УТВЕРЖДЕНО
приказом директора
ООО МКК «СЗЦ» № 5 от 26.06.2024 года
м.п. _____Кофанов

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ, КЛИЕНТОВ И КОНТРАГЕНТОВ ООО МКК «СИБИРСКИЙ ЗАЛОГОВЫЙ ЦЕНТР»

2024 год

1. ОБЩИЕ ПОЛОЖЕНИЯ

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

1.2. Целью настоящего Положения является защита персональных данных работников, клиентов и контрагентов ООО МКК «СЗЦ» (далее – «Общество») от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Настоящее Положение разработано в соответствии с Конституцией РФ, главы 14 Трудового Кодекса РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным Законом «О противодействии легализации (отмыванию денежных средств, полученных преступным путем и финансирования терроризма» № 115-ФЗ от 07.08.2001 г., Федеральным законом от 27.07.2006 № 149-ФЗ «Об информатизации, информационных технологиях и о защите информации», 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 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными актами, действующими на территории Российской Федерации.

1.4. В настоящем Положении используются следующие термины и определения:

Оператор – ООО МКК «СЗЦ» (далее – Общество), вступившее в договорные отношения с работником, клиентом или контрагентом или оказывающее услуги физическому лицу, юридическому лицу или индивидуальному предпринимателю.

Клиент – физическое лицо, официальный представитель – физическое лицо юридического лица и индивидуального предпринимателя, вступившее в договорные отношения с Обществом в сфере микрофинансовой деятельности.

Контрагент – физическое лицо, представитель – физическое лицо юридического лица и индивидуального предпринимателя, вступившие с Обществом в договорные отношения в сфере хозяйственной деятельности.

Персональные данные Клиента – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Клиента, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, паспортные данные, социальное положение, имущественное положение, образование, профессия, специальность, занимаемая должность, доходы, ИНН, сведения ВУС, СНИЛС, сведения о трудовом и общем стаже, адрес электронной почты, телефон, место работы или учебы членов семьи и родственников, состав декларируемых сведений о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию, налоговый статус (резидент/нерезидент), иные сведения указанные заявителем.

Персональные данные Контрагента – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Контрагента, в том числе фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, паспортные данные, социальное положение, имущественное положение, образование, профессия, специальность, занимаемая должность, доходы, ИНН, сведения ВУС, СНИЛС, сведения о трудовом и общем стаже, адрес электронной почты, телефон, место работы или учебы членов семьи и родственников, состав декларируемых сведений о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию, налоговый статус (резидент/нерезидент), иные сведения указанные заявителем.

Персональные данные Работника - информация, необходимая Обществу, как работодателю, в связи с трудовыми отношениями и касающиеся конкретного работника.

Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность, в том числе: фамилия, имя, отчество; образование; сведения о трудовом и общем стаже; сведения о составе семьи; паспортные данные; сведения о воинском учете; ИНН; налоговый статус (резидент/нерезидент); сведения о заработной плате работника; сведения о социальных льготах; специальность; занимаемая должность; адрес места жительства; телефон; место работы или учебы членов семьи и родственников; характер взаимоотношений в семье; содержание трудового договора; состав декларируемых сведений о наличии материальных ценностей; содержание декларации, подаваемой в налоговую инспекцию; иную, не указанную выше информацию, содержащуюся в личных делах и трудовых книжках сотрудников; информацию, являющуюся основанием к приказам по личному составу; информацию, содержащуюся в страховом свидетельстве обязательного пенсионного страхования, свидетельстве о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации, страховом медицинском полисе обязательного медицинского страхования граждан, медицинском заключении установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на работу в Общество; медицинское заключение о состоянии здоровья, дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям.

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 – Работник, Клиент, Контрагент.

Защита персональных данных Работника, Клиента, Контрагента – 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 - это 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.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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.

Электронные сообщения – информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками Общества и (или) клиентами Общества.

1.4. Персональные данные работников Общества относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законодательством Российской Федерации.

1.5. Действия настоящего Положения распространяется на всех Работников, Клиентов и Контрагентов Общества.

1.6. Настоящее Положение вступает в силу с момента его утверждения приказом директором Общества

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные - информация, необходимая в целях исполнения Обществом обязательств, возникших из трудовых отношений с работниками, из гражданско-правовых отношений с клиентами и контрагентами. Под информацией понимаются сведения о фактах, событиях и обстоятельствах жизни субъекта персональных данных, позволяющие идентифицировать его личность.

2.2. В состав персональных данных работника входят:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес регистрации по месту жительства (почтовый адрес);
- адрес фактического проживания (почтовый адрес фактического проживания);
- семейное положение;
- паспортные данные;
- социальное положение;
- адрес электронной почты, телефон;
- данные свидетельства о заключении брака;
- данные свидетельства о расторжении брака;
- данные свидетельства о рождении детей;

- сведения о стаже работы и о местах работы (город, название организации, должность, сроки работы);
- сведения о наградах (поощрениях), почетных званиях;
- данные страхового свидетельства государственного пенсионного страхования (СНИЛС);
- данные свидетельства о постановке на учет в налоговом органе физического лица (ИНН);
- данные полиса медицинского страхования;
- сведения об образовании, повышении квалификации, профессиональной переподготовки и местах обучения (город, образовательное учреждение, сроки обучения, специальность, квалификация, профессия);
- сведения о наличии льгот и гарантий, предоставляемых в соответствии с действующим законодательством;
- сведения о доходах;
- данные документов воинского учета – для военнообязанных и лиц, подлежащих призыву на воинскую службу;
- сведения медицинского характера.

2.3. В состав персональных данных клиентов входят:
- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- паспортные данные;
- данные страхового свидетельства государственного пенсионного страхования (СНИЛС);
- данные свидетельства о постановке на учет в налоговом органе физического лица (ИНН);
- образование;
- место работы или учебы;
- занимаемая должность;
- сведения о трудовом стаже;
- сведения о доходах;
- семейное положение;
- телефон;
- адрес электронной почты.

2.4. В состав персональных данных контрагентов входят:
- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- паспортные данные;
- данные страхового свидетельства государственного пенсионного страхования (СНИЛС);
- данные свидетельства о постановке на учет в налоговом органе физического лица (ИНН);
- адрес электронной почты;
- телефон.

Обществом не производится обработка специальных категорий персональных данных и биометрических персональных данных.

3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. В целях обеспечения прав и свобод человека и гражданина Общество и (или) его представители при обработке персональных данных должны соблюдаться следующие общие требования:

3.1.1. 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 РФ;

3.1.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.1.3. Получение Обществом персональных данных может осуществляться как путем представления их самим работником, клиентом, контрагентом так и путем получения их из иных источников.

31.4. Персональные данные получаются Обществом непосредственно у самого работника, клиента, контрагента. Если персональные данные работника 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 последствиях отказа дать письменное согласие на их получение.

3.1.5. Общество не имеет права получать и обрабатывать персональные данные работника, клиента, контрагента о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни работника, клиента, контрагента (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны Обществом только с его письменного согласия.

3.1.6. Общество не имеет право получать и обрабатывать персональные данные работника, клиента, контрагента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.2. К обработке, передаче и хранению персональных данных могут иметь доступ:

- Директор Общества;
- Главный бухгалтер;
- Руководители структурных подразделений (при наличии).
- сам работник, источник данных;
- другие сотрудники организации при выполнении ими своих служебных обязанностей – на основании приказа.

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

Персональные данные 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.

3.4. При принятии решений, затрагивающих интересы клиента или контрагента, Оператор не имеет права основываться на персональных данных клиента или контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.

3.5. При идентификации клиента или контрагента Общества может затребовать предъявления документов, удостоверяющих личность и подтверждающих полномочия представителя.

3.6. При заключении договора, как и в ходе выполнения договора может возникнуть необходимость в предоставлении клиентом или контрагентом иных документов, содержащих информацию о нем.

3.7. После принятия решения о заключении договора или представления документов, подтверждающих полномочия представителя, а так же впоследствии, в процессе выполнения договора, содержащего персональные данные клиента или контрагента, так же будут относиться:

- договоры;
- приказы по основной деятельности;
- служебные записки;
- приказы о допуске представителей клиента, контрагента;
- разовые или временные пропуска;
- другие документы, где включение персональных данных клиента или контрагента необходимо согласно действующему законодательству.

3.8. Передача персональных данных возможна только с согласия работника, клиента, контрагента или в случаях, прямо предусмотренных законодательством Российской Федерации.

3.8.1. При передаче персональных данных Общество должно соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия работника, клиента, контрагента за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, клиента, контрагента а также в случаях, установленных законодательством Российской Федерации;
- не сообщать персональные данные в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном законодательством Российской Федерации;
- разрешать доступ к персональным данным только специально уполномоченным лицам, определенным приказом директора Общества, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.8.2. Передача персональных данных от Общества и (или) его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

3.8.3. При передаче персональных данных внешним потребителям (в том числе и в коммерческих целях) Общество не должно сообщать эти данные третьей стороне без письменного согласия работника, клиента, контрагента за исключением случаев, установленных законодательством Российской Федерации.

3.9. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.10. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

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

3.12. Период хранения и обработки персональных данных определяется в соответствии с Законом «О персональных данных». Обработка персональных данных начинается с момента поступления персональных данных в информационные системы персональных данных и прекращается:
- в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, Общество устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений, Общество в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные.
Об устранении допущенных нарушений или об уничтожении персональных данных Общество
уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;
- в случае достижения цели обработки персональных данных Общество незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, и уведомляет об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом
по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Общество прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных Общество уведомляет субъекта персональных данных.
- в случае прекращения деятельности Общества.
3.13. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».
3.14. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.
3.15. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

4. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ, РАЗРЕШЕННЫХ СУБЪЕКТОМ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ РАСПРОСТРАНЕНИЯ

4.1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.
Общество обеспечивает субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.
4.2. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных Обществом неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.
4.3. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.
4.4. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.
4.5. Общество в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных публикует информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.
4.6. Общество в любое время по требованию субъекта персональных данных прекращает передачу (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения.
Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления Обществу требования, указанного п. 4.6 настоящего Положения.

5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обществом определено, что на информацию, содержащую персональные данные, распространяется режим конфиденциальности.
5.2. Организация работы по защите Конфиденциальной информации, в том числе персональных данных.
5.2.1. 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».
5.2.2. 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 директора 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.

5.2.3. В целях обеспечения функционирования системы защиты директор 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.

5.2.4. Защите подлежат все персональные данные, определенные п. 2 настоящего Положения, 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.

5.3. Правовые меры защиты персональных данных.

5.3.1. К правовым мерам защиты персональных данных относится:

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

2) Обязанность Общества осуществлять мониторинг действующего законодательства.

5.3.2. Регламентирующие документы разрабатываются самим Обществом или с привлечением третьих лиц и утверждаются директором Общества.

5.3.3. 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.

5.4. Организационные меры защиты персональных данных.

К организационным мерам защиты персональных данных относятся:

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

5.4.1.1. 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.

5.4.1.2. Приказом директора 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 директор Общества.
5.4.1.3. 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.
5.4.1.4. 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 директора 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.
5.4.1.5. 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.

5.4.2. Назначение лица, ответственного за информационную безопасность.

Приказом директора 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;
– проведение обучений для работников Общества в целях ознакомления с требованиями настоящего Положения;
– сбор и анализ статистических данных об Актуальных угрозах безопасности, характерных для Общества;
– внесение предложений директору 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.

5.4.3. Определение порядка передачи персональных данных.

5.4.3.1. Информация, содержащая персональные данные, может быть передана третьим лицам по письменному запросу третьего лица и только с письменного разрешения директора 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.

5.4.3.2. 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;

5.4.4. Обеспечение сохранности носителей информации.

5.4.4.1. 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.

5.4.4.2. 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.

5.4.5. Установление режима использования Криптографических ключей.

5.4.5.1. 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 директором Общества или работником, должность которого определена в Реестре прав доступа.
5.4.5.2. Передача Криптографических ключей, в случае если Криптографический ключ размещен на материальном носителе, не допустима.
5.4.5.3. Криптографические ключи должны использоваться Обществом в соответствии с технической документацией.
5.4.6. Установление режима обеспечения безопасности помещений.
5.4.6.1. 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.
5.4.6.2. 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 директором.
5.4.7. Обнаружение фактов несанкционированного доступа к персональным данным, а также фактов нарушения работниками режима конфиденциальности и принятие мер.
5.4.7.1. 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.
5.4.7.2. Каждый факт несанкционированного доступа фиксируется лицом, ответственным за информационную безопасность, в определенном им порядке.
5.4.7.3. 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.
5.4.7.4. 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.
5.5. Технические меры по защите персональных данных:
5.5.1. 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.
5.5.2. 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.

5.5.3. 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.

5.5.4. Осуществление Резервного копирования информации, содержащей персональные данные.

5.5.5. Ограничение доступа к Информационно-коммуникационной сети Интернет.

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

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

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

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

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

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

5.6.4. 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 директору Общества заключение о проведении оценки достаточности принятых мер по защите информации, содержащей персональные данные.

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

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

6. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА

6.1. Работники и их представители должны быть ознакомлены под расписку с документами Общества, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.
6.2. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

6.3. Работник обязан:

- передавать Обществу и (или) его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации.
- своевременно сообщать Обществу об изменении своих персональных данных.

6.4. Работники ставят Общество в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.
65. В целях защиты частной жизни, личной и семейной тайны работники вправе отказываться от обработки персональных данных без их согласия.

7. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТОВ И КОНТРАГЕНТОВ

7.1. В целях обеспечения защиты персональных данных, хранящихся у Оператора, клиенты и контрагенты имеют право на:
7.1.1. Полную информацию о составе персональных данных и их обработке, в частности клиент или контрагент имеет право знать, кто и в каких целях использует или использовал информацию о его персональных данных.
7.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные клиента или контрагента, за исключением случаев, предусмотренных законодательством РФ.
7.1.3. Определение своих представителей для защиты своих персональных данных.
7.1.4. Требование об исключении или исправлении неверных или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Оператора персональных данных. При отказе Оператора исключить или исправить персональные данные клиента или контрагента он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия.
7.1.5. Требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные клиента или контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях.
7.1.6. Обжалование в суд любых неправомерных действий или бездействия Оператора при обработке и защите его персональных данных.
7.1.7 Требование прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных для распространения.

7.2. В целях обеспечения достоверности персональных данных, клиент и контрагент обязан:

7.2.1. При заключении договора предоставить Оператору полные и достоверные данные о себе;
7.2.2. В случае изменения сведений, составляющих персональные данные клиента или контрагента, незамедлительно, но не позднее пяти рабочих дней, предоставить данную информацию Оператору.

8. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РАБОТНИКОВ

8.1. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
8.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.
8.3. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.
8.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.
8.4.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера Общество вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.
8.4.2. Должностные лица, в обязанность которых входит обработка персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.
8.4.3. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.
8.4.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего 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 вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом.
8.5. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

9. ОБЯЗАННОСТИ РАБОТНИКОВ ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

9.1. В целях охраны конфиденциальности информации все работники обязаны:
9.1.1. Не разглашать сведения, составляющие коммерческую тайну Общества, за исключением случаев, когда есть письменное согласие директора Общества.
9.1.2. Не использовать сведения, составляющие коммерческую тайну Общества, для занятия другой деятельностью, в процессе работы для другой организации, предприятия, учреждения, по заданию физического лица или в ходе осуществления предпринимательской деятельности, а также в личных целях.
9.1.3. Выполнять установленный Обществом режим коммерческой тайны.
9.1.4. Незамедлительно ставить в известность непосредственного руководителя и директора Общества о необходимости отвечать либо об ответах на вопросы должностных лиц компетентных органов (налоговая инспекция, органы предварительного следствия и т.п.), находящихся при исполнении служебных обязанностей, по вопросам коммерческой тайны Общества.
9.1.5. Незамедлительно сообщать непосредственному руководителю и директору Общества об утрате или недостаче носителей информации, составляющей коммерческую тайну, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению коммерческой тайны Общества, а также о причинах и условиях возможной утечки информации, составляющей коммерческую тайну Общества.
8.1.6. В случае попытки посторонних лиц получить от работника сведения, содержащие коммерческую тайну Общества, незамедлительно известить об этом непосредственного руководителя и директора Общества.
9.1.7. Не создавать условия для утечки информации, составляющей коммерческую тайну, и предпринимать все усилия для пресечения такой утечки, если ему стало известно, что утечка имеет место или что складываются условия для возможности таковой.
9.1.8. Не разглашать и не использовать для себя или других лиц коммерческую тайну в течение трех лет после прекращения трудового договора с Обществом (независимо от причин увольнения).
9.1.9. Передать Обществу при прекращении трудового договора или гражданско-правового договора имеющиеся в пользовании работника материальные носители с информацией, составляющей коммерческую тайну.
9.1.10 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной ответственности. К данным лицам могут быть применены следующие дисциплинарные взыскания:
а) замечание; б) выговор; в) предупреждение о неполном должностном соответствии; г) освобождение от занимаемой должности; д) увольнение.
9.1.11. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.
9.1.12. Копия приказа о применении к работнику дисциплинарного взыскания с указанием оснований его применения вручается работнику под расписку в течение пяти дней со дня издания приказа.
9.1.13. Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Работодатель до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с работника по собственной инициативе, по письменному заявлению работника или по ходатайству его непосредственного руководителя.