, приемлемым стандартам безопасности;
- обеспечение надлежащего функционирования систем антивирусной защиты;
- утверждение текста любых заявлений в отношении защиты данных, прилагаемых к сообщениям, таким как электронные и обычные письма;
- обеспечение соответствия любой маркетинговой деятельности принципам защиты данных.

8. ОБЩИЕ УКАЗАНИЯ ДЛЯ СОТРУДНИКОВ

Сотрудники обязаны сохранять безопасность всех персональных данных, принимая для этого разумные меры предосторожности. Сотрудники обязаны следовать процедурам и мерам, определенным в настоящей Политике, в частности:

- доступ к данным, подпадающим под действие настоящей Политики, могут иметь только те сотрудники, которым такой доступ необходим для выполнения своих рабочих обязанностей;
- все сотрудники должны пройти обучение, организованное Компанией, в целях получения четкого представления о своих обязанностях при обработке данных;
- сотрудники не должны раскрывать персональные данные лицам, не имеющим соответствующих полномочий, как в рамках Компании, так и за ее пределами;
- уполномоченные сотрудники должны регулярно просматривать и обновлять персональные данные, обрабатываемые Компанией, в соответствии с принципами Политики и установленными законом обязанностями Компании, а также удалять и уничтожать персональные данные, в которых больше нет необходимости, согласно мерам, определенным в настоящей Политике.

9. НЕОБХОДИМОСТЬ ПОЛУЧЕНИЯ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Компании требуется согласие клиентов на обработку персональных данных в следующих случаях:

- обработка персональных данных осуществляется в отношении клиента, являющегося ребенком в возрасте до 14 лет, причем в таком случае согласие предоставляется или обработка данных разрешается лицом, на которое возложена родительская ответственность за такого ребенка;
- обработка персональных данных клиента связана с особыми категориями персональных данных, такими как расовое происхождение, политические убеждения, религиозные убеждения, генетические данные, биометрические данные;
- заключение клиентского соглашения откладывается;
- при определенных условиях было получено ограничение на обработку;
- передача персональных данных осуществляется в третью страну, причем такая третья страна не включена Европейской комиссией в список утвержденных третьих стран или не предусмотрены соответствующие гарантии.

Если для обработки данных требуется получить согласие клиента, то Компания хранит документальное подтверждение такого согласия для предъявления в случае необходимости.

10. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Сбор данных

Законность сбора и обработки персональных данных Компанией основывается на следующем:

необходимость выполнения Компанией установленных законом обязанностей;
- в целях исполнения договора, стороной которого является Компания, или в целях принятия соответствующих мер по просьбе потенциального клиента до заключения договора; а также
- в законных интересах Компании.

Если Компания намеревается осуществить дополнительные процедуры по обработке персональных данных в целях, отличных от тех, для которых такие персональные данные были собраны, то до проведения такой дополнительной обработки Компания предоставляет субъекту данных информацию о другой цели обработки данных и любую сопутствующую информацию в связи с этим.

10.1.1. Сбор персональных данных клиентов

Компания собирает документально подтвержденную информацию о клиентах, в том числе потенциальных, для проверки их личности с учетом законодательно установленных обязанностей по Противодействию отмыванию доходов, полученных преступным путем, и финансированию терроризма в соответствии с Законом L188 (I)/2007 с изменениями и дополнениями и Директивой D144-2007-08 от 2012 года с изменениями и дополнениями.

Указанные сведения включают в себя:

- номер телефона, адрес электронной почты и номер факса;
- дату и место рождения;
- национальность;
- заверенную и переведенную копию паспорта или удостоверения личности;
- заверенную и переведенную копию свидетельства о постоянном месте жительства с указанием полного адреса, включая почтовый индекс;
- идентификационный номер налогоплательщика;
- подтверждение рода деятельности;
- реквизиты банковского счета;
- резюме;
- справку из банка;
- информацию о профессии или роде занятий;
- наименование работодателя;
- документально подтвержденную информацию о финансовом положении (о размере состояния, источнике состояния, источнике дохода);
- документально подтвержденную информацию о должностях в органах государственной власти, которые клиент, в том числе потенциальный, занимает или занимал в течение последних двенадцати месяцев, а также о том, является ли клиент, в том числе потенциальный, близким родственником или партнером лица, занимающего такую должность.

Если Компания получает персональные данные непосредственно от субъекта данных, то в момент сбора таких данных Компания информирует клиента о следующем:

a) наименование и контактные данные Компании;
b) контактные данные лица, ответственного за защиту персональных данных;
c) цели обработки персональных данных, а также установленные законом основания их обработки;
d) законные цели, преследуемые Компанией или третьими лицами при обработке персональных данных;
e) получатели или категории получателей персональных данных;
f) возможность передачи персональных данных в третью страну или международную организацию и наличие или отсутствие соответствующего решения Комиссии;
g) срок хранения персональных данных;
h) наличие прав у субъекта данных;
i) право на подачу жалобы в надзорный орган;
j) является ли предоставление персональных данных законодательным или договорным требованием либо необходимым условием для заключения договора, а также обязан ли субъект

данных предоставлять персональные данные и каковы возможные последствия непредоставления таких данных;

k) существование автоматизированного порядка принятия решений, включая формирование профиля и содержательную информацию о логике такого принятия решений, а также о значимости и предполагаемых последствиях такой обработки для субъекта данных.

Компания будет собирать такую документально подтвержденную информацию через «Форму заявки на оказание услуг». Указанная Форма:

- заполняется клиентом на физическом носителе; или
- заполняется клиентом в электронной форме; или
- заполняется сотрудником Компании в процессе общения с клиентом.

Кроме того, Компания может собирать дополнительные персональные данные клиентов в соответствии со своими законодательно установленными обязанностями, обновлять персональные данные и дополнительные персональные данные в соответствии с любыми новыми требованиями законодательства, действие которых распространяется на Компанию, а также находить (например, в открытых источниках) информацию о персональных данных, не полученных от субъекта данных.

Если потенциальный клиент не становится клиентом Компании, то Компания обязуется уничтожить все собранные персональные данные. В отступление от этого, если заключение клиентского соглашения откладывается, то Компания сохраняет персональные данные клиента исключительно при наличии предварительного согласия клиента.

10.1.2. Сбор персональных данных сотрудников

Компания собирает персональные данные своих сотрудников с целью регулирования трудовых отношений с ними. В связи с этим сотрудники несут ответственность за поддержание достоверности и актуальности персональных данных, а также информирование Компании о любых изменениях и ошибках в отношении предоставленных ими персональных данных.

10.1.3. Сбор персональных данных прочих физических лиц

Компания может периодически собирать персональные данные других физических лиц, например кандидатов на трудоустройство. В таком случае процесс обработки персональных данных осуществляется в соответствии с требованиями Регламента и принципами настоящей Политики.

10.2. Использование данных

В отношении используемых персональных данных Компания применяет меры безопасности, предусмотренные настоящей Политикой.

10.2.1. Использование персональных данных клиентов

Собранные персональные данные используются Компанией для проверки личности потенциального клиента в соответствии с законодательно установленными обязанностями Компании согласно Закону L188(I)/2007 с изменениями и дополнениями и Директиве DI144-2007-08 от 2012 года с изменениями и дополнениями, а также для принятия решения о начале или прекращении деловых отношений с клиентом.

Компания использует персональные данные клиентов в соответствии со своими установленными законом обязанностями.

10.2.2. Использование персональных данных сотрудников

Компания использует персональные данные сотрудников исключительно в целях регулирования трудовых отношений с ними.

10.2.3. Использование персональных данных прочих физических лиц

Персональные данные, собранные от прочих физических лиц, применяются Компанией в определенных

целях, например использование персональных данных кандидатов на работу в Компании с целью возможного трудоустройства.

10.3. Хранение персональных данных

Компания обеспечивает защиту персональных данных, находящихся в ее распоряжении, от любого случайного или

незаконного уничтожения, потери, изменения, несанкционированного раскрытия персональных данных, являющихся объектом передачи, хранения или обработки иным способом, или несанкционированного доступа к таким данным.

При хранении персональных данных Компания применяет меры физической безопасности, предусмотренные в пункте 12. «МЕРЫ И ПРАВИЛА БЕЗОПАСНОСТИ».

10.3.1. Хранение персональных данных на физическом носителе (на бумажном носителе)

Персональные данные на бумажном носителе хранятся в офисе с круглосуточной охранной сигнализацией и системой видеонаблюдения за входами.

Сотрудники, занимающиеся обработкой персональных данных, должны обеспечить, чтобы распечатки не оставались без присмотра на принтере, где их могут увидеть посторонние.

Если персональные данные на бумажном носителе необходимо перевезти за пределы офиса Компании, то перевозка осуществляется в автомобиле, оснащенном блокировкой дверей, или курьерской службой, утвержденной клиентом, отправляющим персональные данные.

Компания не создает без необходимости дополнительных наборов данных.

Персональные данные на бумажном носителе и связанные с ними распечатки, в дальнейшем хранении которых нет необходимости, уничтожаются Компанией в шредере и выбрасываются.

10.3.2. Хранение персональных данных на электронном носителе

При хранении персональных данных на электронном носителе защита от несанкционированного доступа обеспечивается следующим образом:

- на каждом компьютере устанавливается пароль;
- для защиты от случайного удаления осуществляется резервное копирование;
- для защиты от преднамеренного взлома устанавливаются антивирусные программы.

Персональные данные хранятся в файлах на компьютерах уполномоченных лиц, причем такие файлы защищены паролями.

В случае необходимости хранения персональных данных на мобильных устройствах (например, ноутбуках) такие мобильные устройства защищаются посредством предоставления доступа исключительно владельцам мобильных устройств с использованием паролей, кодов и (или) отпечатков пальцев. Файлы на мобильных устройствах защищены встроенными средствами антивирусной защиты.

Если персональные данные собираются посредством электронной почты, то электронные письма хранятся соответственно в отдельной папке по каждому клиенту до принятия решения о том, будут ли персональные данные сохранены или удалены. Если Компания придет к выводу о том, что хранение персональных данных является целесообразным, они будут перемещены в файлы на компьютерах. Если Компания примет решение, что в хранении персональных данных больше нет необходимости, они будут удалены. В любом случае после принятия Компанией соответствующего решения электронное письмо, содержащее персональные данные, будет удалено.

В случае необходимости передачи персональных данных по электронной почте соответствующие электронные письма подвергаются шифрованию.

Персональные данные в электронном виде хранятся в G Suite (пакет бизнес-приложений на базе технологий Google с возможностью совместной работы в облаке). Доступ к G Suite обеспечивается посредством двухэтапной аутентификации. Данные в G Suite защищены Средствами операционной безопасности (управления уязвимостями, предотвращения установки вредоносного программного обеспечения, контроля и урегулирования инцидентов).

Компания осуществляет резервное копирование персональных данных, которые хранятся в электронном формате в G Suite.

10.4. Доступ к данным

В связи с личным и конфиденциальным характером находящихся на хранении Компании персональных данных доступ к таким персональным данным могут получить только субъект данных, Компания и уполномоченные получатели данных Компании в любых целях, за исключением противоречащих требованиям законодательства, принципам государственной политики или нормам общественного порядка.

Доступ к персональным данным со стороны Компании или ее уполномоченных получателей данных необходим в рамках обычных деловых операций Компании, при этом обеспечивается соблюдение процедур и мер безопасности, предусмотренных настоящей Политикой.

Для целей настоящей Политики уполномоченными получателями данных являются любые третьи лица, с которыми Компания имеет соглашение в связи с оказанием услуг Компании клиентам Компании.

10.5. Раскрытие данных

Все сотрудники, персонал и уполномоченные получатели данных обязаны сохранять конфиденциальность и секретность всех персональных данных, которые становятся им доступны и находятся в их распоряжении, даже после увольнения, расторжения договора или прекращения других договорных отношений.

Персональные данные, находящиеся в распоряжении Компании, раскрываются исключительно в соответствии с законодательно установленной целью и только уполномоченным получателям таких данных.

Если Компании будет необходимо раскрыть ваши персональные данные в рамках обычных деловых операций Компании какому-либо третьему лицу, кроме уполномоченного получателя, надзорного органа, а также кроме как в целях соблюдения принципов государственной политики или общественного порядка, то при первоначальном раскрытии персональных данных такому третьему лицу Компания уведомит вас об этом путем направления письма на предоставленный адрес электронной почты.

10.6. Передача данных

В случае передачи Компанией персональных данных в третью страну или международную организацию Компания гарантирует следующее:

a) наличие решения Комиссии о том, что такая третья страна, территория, один или несколько конкретных секторов в пределах такой третьей страны, соответствующая международная организация обеспечивают надлежащий уровень защиты; или
b) при отсутствии описанного выше решения Комиссии Компания осуществляет передачу данных только при соблюдении одного из следующих условий:
    i. субъект данных проинформирован о возможных рисках такой передачи данных и предоставил свое явное согласие на предполагаемую передачу;
    ii. передача данных необходима для исполнения договора между субъектом данных и Компанией или для осуществления преддоговорных мер по запросу субъекта данных;
    iii. передача данных необходима для заключения или исполнения договора, заключенного в интересах субъекта данных между Компанией и другим физическим или юридическим лицом;
    iv. передача данных необходима по существенным причинам, представляющим общественный интерес;

v. передача данных необходима для установления, осуществления или защиты правовых требований;
vi. передача данных необходима для защиты жизненно важных интересов субъекта данных или других лиц, если субъект данных физически или юридически не способен дать согласие;
vii. передача данных производится из реестра, который в соответствии с законодательством ЕС или Государства-члена ЕС предназначен для предоставления информации общественности и находится в свободном доступе для получения информации общественностью в целом или любым лицом, которое может продемонстрировать доказательства законности своей заинтересованности, но только в той мере, в какой в каждом конкретном случае выполняются условия, установленные законодательством ЕС или Государства-члена ЕС в отношении получения информации.

В таком случае Компания хранит документацию, подтверждающую соблюдение условий, необходимых для передачи данных.

10.7. Уничтожение данных

10.7.1. Физические носители

По окончании срока хранения согласно пункту 10. «СРОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ КОМПАНИЕЙ» персональные данные на бумажном носителе и связанные с ними распечатки уничтожаются Компанией в шредере и выбрасываются.

10.7.2. Электронные носители

Персональные данные, хранящиеся в файлах стационарных компьютеров, мобильных устройств и G Suite, безвозвратно удаляются, включая все резервные копии. Затем производится очищение «Корзины». Мобильные устройства, которые больше не будут использоваться, также уничтожаются посредством применения методик физического разрушения.

11. СРОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ КОМПАНИЕЙ

Компания хранит персональные данные не дольше, чем это необходимо для достижения целей обработки таких данных.

Компания хранит персональные данные клиентов в течение всего периода деловых отношений.

В соответствии с обязанностями, возложенными на Компанию законодательством, после прекращения деловых отношений с клиентом Компания хранит персональные данные клиента не менее 5 (пяти) лет с момента прекращения деловых отношений. Если персональные данные имеют отношение к текущим расследованиям Кипрского подразделения по борьбе с отмыванием денег (MOKAS), то персональные данные хранятся до тех пор, пока MOKAS не подтвердит, что расследование завершено и дело закрыто.

Компания обрабатывает персональные данные в течение срока, необходимого для достижения целей обработки персональных данных, для соблюдения установленных законом обязательств Компании по оказанию услуг, подлежащих регулированию, а также для выполнения любых задач, связанных с налогообложением.

По истечении этого срока все физические и электронные копии персональных данных подлежат уничтожению в соответствии с процедурами, описанными в пункте «Уничтожение».

12. ОБРАБОТКА ПО ИНОЙ ПРИЧИНЕ

При возникновении необходимости обработки персональных данных субъекта данных по причине, отличной от первоначальной причины сбора персональных данных, Компания запрашивает согласие субъекта данных.

13. МЕРЫ И ПРАВИЛА БЕЗОПАСНОСТИ

В процессе осуществления доступа к персональным данным и их использования может возникнуть высокий риск их потери или кражи, в связи с чем Компания гарантирует принятие организационных, физических и технических мер.

Организационные, физические и технические меры, а также правила, применяемые в организации, актуализируются в целях обеспечения постоянного соответствия действующей редакции Регламента по неприкосновенности данных.

13.1 Организационные меры и правила безопасности

13.1.1. Лицо, ответственное за защиту персональных данных

Согласно своей организационной структуре Компания назначила Лицо, ответственное за защиту персональных данных в Компании.

В отношении всех вопросов обработки персональных данных и осуществления своих прав субъекты данных могут связаться с Лицом, ответственным за защиту персональных данных в Компании, по электронной почте: compliance@finartel.fund.

Лицо, ответственное за защиту персональных данных в Компании, надлежащим образом и своевременно участвует в решении всех вопросов защиты обрабатываемых Компанией персональных данных.

Для выполнения соответствующих задач Лицу, ответственному за защиту персональных данных в Компании, предоставлены необходимые ресурсы и возможности доступа к персональным данным и операциям по их обработке.

В обязанности Лица, ответственного за защиту персональных данных в Компании, входит:

a) информирование Компании и сотрудников Компании, осуществляющих обработку данных, об их обязательствах согласно Регламенту и их консультирование по соответствующим вопросам;
b) контроль соответствия настоящей Политики Регламенту и иным нормам Союза или Государства-члена в области защиты данных, а также закрепление обязанностей и обучение сотрудников, участвующих в операциях по обработке;
c) консультирование (по требованию) по проведению оценки воздействия на защиту данных и текущий контроль ее осуществления;
d) оказание содействия надзорному органу;
e) исполнение роли контактного лица надзорного органа по вопросам обработки персональных данных.

13.1.2. Тренинги и семинары

Компания обеспечивает присутствие и участие сотрудников, непосредственно задействованных в обработке персональных данных, в соответствующих тренингах и инструктажах с необходимой периодичностью.

FINARTEL

13.1.3. Выполнение оценки воздействия на неприкосновенность частной жизни

Компания выполняет Оценку воздействия на неприкосновенность частной жизни (ПРИЛОЖЕНИЕ 1) всех мероприятий, проектов и систем, предполагающих обработку персональных данных, перед осуществлением обработки, которая, в частности, предусматривает использование новых технологий (с учетом характера, объема, контекста и целей обработки) и, скорее всего, может представлять высокий риск для прав и свобод субъектов данных.

В таком случае перед проведением процедур обработки данных Компания выполняет Оценку воздействия на неприкосновенность частной жизни, которая включает следующие этапы:

a) определение необходимости Оценки воздействия на защиту данных. На этом этапе Компания устанавливает, требуют ли риски обработки выполнения Оценки воздействия на неприкосновенность частной жизни;
b) описание информационного потока. На этом этапе Компания описывает, как будет осуществляться сбор информации в рамках данной конкретной процедуры обработки, у кого ее получают и кому раскрывают, какая информация используется, кто может получить к ней доступ, где она должна храниться, как должна удаляться, а также любые другие необходимые сведения;
c) определение рисков нарушения неприкосновенности частной жизни и связанных с ними рисков. На этом этапе Компания составляет список угроз и соответствующих факторов уязвимости для прав и свобод лиц, чьи данные собирают (обрабатывают). Например, нарушение безопасности данных и ущерб, который может быть причинен субъекту данных, риски несоблюдения правовых норм, а также ущерб, который может быть причинен Компании;
d) определение и оценка решений в области неприкосновенности частной жизни. На этом этапе Компания принимает решение по каждому выявленному риску. Например, решение о том, принять или не принять риск, передать риск или предпринять иные шаги. Компания может принять определенный уровень риска и относительное воздействие на неприкосновенность персональных данных;
e) формулирование вывода и фиксация результатов Оценки воздействия на неприкосновенность частной жизни. На этом этапе Компания обобщает и фиксирует результаты вышеуказанных этапов в виде отчета. В отчете также отражаются меры по снижению рисков и принятые решения. В необходимых случаях Компания запрашивает мнение субъектов данных;
f) интеграция результатов Оценки воздействия на неприкосновенность частной жизни в план проекта обработки. Компания интегрирует полученные результаты и меры по оценке в план проекта. Компания осуществляет данный этап путем постоянного обращения к указанным результатам оценки, чтобы убедиться в том, что они принимаются во внимание в процессе обработки данных, а также в том, что ответные меры по снижению рисков реализуются эффективным образом.

Компания фиксирует любую Оценку воздействия на защиту данных, выполненную для будущих проектов обработки.

13.1.4. Фиксация и документальное отражение мероприятий по обработке, осуществляемых Компанией

Компания ведет учет мероприятий по обработке персональных данных.

13.1.5. Обязанность соблюдать конфиденциальность

Все сотрудники с правом доступа к персональным данным обращаются с персональными данными и распоряжаются ими, соблюдая строгую конфиденциальность, если такие данные не предназначены для обнародования.

Все сотрудники Компании подписали Трудовой договор, включающий, среди прочего, статью «КОНФИДЕНЦИАЛЬНОСТЬ».

Статьей «КОНФИДЕНЦИАЛЬНОСТЬ» предусмотрено, что, пока между сотрудником и Компанией существуют трудовые отношения, а также после прекращения действия или расторжения Трудового договора, заключенного с таким сотрудником, последний держит в тайне и не раскрывает третьим лицам, в числе прочего, данные, имеющие отношение к базе данных клиентов Компании.

FINARTEL

13.1.6. Пересмотр Политики в области неприкосновенности частной жизни

Политика в области неприкосновенности частной жизни пересматривается, оценивается и актуализируется по мере необходимости, но не реже одного раза в год.

13.2. Меры физической безопасности

13.2.1. Безопасность офиса

Безопасность офиса обеспечивается круглосуточной системой охранной сигнализации и видеонаблюдения с контролем входной группы.

13.2.2. Формат собираемых и хранящихся данных

Сбор персональных данных, находящихся в распоряжении Компании, может осуществляться в печатной форме (на физическом носителе) и в цифровом (электронном) виде.

13.2.3. Печатная форма (на физическом носителе)

Персональные данные, сбор которых осуществляется в печатной форме (на физическом носителе), хранятся в офисе. Безопасность офиса обеспечивается круглосуточной системой охранной сигнализации и видеонаблюдения.

Если Компания перемещает персональные данные в печатной форме (на физическом носителе) за пределы офиса Компании, то персональные данные транспортируются в автомобиле, оснащенном блокировкой дверей, или курьерской службой, утвержденной клиентом или соответствующим третьим лицом.

13.2.4. Цифровой (электронный) формат

Устройства, используемые для обработки персональных данных в цифровом (электронном) виде (персональный компьютер, ноутбук, смартфон), защищены системами антивирусной защиты. Используются следующие системы антивирусной защиты: для Windows — антивирусная программа Bitdefender, для MacBook Pro — встроенное средство защиты от вредоносных программ, для смартфона — встроенный антивирус.

Доступ к указанным устройствам имеют только их владельцы. Доступ осуществляется при помощи паролей, кодов и (или) отпечатка пальца.

Персональные данные, хранящиеся в приложениях облачных сервисов G-Suite, защищены двухэтапной аутентификацией и Средствами операционной безопасности (управления уязвимостями, предотвращения установки вредоносного программного обеспечения, контроля и урегулирования инцидентов).

Если для транспортировки персональных данных в цифровом (электронном) виде за пределы офиса Компании используются ноутбуки, то эти устройства защищаются паролями, кодами и (или) отпечатком пальца, а доступ могут получить только их владельцы.

В случае передачи персональных данных в цифровом (электронном) формате в виде файлов их передача осуществляется через сервисы G-Suite, защищенные Средствами операционной безопасности (управления уязвимостями, предотвращения установки вредоносного программного обеспечения, контроля и урегулирования инцидентов).

В случае отправки персональных данных по электронной почте соответствующие электронные письма подвергаются шифрованию.

13.2.5. Контроль и ограничение доступа

Персональные данные обрабатываются только уполномоченными лицами в ходе обычной хозяйственной деятельности.

13.2.6. Устройство офисного пространства (рабочего места)

Мониторы компьютеров в нерабочем режиме блокируются.

Мониторы компьютеров располагаются таким образом, чтобы другие проходящие мимо сотрудники не могли их видеть.

Не разрешается оставлять копии без присмотра на рабочем столе или копировальном аппарате.

13.2.7. Обязанности Лиц, задействованных в обработке

Лица, задействованные в обработке, всегда соблюдают конфиденциальность и обеспечивают целостность персональных данных. Указанные лица:

- не могут пользоваться собственными гаджетами или устройствами хранения при обработке персональных данных;
- обеспечивают, чтобы мониторы их компьютеров всегда были заблокированы в нерабочем режиме;
- гарантируют, что в случае отправки ими персональных данных по электронной почте соответствующие сообщения будут зашифрованы с целью предоставления возможности просмотра таких сообщений и доступа к ним только уполномоченному получателю;
- не могут раскрывать никаких персональных данных другим сотрудникам без разрешения руководства Компании или не в соответствии с хозяйственной деятельностью Компании.

13.2.8. Способы передачи персональных данных в рамках Компании, в адрес уполномоченных получателей или третьих лиц по электронной почте или с помощью средств факсимильной связи

Передача персональных данных по электронной почте осуществляется при условии шифрования сообщений, включая любые (все) вложения.

Компания не использует аппарат факсимильной связи для сбора и (или) отправки персональных данных.

13.2.9. Порядок раскрытия

Компания хранит персональные данные клиента в течение периода, определенного в пункте 10 «СРОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ КОМПАНИЕЙ». По истечении указанного периода все физические и электронные копии персональных данных уничтожаются и утилизируются в порядке, описанном в пункте «Уничтожение».

13.3. Технические средства безопасности

13.3.1. Выявление нарушений безопасности

В связи с тем что персональные данные хранятся в электронном виде и печатной форме, Компания приняла следующие меры безопасности для контроля любых нарушений.

a) Применительно к персональным данным, хранящимся в электронном виде

Для обеспечения безопасности персональных данных, хранящихся в электронном виде, Компания использует системы антивирусной защиты, описанные в подпункте 12.2.4 «Цифровой (электронный) формат» и позволяющие выявлять нарушения безопасности, предупреждать Компанию о попытках прервать или вмешаться в надлежащую работу системы.

В случае попытки вмешательства в работу системы на экране устройства появляется предупреждение системы антивирусной защиты с блокировкой открытия или запуска подозрительного файла.

b) Применительно к персональным данным, хранящимся в печатной форме

Для гарантии защиты персональных данных, хранящихся в печатной форме, безопасность офиса Компании обеспечивается круглосуточной системой охранной сигнализации и видеонаблюдения.

13.3.2. Безопасность используемого программного обеспечения и приложений (одного или нескольких)

Перед установкой на компьютерах и устройствах Компании каких-либо программных приложений Компания предварительно выполняет их анализ и оценку с целью обеспечения совместимости средств безопасности с используемой операционной системой в целом.

14. ДОСТОВЕРНОСТЬ ДАННЫХ

В соответствии с Регламентом ЕС 2016/679 Компания должна принимать обоснованно необходимые меры по обеспечению достоверности и актуальности хранящихся персональных данных.

Принятие обоснованно необходимых мер по обеспечению максимальной достоверности и актуальности хранящихся персональных данных входит в обязанности сотрудников, работающих с персональными данными. Согласно нашим законодательно установленным обязательствам персональные данные, которые хранятся у нас, проверяются по каждому клиенту.

Проверка производится один раз в год или один раз в 4 (четыре) года в зависимости от категории, к которой относятся наши клиенты. Доказательства проведения проверки помещаются в досье клиента.

Сотрудники обязаны информировать Компанию о любых изменениях в своих персональных данных, хранящихся в Компании в связи с их трудовыми отношениями.

15. ПРАВА СУБЪЕКТОВ ДАННЫХ

Всем лицам, являющимся субъектами персональных данных, находящихся в распоряжении Компании, предоставлены нижеуказанные права в значении, приведенном в Регламенте ЕС 2016/679, если эти права не ограничены в рамках указанного Регламента:

- **Право доступа.** Вы вправе запросить копию своих персональных данных, находящихся в распоряжении Компании в отношении вас. Компания предоставляет копию ваших персональных данных, которые подвергаются обработке. Компания может взимать обоснованную плату за дополнительно запрашиваемые вами копии, рассчитанную на основе административных издержек.

Вы можете направить электронное письмо с запросом копии (ПРИЛОЖЕНИЕ 2) своих персональных данных, которые подвергаются обработке, по адресу: compliance@finartel.fund.

- **Право на внесение исправлений.** Вы имеете право потребовать от Компании исправления любых неточностей в персональных данных, касающихся вас.

Вы можете направить электронное письмо с требованием внести соответствующие исправления по адресу: compliance@finartel.fund. Компания направит вам дополнительную форму (ПРИЛОЖЕНИЕ 3), которую необходимо заполнить и прислать обратно Компании.

- **Право на удаление данных.** При определенных обстоятельствах, предусмотренных Регламентом ЕС 2016/679, вы вправе добиваться от Компании удаления ваших персональных данных.
- **Право на ограничение обработки данных.** При возникновении спора по поводу достоверности ваших персональных данных или процесса их обработки вы имеете право потребовать ограничения их дальнейшей обработки в соответствии с положениями Генерального регламента о защите персональных данных (GDPR) ЕС 2016/679.

Если обработка ваших персональных данных ограничена в соответствии с условиями, определенными в Регламенте ЕС 2016/679, то Компания обрабатывает ваши персональные данные (за исключением их хранения) только с вашего согласия или в целях возбуждения, осуществления, ведения защиты судебных исков, или для защиты прав другого физического или юридического лица, или по причинам особого общественного интереса на основании законодательства Союза или Государства-члена ЕС.

Компания уведомит вас перед снятием ограничений.

- **Право на переносимость данных.** Если обработка осуществляется с согласия или по договору и автоматическими средствами, то вы имеете право получить персональные данные, а также право передать эти данные другому контролеру.

- **Право на предъявление возражений.** В случаях, установленных Регламентом ЕС 2016/679, вы имеете право предъявить возражение против обработки своих персональных данных.
- **Право не подчиняться** решению, принятому посредством только автоматической обработки, включая формирование профиля.

Если Компания использует автоматическую обработку, включая формирование профиля, то при принятии касающегося вас решения вы имеете право на вмешательство работника Компании, выражение своей точки зрения и оспаривание решения.

- **Право отозвать свое согласие.** В случаях, когда обработка осуществляется с вашего согласия, вы имеете право отозвать свое согласие в любое время.

Для отзыва согласия отправьте электронное письмо, содержащее требование отзыва своего согласия, по адресу: compliance@finartel.fund.

- **Право подачи жалобы** в Службу уполномоченного по защите персональных данных.

В этом случае Компания просит субъекта данных в первую очередь обратиться в организацию FINARTEL CAPITAL VCIC LTD по электронной почте: compliance@finartel.fund (ПРИЛОЖЕНИЕ 4).

Независимо от вида обращения или жалобы Компания может запросить дополнительную информацию, необходимую для подтверждения личности субъекта данных, направляющего запрос или жалобу.

Компания предоставляет информацию о мерах, принятых по запросу субъектов данных в соответствии с их правами, в течение 1 (одного) месяца с момента поступления запроса. В случае необходимости (с учетом сложности и количества запросов) указанный срок может быть дополнительно продлен на 2 (два) месяца. Компания информирует субъекта данных о любом подобном продлении срока в течение 1 (одного) месяца с момента поступления запроса с указанием причин задержки.

Компания по возможности предоставляет субъекту данных запрашиваемую информацию электронным способом.

Запрашиваемая информация предоставляется на бесплатной основе. Компания сохраняет за собой право установить обоснованную плату с учетом административных издержек, связанных с предоставлением информации, сообщения или принятия требуемых мер, либо отказаться выполнить требование в случае, если ваш запрос является заведомо необоснованным или чрезмерным.

16. НАРУШЕНИЕ БЕЗОПАСНОСТИ И ИНЦИДЕНТЫ В СИСТЕМЕ БЕЗОПАСНОСТИ

Нарушение безопасности приводит к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к персональным данным, являющимся объектом передачи, хранения или обработки иным способом.

16.1. Порядок действий в случае нарушения

При возникновении инцидента в системе безопасности или нарушения безопасности персональных данных Компания обязана незамедлительно принять меры. Руководство оценивает инцидент или нарушение в целях установления его характера и степени.

16.2. Сообщение об инциденте или нарушении в Службу уполномоченного по защите персональных данных

Компания оценивает инцидент и, если будет принято решение о том, что нарушение безопасности персональных данных может привести к возникновению риска для прав и свобод физических лиц, уведомляет Службу уполномоченного по защите персональных данных (http://www.dataзащит.gov.cy) не позднее чем через 72 часа после того, как о таком нарушении станет известно (ПРИЛОЖЕНИЕ 5).

Если Компания не сможет отправить всю информацию, включенную в уведомление Уполномоченному, за один раз, то Компания направляет информацию поэтапно, не допуская необоснованных отсрочек.

16.3. Сообщение об инциденте или нарушении субъекту данных

Компания оценивает инцидент и, если будет принято решение о том, что нарушение безопасности персональных данных может привести к возникновению риска для прав и свобод физических лиц, безотлагательно сообщает субъекту данных о таком нарушении безопасности персональных данных (ПРИЛОЖЕНИЕ 6).

Во время процедуры оценки инцидента Компания может принять решение об отсутствии необходимости уведомления субъекта данных при выполнении любого из следующих условий:

a) Компания приняла надлежащие технические и организационные меры защиты персональных данных, в отношении которых зафиксирован инцидент (шифрование);
b) Компания приняла последующие меры, которые гарантируют, что вероятность дальнейшей реализации высокого риска для прав и свобод субъектов данных, пострадавших от нарушения, будет сведена к нулю;
c) сообщение о нарушении сопряжено с несоразмерными усилиями. В этом случае Компания выступает с открытым заявлением или принимает аналогичную меру по информированию субъектов данных равнозначным по эффективности способом.

16.4. Меры по предотвращению и минимизации инцидентов, связанных с нарушениями безопасности данных

С целью минимизации нарушений и инцидентов в системе безопасности Компанией предусмотрены технические меры безопасности, описанные выше в подпункте 12.3.1 «Выявление нарушений безопасности».

В случае попытки вмешательства в работу системы на экране устройства появляется предупреждение системы антивирусной защиты с блокировкой открытия или запуска подозрительного файла.

Офис Компании оборудован круглосуточной системой охранной сигнализации и видеонаблюдения с контролем входной группы.

16.5. Восстановление персональных данных

В некоторых случаях персональные данные, хранящиеся в печатной форме, также помещаются в архив в электронном виде.

Если персональные данные также хранятся в электронном виде, то при возникновении инцидента, связанного с нарушением персональных данных в печатной форме, Компания может извлечь из электронных файлов персональные данные, в отношении которых зафиксировано нарушение.

В сервисах G-Suite Компания осуществляет резервное копирование всех персональных данных, находящихся на ее ответственном хранении в электронном виде.

В случае инцидента в системе безопасности или нарушения безопасности персональных данных, хранящихся в электронном виде, Компания всегда сравнивает файл резервного копирования с файлом, в отношении которого зафиксирован инцидент, чтобы установить наличие каких-либо несоответствий или изменений, обусловленных инцидентом или нарушением.

16.6. Учет нарушений безопасности персональных данных

Компания оформляет и хранит подробную документацию по каждому инциденту или нарушению, с которым она сталкивается. Записи, которые ведет Компания, представляют собой документацию, включающую:

a) факты, относящиеся к нарушению безопасности персональных данных;
b) его последствия; и
c) принятые корректирующие меры.

17. ОБРАЩЕНИЯ И ЖАЛОБЫ

Независимо от вида обращения или жалобы Компания может запросить дополнительную информацию, необходимую для подтверждения личности субъекта данных, направляющего запрос или жалобу.

Компания предоставляет информацию в отношении обращения или жалобы в течение 1 (одного) месяца с момента поступления обращения или жалобы. В случае необходимости (с учетом сложности и количества обращений или жалоб) указанный срок может быть дополнительно продлен на 2 (два) месяца. Компания информирует субъекта данных о любом подобном продлении срока в течение 1 (одного) месяца с момента поступления обращения или жалобы с указанием причин задержки.

Компания ведет учет запросов и жалоб, а также принятых мер, связанных с обработкой персональных данных субъектов данных, в бумажном или электронном виде в досье соответствующего субъекта данных.

17.1. Обращения

Субъекты данных могут наводить справки или запрашивать информацию по любому вопросу, относящемуся к обработке своих персональных данных, находящихся на хранении в Компании, в том числе к правилам обеспечения неприкосновенности данных и безопасности, введенным для обеспечения защиты их персональных данных. Субъекты данных могут обращаться в Компанию и в краткой форме обсуждать возникающие вопросы, направляя сообщения с указанием своих контактных данных по адресу: compliance@finartel.fund.

17.2. Жалобы

В случае подачи жалобы Компания просит субъекта данных в первую очередь обратиться в компанию FINARTEL CAPITAL VCIC LTD по электронной почте: compliance@finartel.fund. Далее субъекту данных направляется форма жалобы для ее заполнения.

Компания подтверждает заявителю факт получения заполненной формы жалобы, а руководство Компании расследует обстоятельства полученной жалобы и принимает необходимые меры в указанные выше сроки.

18. УЧЕТ

Компания ведет учет мероприятий по обработке персональных данных.

19. ВСТУПЛЕНИЕ В СИЛУ

Положения настоящей Политики (в редакции 2.0) считаются неотъемлемой частью Политики (в редакции 1.0) и вступают в силу немедленно. Настоящая Политика действует до момента ее отзыва или изменения Компанией.

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

+357 25 057 150

hq@finartel.fund

Номер лицензии, выданной Кипрской комиссией по ценным бумагам и биржам: LPAIF114/2014

ПРИЛОЖЕНИЕ 1

Документация по Оценке воздействия на неприкосновенность частной жизни

Оценка воздействия на защиту данных

Согласно статьям 35(1) и 35(3) Регламента (ЕС) 2016/679 Компания FINARTEL CAPITAL VCIC LTD приняла решение перед обработкой _____ выполнить оценку воздействия предусмотренных операций по обработке на защиту персональных данных.

Оценка воздействия на неприкосновенность частной жизни (в соответствии со статьей 35(7) Регламента GDPR):

1) Описание предусмотренной обработки:

2) Цель обработки:

3) Необходимость проведения Оценки воздействия на неприкосновенность частной жизни в процессе обработки указанных сведений (причины, риски):

4) Законный интерес нашей Компании:

5) Описание информационного потока по конкретной процедуре обработки (принципы сбора информации, источники информации, получатели информации, типы данных, лица, уполномоченные на получение доступа к таким данным, способ хранения и удаления данных, а также любые другие необходимые сведения):

6) Необходимость и соответствие операций по обработке поставленным целям:

7) Описание рисков для прав и свобод субъектов данных, в отношении которых такие риски могут возникнуть (составить список угроз и факторов уязвимости):

8) Описание предусмотренных мер по устранению рисков, в том числе мер предосторожности, мер безопасности и механизмов по обеспечению защиты персональных данных, а также подтверждение соблюдения Регламента с учетом прав и законных интересов субъектов данных и других заинтересованных лиц (решение о принятии или непринятии риска или по любым другим принимаемым мерам):

Вывод:

Принятое решение или шаги по снижению рисков:

Интеграция (интеграция результатов Оценки воздействия на неприкосновенность частной жизни в план проекта обработки для обеспечения его выполнения, а также эффективной реализации соответствующих ответных мер по устранению рисков):

ПРИЛОЖЕНИЕ 2

Форма «Доступ к персональным данным»

Персональные данные, которые хранятся в компании FINARTEL CAPITAL VCIC LTD по субъекту данных

(Право доступа)

ФИО: _____

Цель обработки	Категории персональных данных	Лица, которым такие данные раскрываются или будут раскрыты	Срок хранения данных	Источник	Предусмотренное автоматизированное принятие решений

Компания FINARTEL CAPITAL VCIC LTD (далее — «Компания») извещает вас о хранении указанных данных в соответствии с целями и сроками, обозначенными выше.

В соответствии со статьей 15 Регламента (ЕС) 2016/679 вы имеете право:

a) потребовать от Компании внести исправления или удалить персональные данные либо ограничить обработку касающихся вас персональных данных или предъявить возражение против их обработки;
b) подать жалобу в компетентный надзорный орган.

Ваши права подпадают под ограничения, предусмотренные статьей 23 Регламента (ЕС) 2016/679.

ПРИЛОЖЕНИЕ 3

Дополнительное заявление об исправлении недостоверных данных

По вашему запросу от «__» _____ ____ года, полученному _____, на исправление ваших персональных данных, обрабатываемых компанией FINARTEL CAPITAL VCIC LTD, и в соответствии с вашим правом согласно статье 16 Регламента (ЕС) 2016/679 компания FINARTEL CAPITAL VCIC LTD просит вас сообщить, в какие из ваших персональных данных вы хотите внести исправления.

Просьба соответствующим образом заполнить приведенные ниже поля:

Персональные данные в настоящее время:	**Персональные данные по результатам внесения изменений:**

Компания FINARTEL CAPITAL VCIC LTD настоящим сообщает, что рассмотрит ваш запрос, примет соответствующие меры с учетом любых существующих ограничений согласно статье 23 Регламента (ЕС) 2016/679 и проинформирует вас не позднее чем через 1 (один) месяц с момента получения вашего запроса (если нам потребуется больше времени, об этом будет сообщено дополнительно).

От имени и по поручению FINARTEL CAPITAL VCIC LTD

.....

Дата

.....

ПРИЛОЖЕНИЕ 4

Форма жалобы в отношении Персональных данных

Компания FINARTEL CAPITAL VCIC LTD (далее — «Компания») просит вас подробно изложить в приведенном ниже поле вашу жалобу касательно обработки ваших персональных данных (просьба заполнить поле в электронном виде и прислать в заполненном виде по адресу: compliance@finartel.fund).

Ваши ФИО:.....

Дата: .....

Жалоба:

Для использования Компанией:

Меры (рекомендации):

.....

.....

От имени и по поручению FINARTEL CAPITAL VCIC LTD:

.....

Дата:

.....

ПРИЛОЖЕНИЕ 5

Уведомление о нарушении безопасности персональных данных, адресованное кипрскому Компетентному органу

Уведомление о нарушении безопасности персональных данных

Адресат:

Служба уполномоченного по защите персональных данных
Эл. почта: commissioner@dataprotection.gov.cy
Тел.: 22818456, факс: 22304565

FINARTEL CAPITAL VCIC LTD (далее — «Компания») настоящим сообщает, что «__» _____ ____ года Компанией было зафиксировано нарушение, касающееся обработки персональных данных в Компании. Подробные сведения об указанном нарушении приведены ниже:

1) Нарушение (описание):

.....

2) Категории персональных данных, в отношении которых зафиксировано нарушение:

.....

3) Точное (или приблизительное) число пострадавших субъектов данных:

.....

4) Точное (или приблизительное) количество записей, в отношении которых зафиксировано нарушение:

.....

5) Контактное лицо Компании:

.....

6) Последствия нарушения безопасности персональных данных:

.....

7) Принятые или предлагаемые меры:

.....

8) Причина ненаправления уведомления в течение 72 часов с момента инцидента:

.....

От имени и по поручению FINARTEL CAPITAL VCIC LTD

.....

Дата:

.....

ПРИЛОЖЕНИЕ 6

Уведомление о нарушении безопасности персональных данных, адресованное субъекту данных

Уведомление о нарушении безопасности персональных данных

Адресат (Субъект данных):
ФИО: .....
Эл. почта: .....
Тел.: .....
Факс: .....

FINARTEL CAPITAL VCIC LTD (далее — «Компания») настоящим сообщает, что «__» _____ ____ года Компанией было зафиксировано нарушение, касающееся обработки персональных данных в Компании. Нарушение возникло в процессе обработки Компанией ваших персональных данных.

Подробные сведения об указанном нарушении приведены ниже:

1) Описание нарушения:

.....

2) Контактное лицо Компании:

.....

3) Последствия нарушения безопасности персональных данных:

.....

4) Принятые или предлагаемые меры:

.....

От имени и по поручению FINARTEL CAPITAL VCIC LTD

.....

Дата:

.....