Приложение № 2
к приказу от 20.10.2023 г. № 20-10-1/23

УТВЕРЖДЕНО
Приказом директора
ООО «Кредиска МКК»
от 20.10.2023 г. № 20-10-1/23

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ООО «КРЕДИСКА МКК»

г. Нижний Новгород
2023 год

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о защите персональных данных работников, клиентов и контрагентов ООО «Кредиска МКК» является локальным нормативным актом Общества с ограниченной ответственностью Микрокредитной компании «Кредиска» (далее - Общества), устанавливающим порядок получения, обработки, хранения, передачи и защиты персональных данных в Обществе.

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Главой 14 Трудового кодекса Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлениями Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Положением Банка России от 20 апреля 2021 г. № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций», Приказом ФСТЭК России № 21 от 18.02.2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. В настоящем Положении используются следующие термины и определения:

Оператор – ООО «Кредиска МКК», вступившее в договорные отношения с работником, клиентом или контрагентом, организующее и осуществляющее, в связи с этим обработку персональных данных.

Пользователь сайта - физическое лицо, выступающее от своего имени и в своих интересах или от имени и в интересах представляемого им юридического лица, заполняющее форму обратной связи и (или) подающее заявку на взаимодействие с Обществом на сайте Общества.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Положением;

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Субъект персональных данных – физическое лицо, персональные данные которого обрабатываются Обществом в целях, определенных настоящим Положением.

Защита персональных данных – комплекс мер, принимаемых Обществом для защиты персональных данных от неправомерного или случайного доступа к ним,

уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Актуальные угрозы безопасности - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Конфиденциальная информация – информация, содержащая сведения конфиденциального характера, в том числе получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах, в отношении которой Общество принимает меры по защите от несанкционированного доступа третьих лиц, не имеющих право доступа к такой информации.

Режим конфиденциальности – правовые, организационные, технические и иные меры по защите конфиденциальной информации, принимаемые ее обладателем на основании закона.

Реестр определения прав доступа к Конфиденциальной информации (далее – Реестр прав доступа) – внутренний документ Общества, закрепляющий перечень должностей и категории Конфиденциальной информации, ресурсы информационной системы, криптографические ключи, к которым работники Общества имеют доступ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

«Куки» (cookies) - небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере для взаимодействия с веб-сервером, позволяющий пользователю сайта в полном объеме получать услуги на сайте Общества.

1.1. Настоящее Положение вступает в силу с момента его утверждения приказом руководителя Общества.

1.2. Настоящее Положение является обязательным для исполнения всеми работниками Общества, имеющими доступ к персональным данным, и доводится до их сведения персонально под подпись.

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. В целях обеспечения прав и свобод человека и гражданина Обществом и его представителями при обработке персональных данных должны соблюдаться следующие общие требования:

2.1.1. Обработка персональных данных должна осуществляться на законной и справедливой основе, исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия выполнения договорных обязательств в соответствии с законодательством Российской Федерации.

2.1.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, а также объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой.

2.1.3. Получение Обществом персональных данных может осуществляться как путем представления их самим субъектом персональных данных, так и путем получения их из иных источников. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Общество должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и юридическое последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку, если в соответствии с федеральным законом предоставление персональных данных и (или) получение Обществом согласия на обработку персональных данных являются обязательными.

2.1.4. Общество не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его политических, религиозных и иных убеждениях, о частной жизни. В необходимых случаях данные о частной жизни работника или клиента (информация о семейных, бытовых, личных отношениях) могут быть получены и обработаны Обществом только с его письменного согласия.

2.1.5. Общество не имеет право получать и обрабатывать персональные данные субъектов персональных данных об их членстве в общественных объединениях или их профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

2.2. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

2.3. Персональные данные субъекта персональных данных не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено действующим законодательством Российской Федерации.

2.4. При принятии решений, затрагивающих интересы субъекта персональных данных, Общество не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки без письменного согласия субъекта персональных данных на такие действия.

2.5. При идентификации клиента или контрагента Общество может затребовать предъявления документов, удостоверяющих личность и подтверждающих полномочия

представителя. При заключении договора, как и в ходе выполнения договора, Общество может затребовать предоставление клиентом или контрагентом иных документов, содержащих информацию о нем.

2.6. После принятия решения о заключении договора или предоставления документов, подтверждающих полномочия представителя, а также, впоследствии, в процессе выполнения договора, к документам, содержащим персональные данные клиента или контрагента, так же будут относиться:

–договоры;

–приказы по основной деятельности;

–служебные записки;

–другие документы, где включение персональных данных клиента или контрагента необходимо согласно действующему законодательству.

2.7. Не допускается отвечать на вопросы, связанные с предоставлением персональных данных по телефону или факсу, по электронной почте и иным видам связи.

2.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

2.9. Период хранения и обработки персональных данных определяется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2.10. Общество осуществляет обработку персональных данных в целях:

- осуществления предпринимательской деятельности, предусмотренной Уставом Общества, в том числе предоставление займов в порядке, установленном Федеральным законом от 21 декабря 2013 г. № 353-ФЗ "О потребительском кредите (займе)",

- заключения и исполнения гражданско-правовых договоров с физическими, юридическим лицами, индивидуальными предпринимателями и иными лицами, в связи с осуществлением хозяйственной деятельности Общества;

- оформления трудовых отношений; исполнение обязательств по трудовым договорам; ведение кадрового делопроизводства; содействие работникам в обучении и продвижении по службе; исполнение требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение;

- организации учета участников Общества и лиц, под контролем либо значительным влиянием которых находится Общество.

2.11. Категории субъектов персональных данных для достижения целей их обработки Обществом, способы обработки, прекращение, хранение, уничтожение персональных данных, права и обязанности субъекта персональных данных, права и обязанности Общества как оператора персональных данных регламентируются Политикой в отношении обработки и защиты персональных данных, утверждаемой приказом руководителя Общества.

2.12. Уничтожение персональных данных осуществляется комиссией, назначаемой приказом руководителя Общества. Лицо, ответственное за организацию обработки

персональных данных назначается председателем комиссии по уничтожению персональных данных.

2.13. При наступлении любого из событий, повлекших, необходимость уничтожения персональных данных, в соответствии с законодательством Российской Федерации, лицо, ответственное за организацию обработки персональных данных обязано:

- уведомить членов комиссии о дате начала работ по уничтожению персональных данных;
- определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);
- установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению (и/или материальные носители персональных данных);
- руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных): документы, подлежащие уничтожению, измельчаются в шредере, персональные данные клиентов в электронном виде стираются с электронных носителей, либо физически уничтожаются сами материальные носители, на которых хранится информация;
- в случае необходимости уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

В целях подтверждения уничтожения персональных данных составляются следующие документы:

1) В случае если обработка персональных данных осуществляется без использования средств автоматизации - Акт об уничтожении персональных данных.

2) В случае если обработка персональных данных осуществляется с использованием средств автоматизации либо одновременно с использованием средств автоматизации и без использования средств автоматизации - Акт об уничтожении персональных данных, и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

2.1) Формы акта об уничтожении персональных данных и выгрузки из журнала утверждаются приказом руководителя Общества и содержат все обязательные сведения, указанные в Приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

2.2) Акт об уничтожении персональных данных может быть составлен как на бумажном носителе, так и в электронном виде и подписан лицом (лицами), уничтожившими персональные данные, собственноручной либо электронной подписью соответственно.

2.3) Акт об уничтожении персональных данных и выгрузка из журнала хранятся Обществом в течение 3 лет с момента уничтожения персональных данных.

2.14. Общество использует средства «Яндекс Метрика» для сбора сведений об использовании Сайта Общества, таких как частота посещения Сайта пользователями, посещенные страницы и сайты, на которых были пользователи до перехода на данный Сайт. Яндекс Метрика собирает только IP-адреса, назначенные Пользователю в день посещения данного Сайта, но не имя или другие идентификационные сведения.

2.15. Яндекс Метрика размещает постоянный cookie-файл в веб-браузере пользователя для его идентификации в качестве уникального пользователя при следующем

посещении данного Сайта. Оператор использует сведения, полученные через Яндекс Метрику, только для совершенствования услуг на данном Сайте.

2.16. Возможности Яндекс по использованию и передаче третьим лицам сведений, собранных средством Яндекс Метрики о посещениях данного Сайта пользователем, ограничиваются Политикой конфиденциальности Яндекс. Пользователь может запретить Яндекс Метрике узнавать его при повторных посещениях данного Сайта, отключив cookie-файлы Яндекс Метрики в своем браузере или пользователь может использовать Блокировщик Яндекс Метрики.

3. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Обществом определено, что на информацию, содержащую персональные данные, распространяется режим конфиденциальности.

3.1. Организация работы по защите Конфиденциальной информации, в том числе персональных данных.

3.1.1. Безопасность персональных данных при их использовании и обработке в Обществе обеспечивается с помощью системы защиты Конфиденциальной информации, разработанной самим Обществом (далее – система защиты).

При разработке системы защиты учитывалась обязанность Общества обеспечивать защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, в том числе принимать меры, установленные статьей 19 Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных».

3.1.2. Система защиты реализуется путем проведения нескольких взаимосвязанных процессов. К ним относятся:

−определение актуальных угроз безопасности персональных данных.

Порядок определения актуальных угроз безопасности персональных данных, и ответственный за проведение процедуры определения актуальных угроз безопасности, определяется приказом руководителя Общества.

Результатом проведения процедуры определения актуальных угроз безопасности персональных данных, является составление акта определения актуальных угроз безопасности;

−определение необходимых правовых, организационных и технических мер по обеспечению безопасности персональных данных, при их обработке в информационных системах, исполнение которых обеспечивает необходимый уровень защищенности;

Необходимый уровень защищенности персональных данных при обработке в информационных системах определяется Обществом при выявлении актуальных угроз безопасности и фиксируется в акте определения актуальных угроз безопасности.

−надлежащее применение определенных правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах, а так же применение прошедших в установленном порядке процедуру оценки соответствия средств защиты персональных данных;

−проведение оценки эффективности принимаемых мер по обеспечению безопасности персональных данных с установленной в настоящем Положении периодичностью;

−обеспечение контроля надлежащей реализации мер по обеспечению безопасности персональных данных.

3.1.3. В целях обеспечения функционирования системы защиты руководитель выполняет следующие функции:

−организация разработки проектов и утверждение внутренних документов Общества по вопросам обеспечения режима конфиденциальности, определения режима порядка обращения с персональными данными с привлечением иных работников Общества;

−организация взаимодействия с органами государственной власти, правоохранительными и надзорными органами по вопросам обеспечения и соблюдения режима конфиденциальности;

−утверждение Реестра прав доступа, в том числе при внесении изменений и дополнений;

−рассмотрение вопроса о передаче персональных данных третьим лицам;

−определение требований к техническому оснащению помещений, в которых осуществляется работа с персональными данными;

−осуществление контроля за обеспечением режима безопасности помещений;

−принятие решений о необходимости проведения обучений для работников Общества;

−проведение плановых и внезапных проверок на предмет соблюдения режима конфиденциальности в Обществе работниками Общества;

−принятие решений о необходимости отстранения от работы с конфиденциальной информации работников Общества, нарушающих режим конфиденциальности в Обществе;

−рассмотрение иных вопросов обеспечения и соблюдения режима конфиденциальности.

3.1.4. Защите подлежат все персональные данные, определенные в Политике по обработке и защите персональных данных, утверждаемой приказом руководителя, в том числе:

−персональные данные субъекта, содержащиеся в копиях документов;

−персональные данные субъекта, содержащиеся в документах, созданных Обществом;

−персональные данные субъекта, занесенные в учетные формы;

−записи, содержащие персональные данные субъекта;

−персональные данные субъекта, содержащиеся на электронных носителях;

−персональные данные субъекта, обрабатываемые в информационных системах персональных данных;

−персональные данные субъекта, разрешенные субъектом для распространения.

3.2. Правовые меры защиты персональных данных.

3.2.1. К правовым мерам защиты персональных данных относится:

3) Разработка и утверждение локальных нормативных актов Общества: Политики в отношении обработки и защиты персональных данных, Положения о защите персональных данных, иных документов, которыми регламентируется порядок организации системы защиты в Обществе (далее – Регламентирующие документы).

4) Обязанность Общества осуществлять мониторинг действующего законодательства.

3.2.2. Регламентирующие документы разрабатываются самим Обществом или с привлечением третьих лиц и утверждаются руководителем Общества.

3.2.3. Регламентирующие документы должны пересматриваться на предмет их актуальности и необходимости внесения изменений не реже одного раза в год, а также:

−в случае изменения законодательства, регламентирующего порядок обращения организаций с Конфиденциальной информацией и устанавливающего требования к защите информации, в том числе законодательства о персональных данных;

−в случае установления фактов несанкционированного доступа к персональным данным, грубого нарушения работниками Общества режима конфиденциальности, разглашения и утечки информации, содержащей персональные данные;

−на основании заключения, сформированного по результатам проведения очередной оценки достаточности принятых мер по защите персональных данных.

3.3. Организационные меры защиты персональных данных.

К организационным мерам защиты персональных данных относятся:

3.3.1. Определение правил доступа к информации, содержащей персональные данные.

3.3.1.1. К работе с информацией, содержащей персональные данные, могут быть допущены работники Общества при одновременном выполнении следующих условий:

−должность работника указана в Реестре прав доступа;

−работник ознакомлен под подпись с Реестром прав доступа и настоящим Положением;

−работником Общества подписано Обязательство о неразглашении конфиденциальной информации.

3.3.1.2. Приказом руководителя Общества с целью определения перечня лиц, доступ которых к информации, содержащей персональные данные, необходим для выполнения ими своих должностных обязанностей, и определения необходимого объема информации, содержащей персональные данные, с которым вправе работать каждый из таких работников, утверждается Реестр прав доступа.

1) При утверждении Реестра прав доступа Общество руководствуется правилом о том, что доступ к персональным данным должен предоставляться только тем лицам, которым персональные данные необходимы для выполнения возложенных на них должностных обязанностей и только в том объеме (к той ее части), который необходим для выполнения определенных функций.

2) Реестр прав доступа Общества содержит следующую информацию:

−должности работников Общества, допущенных к работе с информацией, содержащей персональные данные;

−категории информации, к которым работники имеют доступ;

−ресурсы информационной системы, к которым работники имеют доступ;

−Криптографические ключи, к которым работники имеют доступ.

3) Реестр прав доступа подлежит обязательному пересмотру не реже одного раза в год, а также в случае:

−изменения штатного расписания Общества;

−изменения функционала определенной должности;

−изменения перечня ресурсов информационной системы;

−приобретения или уничтожения Криптографических ключей.

4) Правом предоставления, ограничения, прекращения доступа ко всей информации, содержащей персональные данные, создаваемой, хранимой и обрабатываемой в Обществе, включая информацию, полученную от третьих лиц, обладает руководитель Общества.

3.3.1.3. До начала работы с персональными данными работник должен подписать Обязательство о неразглашении конфиденциальной информации.

Обязательство о неразглашении конфиденциальной информации, подписанное работником Общества, приобщается к личному делу работника.

3.3.1.4. Определение обязанностей для работников Общества при работе с персональными данными. Работник Общества, допущенный к работе с информацией, содержащей персональные данные, обязан:

−знать и выполнять требования настоящего Положения, иных внутренних документов по защите информации;

−соблюдать ограничения, установленные Реестром прав доступа: работать только с теми сведениями и использовать только те ресурсы информационной системы, которые определены Реестром прав доступа;

−соблюдать порядок работы и меры по защите ставших ему известными сведений конфиденциального характера;

−соблюдать правила работы с носителями информации, содержащей персональные данные, порядок их учета и хранения, обеспечивать в процессе работы сохранность сведений, содержащихся в них от посторонних лиц;

−незамедлительно в письменной форме, информировать руководителя Общества о попытках несанкционированного доступа к информационным ресурсам и сведениям, содержащим персональные данные, о попытках подкупа, угроз, шантажа другими лицами с целью получения доступа к указанной информации;

−давать письменные объяснения о допущенных личных нарушениях установленного порядка работы, учета и хранения документов, содержащих персональные данные, и машинных съемных носителей информации, а также о фактах их утраты, передачи другим лицам.

3.3.1.5. Определение ограничений для работников Общества при работе с персональными данными.

Работнику, допущенному к работе с информацией, содержащей персональные данные, запрещается:

−передавать сведения конфиденциального характера и документы (в устной форме, по телефону, на бумажных и машинных носителях, в электронной виде и т.д.) другим лицам;

−использовать информацию, содержащую персональные данные, в открытой переписке, статьях и выступлениях, а также в личных интересах;

−передавать по незащищенным техническим каналам связи, в том числе сообщать (обсуждать) по телефону сведения, содержащие персональные данные;

−снимать копии с документов, содержащих персональные данные, или производить выписки из них;

−копировать документы Общества, содержащие персональные данные, и хранить их на машинных съемных носителях информации, а также использовать различные технические средства, способные накапливать и хранить информацию в электронном виде

(фото, видео и звукозаписывающую аппаратуру, сотовые телефоны и т.п.), за исключением случаев, описанных в настоящем Положении;

−выполнять работы с материальными и машинными носителями, содержащими персональные данные, вне служебных помещений (помещений, где размещены подразделения Общества);

−выносить из служебных помещений документы и машинные носители с информацией, содержащей персональные данные.

3.3.2. Назначение лица, ответственного за информационную безопасность.

Приказом руководителя Общества назначается лицо, ответственное за информационную безопасность. В число его обязанностей входят:

−организация процесса реализации норм, установленных настоящим Положением, в том числе обеспечение работы системы защиты информации, содержащей персональные данные;

−обеспечение применения в Обществе определенных мер защиты информации, содержащей персональные данные;

−контроль за соблюдением работниками Общества требований настоящего Положения;

−ознакомление работников Общества с требованиями настоящего Положения;

−сбор и анализ статистических данных об Актуальных угрозах безопасности, характерных для Общества;

−внесение предложений руководителю Общества о необходимости проведения оценки достаточности принятых мер по защите информации, содержащей персональные данные, предложений по внесению изменений во внутренние документы Общества, регламентирующие деятельность Общества по защите информации, содержащей персональные данные, предложений по иным вопросам, связанным с деятельностью Общества по защите информации, содержащей персональные данные.

3.3.3. Определение порядка передачи персональных данных.

1) Информация, содержащая персональные данные, может быть передана третьим лицам по письменному запросу третьего лица и только с письменного разрешения руководителя Общества, при условии соблюдения требований действующего законодательства:

−по требованию органов государственной власти и местного самоуправления, государственных, надзорных и контролирующих органов, а также участников Общества в соответствии с действующим законодательством;

−работникам Общества в соответствии с учредительным документом Общества;

−другим физическим и юридическим лицам на основании гражданско-правовых договоров, заключенных между ними и Обществом, при условии наличия в этих договорах обязательств по соблюдению режима конфиденциальности в отношении информации, ответственности за разглашение этой информации или заключения с ними отдельного договора о конфиденциальности.

2) При передаче персональных данных Общество должно соблюдать следующие требования:

−не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных за исключением случаев, когда это необходимо в целях

предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных законодательством Российской Федерации;

–предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они получены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

–передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций;

3.3.4. Обеспечение сохранности носителей информации.

3.3.4.1. Режим сохранности материальных носителей информации.

1) Доступ к материальным носителям информации, содержащей персональные данные, имеют только те работники Общества, которым такая информация необходима для выполнения должностных обязанностей.

2) Доступ к материальным носителям информации, содержащей персональные данные, посторонним лицам запрещен.

3) Рабочие места работников размещаются таким образом, чтобы исключить возможность обозрения находящихся на столе документов, а также мониторов компьютеров посторонними лицами.

4) Материальные носители, содержащие персональные данные должны храниться в специальных сейфах или запирающихся металлических шкафах.

5) Персональные данные, обработка, которых осуществляется в различных целях, хранятся раздельно.

3.3.4.2. Режим сохранности машинных носителей информации.

1) Учет машинных носителей информации осуществляется лицом, ответственным за информационную безопасность, путем ведения журнала учета машинных носителей информации. В журнале учета машинных носителей информации каждый машинный носитель информации Общества закрепляется за ответственным работником, который не вправе передавать закрепленный за ним машинный носитель информации третьим лицам.

2) Запрещается копирование файлов с информацией, содержащей персональные данные, и хранение их на жестких дисках рабочих станций (компьютеров, ноутбуков), съемных машинных носителях информации, других устройствах, способных накапливать и хранить информацию в электронном виде, за исключением случаев, описанных в настоящем Положении.

3) Общество приобретает съемные машинные носители информации, способные накапливать и хранить информацию, для использования работниками Общества в рабочих целях. Такие машинные носители должны проверяться на наличие вирусов и вредоносных программ на регулярной основе.

3.3.5. Установление режима использования Криптографических ключей.

3.3.5.1. Общество осуществляет учет Криптографических ключей путем закрепления права их использования за определенным должностным лицом в Реестре прав доступа. При этом каждый Криптографический ключ используется только руководителем Общества или работником, должность которого определена в Реестре прав доступа.

3.3.5.2. Передача Криптографических ключей, в случае если Криптографический ключ размещен на материальном носителе, не допустима.

3.3.5.3. Криптографические ключи должны использоваться Обществом в соответствии с технической документацией.

3.3.6. Установление режима обеспечения безопасности помещений.

3.3.6.1. В целях исключения возможности неконтролируемого проникновения или пребывания в помещениях, в которых обрабатывается и(или) хранится информация, содержащая персональные данные, посторонних лиц Общества устанавливает режим обеспечения безопасности этих помещений.

3.3.6.2. Требования к помещениям, в которых обрабатывается и(или) хранится информация, содержащая персональные данные, а также правила доступа к таким помещениям устанавливаются в локальном нормативном акте по обеспечению безопасности помещений, которое утверждается руководителем.

3.3.7. Обнаружение фактов несанкционированного доступа к персональным данным, а также фактов нарушения работниками режима конфиденциальности и принятие мер.

3.3.7.1. Общество принимает меры по обнаружению фактов несанкционированного доступа путем:

–установления обязанности работников сообщать о фактах, свидетельствующих о несанкционированном доступе к информации, содержащей персональные данные, в том числе о фактах несанкционированного проникновения в помещения, в которых обрабатывается и(или) хранится информация, содержащая персональные данные;

–применения технических средств обнаружения фактов несанкционированного доступа в информационную систему.

3.3.7.2. Каждый факт несанкционированного доступа фиксируется лицом, ответственным за информационную безопасность, в определенном им порядке.

3.3.7.3. По всем фактам нарушений работниками режима конфиденциальности должны быть проведены расследования, в ходе которых определен круг лиц, виновных в этих нарушениях и причастных к ним, а также причины и условия, способствовавшие совершению данных нарушений. К проведению расследования привлекается лицо, ответственное за информационную безопасность.

3.3.7.4. По каждому факту несанкционированного доступа к персональным данным, а также факту нарушения работниками режима конфиденциальности проводится анализ причин и условий, совершению указанных фактов, по результатам которого составляется заключение, содержащее дополнительные меры по защите персональных данных, а также план по реализации данных мер, включающий сроки их реализации и ответственных лиц.

3.3.7.5. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, с момента выявления такого инцидента самим Обществом или уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом, Общество уведомляет уполномоченный орган по защите прав субъектов персональных данных:

–в течение 24 (двадцати четырех) часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о представителе Общества, уполномоченном на взаимодействие с

уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

–в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

3.4. Технические меры по защите персональных данных:

3.4.1. Приобретение и установка антивирусного программного обеспечения. Обязательным условием для приобретения антивирусного программного обеспечения является наличие лицензии. Антивирусное программное обеспечение должно регулярно обновляться в соответствии с последней версией. Антивирусное программное обеспечение устанавливается на все персональные компьютеры информационной системы Общества.

3.4.2. Создание учетных записей для работников Общества. Каждому пользователю информационной системы Общества, работающему с информацией, содержащей персональные данные, присваиваются личная учетная запись, для входа в которую устанавливается пароль. Пароль для входа в учетную запись не может совпадать с паролем для входа в учетные записи иных работников Общества. Пароль для входа в учетную запись не может передаваться третьим лицам, за исключением случаев, установленных настоящим Положением.

3.4.3. Установление режима защиты сетевого взаимодействия. Обмен данными между элементами информационной системы Общества и другими компьютерами (рабочими станциями, серверами) должен быть организован через защищенные соединения, организованные с использованием протоколов IPSec с проверкой подлинности и шифрованием IP-пакетов.

3.4.4. Осуществление Резервного копирования информации, содержащей персональные данные.

3.4.5. Ограничение доступа к Информационно-коммуникационной сети Интернет.

3.4.6. Пользователям информационной системы Общества (учетным записям пользователей), работающим с информацией, содержащей персональные данные, может быть ограничен доступ к сети Интернет и средствам электронной почты.

3.4.7. Применение технических средств, обеспечивающих восстановление модифицированной или уничтоженной вследствие несанкционированного доступа информации, содержащей персональные данные.

3.5. Проведение оценки эффективности принятых мер по защите информации, содержащей персональные данные.

3.5.1. Оценка эффективности принятых мер по защите информации, содержащей персональные данные, может проводиться Обществом самостоятельно или с привлечением сторонней организации.

3.5.2. Оценка эффективности принятых мер по защите информации, содержащей персональные данные, проводится по результатам внутренней проверки, проводимой лицом, ответственным за информационную безопасность.

Приказом руководителя утверждаются периодичность проведения проверок (но не реже одного раза в год), сроки проведения плановых проверок, а также их содержание.

По результатам проведения проверок составляется письменный отчет, который должен содержать:

–сведения обо всех фактах несанкционированного доступа к информации, содержащей персональные данные, нарушения работниками режима конфиденциальности;

−предложения по внесению изменений в систему защиты информации, содержащей персональные данные, и представляет руководителю Общества заключение о проведении оценки достаточности принятых мер по защите информации, содержащей персональные данные.

В случае подтверждения недостаточности принятых мер по защите информации, содержащей персональные данные, руководитель Общества принимает решение о необходимости применения дополнительных мер по изменению системы защиты информации, содержащей персональные данные, в целях приведения ее к достаточному уровню.

Контроль за соблюдением работниками Общества требований, предъявляемых к ним и установленных настоящим Положением, осуществляется лицом, ответственным за информационную безопасность.

4. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

4.1. Лица, виновные в нарушении порядка обращения с персональными данными, несут предусмотренную законодательством Российской Федерации ответственность.

4.1.1. Дисциплинарная ответственность:

a) Разглашение персональных данных субъекта персональных данных Общества, то есть передача посторонним лицам, не имеющим к ним доступа; публичное раскрытие; утрата документов и иных носителей, содержащих персональные данные работника; иные нарушения обязанностей по их защите, обработке и хранению, установленных настоящим Положением, а также иными локальными нормативными актами Общества, лицом, ответственным за получение, обработку и защиту персональных данных работника, влекут наложение на него дисциплинарного взыскания - выговора, увольнения (пп. «в» п.6 ч. 1 ст. 81 Трудового кодекса РФ).

b) В случае причинения ущерба Обществу работник, имеющий доступ к персональным данным сотрудников и совершивший указанный дисциплинарный поступок, несет полную материальную ответственность в соответствии с п. 7 ч. 1 ст. 243 Трудового кодекса РФ.

4.1.2. Административная ответственность:

a) За нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11 КоАП РФ).

b) За разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

4.1.3. Уголовная ответственность – за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения.

Приложение № 1
к Положению о защите персональных данных работников, клиентов и контрагентов ООО «Кредиска МКК»

Реестр
определения прав доступа к конфиденциальной информации

№ п/п	Должность	Категории Информации, к которым сотрудник имеет доступ, цель	Ресурсы информационной системы, к которым сотрудник имеет доступ, цель	Криптографические ключи, к которым сотрудник имеет доступ, цель
1	Директор, сотрудники ООО «Кредиска МКК»	Конфиденциальная информация о контрагентах и клиентах организации, о финансовых операциях, совершаемых организацией, ее контрагентами и клиентами, в том числе в электронном виде. Информация, содержащая персональные данные клиентов, контрагентов и сотрудников.	Доступ к программному обеспечению. Доступ к личному кабинету участника финансового рынка на официальном сайте Банка России – направление отчетности в Банк России. Доступ к личному кабинету на сайте Росфинмониторинга – направление отчетности в Росфинмониторинг. Доступ к личному кабинету на сайте службы Финансового Уполномоченного кабинет участника информационного обмена. Доступ к личному кабинету на сайте СРО «МиР» кабинет члена информационного обмена Доступ к программному обеспечению– взаимодействие с клиентом в рамках рассмотрения заявлений, обращений.	Ключ квалифицированной электронной подписи на ключевом носителе

Приложение № 2 к Положению о защите персональных данных работников, клиентов и контрагентов
ООО «Кредиска МКК»

Журнал учёта машинных носителей информации

№ п/п	Дата регистрации	Вид носителя	Тип носителя	Наименование отдела организации, цель использования	Ф.И.О., должность работника, получившего машинный носитель в пользование	Дата и подпись работника в получении машинного носителя	Дата возврата и подпись уполномоченного работника в получении машинного носителя от работника	Дата и подпись уполномоченного работника и исполнителя об уничтожении машинного носителя
1	2	3	4	5	6	7	8	9
1	дд.мм.гггг					дд.мм.гггг _____ (личная подпись)	_____ (личная подпись)	_____ (личная подпись)
2	дд.мм.гггг					дд.мм.гггг _____ (личная подпись)	_____ (личная подпись)	_____ (личная подпись)

Пояснения:

В графе 1 проставляется арабскими цифрами порядковый номер машинного носителя. Нумерация сквозная.

В графе 2 дата проставляется арабскими цифрами, с указанием числа, месяца и года приобретения машинного носителя.

В графе 3 проставляется: магнитный диск, дискета, оптический диск, USB-флеш-накопитель и т.д.

В графе 4 пишется название (марка) носителя.

В графе 5 указывается наименование отдела организации, в котором планируется использование машинного носителя информации, и цель использования.

В графе 6 проставляется должность и фамилия, имя и отчество (при наличии) полностью сотрудника, получившего машинный носитель в пользование.

В графе 7 дата проставляется арабскими цифрами, с указанием числа, месяца и года получения машинного носителя сотрудником и его личная подпись

В графе 8 дата проставляется арабскими цифрами, с указанием числа, месяца и года возврата машинного носителя сотрудником и личная подпись уполномоченного сотрудника.

В графе 9 дата проставляется арабскими цифрами, с указанием числа, месяца и года уничтожения машинного носителя уполномоченным сотрудником и его личная подпись.

Журнал распечатывается и заполняется от руки уполномоченным сотрудником, назначенным приказом руководителя организации. Изменения в журнале допустимы. При этом при внесении изменений в Журнал уполномоченный сотрудник ставит свою подпись и дату внесения изменений. Все изменения доводятся до непосредственного руководителя.