УТВЕРЖДАЮ:
Директор Фонда финансирования промышленности
и предпринимательства Челябинской области
– Центр «Мой бизнес» (микрокредитная компания)

Приказ №6 от «22» мая 2023г.

_____ (Е.А. Вахитова)
М.П.

П О Л О Ж Е Н И Е
«О защите персональных данных Клиентов/Контрагентов/Работников Фонда финансирования промышленности и предпринимательства Челябинской области – Центр «Мой бизнес» (микрокредитная компания)»

2023

I. Общие положения

1.1. Положение «О защите персональных данных Клиентов/Контрагентов/Работников Фонда финансирования промышленности и предпринимательства Челябинской области – Центр «Мой бизнес» (микрокредитная компания)» (далее – Положение) определяет порядок обработки включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение, распространение (в том числе передачу при сотрудничестве с третьими лицами) и защиты персональных данных клиентов/контрагентов/Работников Фонда финансирования промышленности и предпринимательства Челябинской области – Центр «Мой бизнес» (микрокредитная компания) (далее – Фонд).

1.2. Настоящее Положение разработано в соответствии с Конституцией РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее по тексту – Федеральный закон №152-ФЗ), Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Федеральным законом от 30.12.2004 № 218-ФЗ «О кредитных историях», 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 правовыми актами РФ.

1.3. Целями настоящего Положения являются создание и определение условий для сбора, обработки, хранения, блокирования, уничтожения, обезличивания, распространения и предоставления персональных данных, характеризующих своевременность исполнения Клиентами/Контрагентами/Работниками своих обязательств по договорам микрозайма/договорам залога/договорам поручительства, повышения защищенности Фонда и Клиентов/Контрагентов за счет общего снижения кредитных рисков, повышения эффективности работы Фонда.

1.4. В настоящем Положении используются следующие термины и определения:

«Защита персональных данных Клиента/Контрагента/Работника» – деятельность Фонда по обеспечению с помощью локального регулирования порядка обработки включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение, распространение (в том числе передачу при сотрудничестве с третьими лицами) и защиты персональных данных Клиентов/Контрагентов/Работников Фонда и организационно-технических мер обеспечения конфиденциальности информации.

«Клиент» – физическое лицо, в т.ч. официальный представитель юридического лица и (или) индивидуального предпринимателя, вступившее/намеревающееся вступить в договорные отношения с Фондом.

«Контрагент» – физическое лицо, в т.ч. официальный представитель юридического лица и (или) индивидуального предпринимателя, вступившие/намеревающееся вступить в договорные отношения с Фондом.

«Работник» - физическое лицо, состоящее в трудовых отношениях (планирующее вступить в трудовые отношения) с Фондом.

«Конфиденциальность персональных данных» – обязательное для соблюдения Фондом, получившим доступ к персональным данным Клиента/Контрагента/Работника, требование не допускать их обработки включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение, распространение (в том числе передачу при сотрудничестве с третьими лицами) без согласия субъекта персональных данных или наличия иного на это законного основания.

«Оператор, Фонд» – Фонд, самостоятельно или совместно с другими лицами (при сотрудничестве с третьими лицами) организующий и (или) осуществляющий обработку включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение),

использование, обезличивание, блокирование, уничтожение, распространение (в том числе передачу при сотрудничестве с третьими лицами) персональных данных Клиента/Контрагента, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

«Обработка персональных данных» – любое действие (операция) или совокупность действий (операций), совершаемых Фондом 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 Клиента/Контрагента.

«Персональные данные» - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу – Клиенту/Контрагенту (субъекту персональных данных).

«Персональные данные Клиента/Контрагента/Работника» – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Клиента/Контрагента/Работника, 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, кредитная история, 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 или бухгалтерской отчётности, подаваемой в налоговую инспекцию, налоговый статус (резидент/нерезидент), иные сведения указанные Клиентом/Контрагентом/Работником.

«Пароль» – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

«Субъект персональных данных» («Субъект») – Клиент/Контрагент/Работник.

1.5. Действия настоящего Положения распространяется на всех сотрудников Фонда, на Клиентов/Контрагентов/Работников Фонда.

1.6. Фонд в своей деятельности не осуществляет трансграничную передачу персональных данных.

1.7. Фонд в своей деятельности не осуществляет сбор и обработку биометрических персональных данных.

II. Правила предоставления доступа работников Фонда к персональным данным

2.1. Список работников Фонда, допущенных к обработке персональных данных (далее - Список) и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение правил обработки персональных данных, определяется и утверждается приказом директора Фонда.

2.2. Ответственное лицо по работе с персоналом при принятии на работу, увольнении или изменении должностных обязанностей работников Фонда не позднее чем в трехдневный срок вносит изменения в список лиц, допущенных к обработке персональных данных.

2.3. Ответственное лицо по работе с персоналом Фонда не реже одного раза в квартал, обязано проверять актуальность Списка. В случае выявления расхождений, ответственное лицо по работе с персоналом не позднее чем в трехдневный срок вносит соответствующие изменения в Список.

2.4. Работники Фонда выполняют действия по обработке персональных данных Клиентов/Контрагентов в соответствии с возложенными на них функциями.

2.5. Работники Фонда, уполномоченные на обработку персональных данных Клиентов/Контрагентов, обеспечивают обработку персональных данных в соответствии с

требованиями законодательства РФ, других нормативных правовых актов Российской Федерации и несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.
2.6. Доступ к персональным данным Клиентов/Контрагентов предоставляется только лицам, замещающим должности из Списка.
2.7. Работники Фонда имеют право на ввод и корректировку персональных данных Клиентов/Контрагентов в пределах, определенных их должностными обязанностями.
2.8. Лица, получившие доступ к персональным данным Клиентов/Контрагентов, должны использовать эти данные лишь в целях, для которых они сообщены, обязаны соблюдать режим конфиденциальности и дать обязательство о неразглашении персональных данных.
2.9. Фонд обеспечивает неограниченный доступ к сведениям о реализуемых требованиях к защите персональных данных Клиентов/Контрагентов.
2.10. Фонд представляет всю имеющуюся у него информацию, определенную ст. 4 Федерального закона от 30.12.2004 № 218-ФЗ «О кредитных историях», в отношении всех заемщиков, поручителей, залогодателей, принципалов хотя бы в одно бюро кредитных историй, включенное в государственный реестр бюро кредитных историй, без получения согласия на ее представление, за исключением случаев, в которых Правительством Российской Федерации установлены ограничения на передачу информации в соответствии с ч. 7 ст. 5 Федерального закона от 30.12.2004 N 218-ФЗ «О кредитных историях», а также лиц, в отношении которых Правительством Российской Федерации установлены указанные ограничения.

III. Обработка персональных данных

3.1. Персональные данные Клиента/Контрагента/Работника относятся к категории конфиденциальной информации.
3.2. В целях обеспечения прав и свобод Клиента/Контрагента/Работника Оператор и его представители при обработке персональных данных Клиента/Контрагента обязаны соблюдать следующие общие требования:
3.2.1. Обработка персональных данных Клиента/Контрагента/Работника 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.
3.2.2. Обработка персональных данных Клиента/Контрагента/Работника осуществляется с согласия субъекта персональных данных на обработку его персональных данных за исключением случаев, предусмотренных законодательством Российской Федерации, когда обработка персональных данных допускается без согласия субъекта персональных данных, при условии регламентации вопросов обработки персональных данных соответствующим законодательством Российской Федерации.
3.2.3. Обработка персональных данных Клиента/Контрагента/Работника должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Обработка персональных данных осуществляется Фондом для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных.

3.2.4. Не допускается объединение баз данных, содержащих персональные данные Клиента/Контрагента/Работника, обработка которых осуществляется в целях, несовместимых между собой.
3.2.5. Обработке подлежат только персональные данные Клиента/Контрагента/Работника, которые отвечают целям их обработки.
3.2.6. Содержание и объем обрабатываемых персональных данных Клиента/Контрагента/Работника должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные Клиента/Контрагента/Работника не должны быть избыточными по отношению к заявленным целям их обработки.
3.2.7. При обработке персональных данных Клиента/Контрагента/Работника должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
3.2.8. Хранение персональных данных Клиента/Контрагента/Работника должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством, договором, стороной которого является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством РФ.
3.2.9. Фонд не имеет права получать и обрабатывать персональные данные Клиента/Контрагента/Работника о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных законодательством Российской Федерации.
3.2.10. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда Клиента/Контрагента/Работника, затруднения реализации его прав и свобод.
3.2.11. При принятии решений, затрагивающих интересы Клиента/Контрагента/Работника, Оператор не имеет права основываться на персональных данных Клиента/Контрагента/Работника, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.
3.2.12. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить 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.
3.3. Персональные данные Клиента/Контрагента/Работника, которые обрабатываются в информационных системах Фонда, подлежат защите от несанкционированного доступа и копирования. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.
3.4. При идентификации Клиента/Контрагента/Работника Фонда может затребовать предъявления документов, удостоверяющих личность и подтверждающих полномочия представителя Клиента/Контрагента/Работника.
3.5. При заключении договора, как и в ходе выполнения договора может возникнуть необходимость в предоставлении Клиентом/Контрагентов/Работника иных документов, содержащих информацию о нем.
3.6. После принятия решения о заключении договора или представления документов, подтверждающих полномочия представителя Клиента/Контрагента/Работника, а также

впоследствии, в процессе выполнения договора, содержащего персональные данные Клиента/Контрагента/Работника, так же будут относиться:
- договоры;
- приказы по основной деятельности;
- служебные записки;
- приказы о допуске представителей Клиента/Контрагента/Работника;
- разовые или временные пропуска;
- другие документы, где включение персональных данных Клиента/Контрагента/Работника необходимо согласно действующему законодательству РФ.

3.7. Фонд вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Фонда, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом №152-ФЗ. 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 №152-ФЗ. Лицо, осуществляющее обработку персональных данных по поручению Фонда, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством РФ, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных законодательством РФ. В поручении Фонда должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федерального закона №152-ФЗ, обязанность по запросу Оператора персональных данных в течение срока действия поручения Оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с настоящей статьей, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона, в том числе требование об уведомлении оператора о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона №152-ФЗ.

Лицо, осуществляющее обработку персональных данных по поручению Фонда, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случае, если Фонд поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Фонд. Лицо, осуществляющее обработку персональных данных по поручению Фонда, несет ответственность перед Фондом.

Обработка персональных данных Клиентов/Контрагентов/Работников Фонда также осуществляется Фондом развития предпринимательства Челябинской области – Центр «Мой бизнес» на основании договора аутсорсинга от 01.04.2022 года.

Цель обработки персональных данных Клиентов/Контрагентов/Работников Фонда Фондом развития предпринимательства Челябинской области – Центр «Мой бизнес»: исполнение договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

3.8. Фонд не имеет права поручать кредитной организации на основании договора проведение идентификации или упрощенной идентификации клиента - физического лица.
3.9. Лицо, осуществляющее обработку персональных данных по поручению Оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.
3.10. 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.
3.11. Фонд, Клиенты/Контрагенты/Работники и их представители должны совместно вырабатывать меры защиты персональных данных.
3.12. Персональные данные следует получать лично у Клиентов/Контрагентов/Работников. В случае возникновения необходимости получения персональных данных у третьей стороны следует известить об этом Клиентов/Контрагентов/Работников заранее, получить их письменное согласие и сообщить им о целях, предполагаемых источниках и способах получения персональных данных.
3.13. Согласие Клиента/Контрагента как субъекта кредитной истории, полученное Фондом, сохраняет силу в течение всего срока действия договора микрозайма/займа, заключенного с клиентом в течение установленного срока.
3.14. Запрещается получать, обрабатывать и приобщать к личному делу Клиентов/Контрагентов/Работников не установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 30.12.2004 N 218-ФЗ «О кредитных историях», Федеральным законом от 02.07.2010 № 151-ФЗ «О микрофинансовой деятельности и микрофинансовых организациях» персональные данные об их политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах.
3.15. При принятии решений, затрагивающих интересы Клиентов/Контрагентов/Работников, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей.
3.16. В Фонде установлен следующий порядок получения персональных данных:
- при обращении за микрозаймом/займом Клиент заполняет Анкеты установленной формы (являются приложениями к Правилам предоставления займов субъектам малого и среднего предпринимательства (юридическим лицам) Челябинской области, в том числе осуществляющим деятельность в сфере промышленности, к Правилам предоставления микрозаймов субъектам малого и среднего предпринимательства Челябинской области и к Правилам предоставления микрозаймов физическим лицам и/или индивидуальным предпринимателям, применяющим специальный налоговый режим «Налог на профессиональный доход» (самозанятым) и прикладывает к ней надлежащим образом заверенные необходимые документы. Анкета и приложенные к ней документы помещаются в досье Клиента.
- при обращении физического лица в Фонд с целью установления трудовых отношений, физическое лицо заполняет анкету установленной формы и прикладывает к ней надлежащим образом заверенные необходимые документы. Анкета и приложенные к ней документы помещаются в личное дело Работника.

Согласие Клиента/Контрагента на обработку его персональных данных содержится во внутренних нормативных документах Фонда, утверждаемых коллегиальным органом управления Фонда – Наблюдательный совет Фонда). Согласие Клиента/Контрагента на обработку его персональных данных оформляется в письменной форме на бумажном носителе и является неотъемлемой частью Анкет установленной формы (являются приложениями к Правилам предоставления займов субъектам малого и среднего предпринимательства (юридическим лицам) Челябинской области, в том числе осуществляющим деятельность в сфере промышленности, к Правилам предоставления микрозаймов субъектам малого и среднего предпринимательства Челябинской области и к Правилам предоставления микрозаймов физическим лицам и/или индивидуальным предпринимателям, применяющим

специальный налоговый режим «Налог на профессиональный доход» (самозанятым).
Фонд не имеет права получать и обрабатывать персональные данные Клиента/Контрагента/Работника о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни.
3.17. Письменное согласие Клиента на обработку его персональных данных должно включать в себя:
- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.
3.18. Основания прекращения Фондом обработки персональных данных Клиента/Контрагента/Работника:
- получение Фондом требования Клиента/Контрагента/Работника о прекращении обработки персональных данных;
- получение Фондом отзыва субъектом персональных данных согласия на обработку его персональных данных;
- достижение цели обработки персональных данных;
- получение Фондом решения суда или органа по защите прав субъектов персональных данных о прекращении обработки персональных данных;
- выявление Фондом неправомерной обработки персональных данных.
3.19. Обработка персональных данных Клиентов/Контрагентов/Работников Фонда осуществляется Фондом по следующим адресам:
- Челябинская область, город Челябинск, Российская улица, дом 110, стр1, неж. пом. 6.
- Челябинская область, город Челябинск, Российская улица, дом 110, стр1, неж.пом. №001.
Обработка персональных данных Клиентов/Контрагентов/Работников Фонда осуществляется Фондом развития предпринимательства Челябинской области – Центр «Мой бизнес» по следующим адресам:
- Челябинская область, город Челябинск, Российская улица, дом 110, стр1, неж.пом. №6.
- Челябинская область, город Челябинск, Российская улица, дом 110, стр1, неж.пом. №308.
Данные помещения используются на основании договора аренды.
3.20. Фонд приказом назначает лицо, ответственное за организацию обработки персональных данных.
3.21. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от органов управления Фонда, являющегося Оператором, и подотчетно ему.
3.22. Лицо, ответственное за организацию обработки персональных данных в Фонде, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением Фондом и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
2) доводить до сведения работников Фонда положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

IV. Организация защиты персональных данных

4.1. Все работники Фонда, имеющие доступ к персональным данным Клиентов/Контрагентов/работникам, обязаны подписать соглашение о неразглашении персональных данных.
4.2. Защита персональных данных Клиентов/Контрагентов/Работников от неправомерного их использования или утраты обеспечивается Оператором в порядке, установленном законодательством Российской Федерации.
4.3. Клиенты/Контрагенты до предоставления своих персональных данных должны иметь возможность ознакомиться с настоящим Положением.
4.4. Защите подлежат:
- информация о персональных данных субъекта;
- документы, содержащие персональные данные субъекта;
- персональные данные, содержащиеся на электронных носителях.
4.5. Лицом, ответственным за организацию обработки персональных данных в Фонда является директор Фонда.
4.6. Оператор издает локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.
4.7. Оператор принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие 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 в соответствии со статьей 19 Федерального закона №152-ФЗ «О персональных данных», в том числе:
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4.8. Оператор осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону №152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

4.9. Оператор осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Положения и (или) законодательства Российской Федерации, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Положением и (или) законодательством Российской Федерации;

4.10. Оператор ознакамливает своих работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

4.11. Ответственные лица, обрабатывающие и хранящие персональные данные на бумажных носителях и машинных носителях информации, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному Постановлением правительства РФ 15.09.2008г. № 687.

4.12. Ответственные лица, обрабатывающие и хранящие персональные данные в информационных системах персональных данных и машинных носителях информации, обеспечивают защиту в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными, нормативно-методическими, методическими документами.

V. Хранение персональных данных

5.1. Сведения о Клиентах/Контрагентах/Работниках хранятся на бумажных носителях в помещении Фонда. Для хранения носителей используются специально оборудованные металлические шкафы и сейфы, которые запираются и сдаются под охрану.

5.2. Обязанности по хранению документов, где содержатся персональные данные Клиентов/Контрагентов/Работников, возлагаются на конкретного работника Фонда или иного лица (закрепляются в его должностной инструкции), на которого возложены данные обязанности.

5.3. Ключи от шкафов и сейфов, в которых хранятся носители, находится у ответственного работника Фонда или иного лица, на которого возложены данные обязанности.

При отсутствии данного работника используются дубликаты ключей, находящиеся у непосредственного руководителя ответственного работника.

5.4. Персональные данные Клиентов/Контрагентов/Работников хранится в электронном виде, доступ к которым ограничен и регламентируется Фондом.

Хранение персональных данных Клиентов/Контрагентов/Работников осуществляется Фондом также и в электронном виде на следующих носителях:

- персональные компьютеры работников Фонда. Персональные компьютеры работников Фонда являются собственностью Фонда.

На персональных компьютерах работников Фонда установлено лицензионное программное обеспечение и антивирусная защита (приложение №2 к настоящему Положению - Инструкция по организации антивирусной защиты). Доступ в персональные компьютеры работников

Фонда осуществляется каждым работником путем ввода пароля, состоящего из не менее чем 7 цифр. Пароль для входа в персональные компьютеры работников Фонда устанавливается сотрудником организации, осуществляющей их обслуживание и техническое сопровождение (приложение №1 к настоящему Положению - Инструкция по организации парольной защиты).
Обслуживание и техническое сопровождение персональных компьютеров работников Фонда осуществляется сторонними организациями на основании договора.
- сетевое хранилище (сервер «Тринити С914379»). Сервер является собственностью Фонда.
Сервер имеет лицензионное программное обеспечение, антивирусную защиту и межсетевой защитный экран (приложение №2 к настоящему Положению - Инструкция по организации антивирусной защиты).
На сервере установлен лицензионный программный продукт для обработки и хранения персональных данных Клиентов/Контрагентов/Работников: 1С:Управление микрофинансовой организацией и кредитным потребительским кооперативом КОРП (разработчик ООО «1С-Софт»). Обслуживание и техническое сопровождение сервера, программного продукта и иного программного обеспечения осуществляется сторонними организациями на основании договора.
Сервер установлен в помещении по адресу: Челябинская область, г. Челябинск, ул. Российская, д. 110, корп. 1, неж.пом. 6, которое имеет ограниченный доступ.
5.5. Доступ к персональным данным Клиентов/Контрагентов/Работников без специального разрешения имеют работники, занимающие в Фонде следующие должности:
- директор Фонда.
- заместители директора Фонда.
- главный бухгалтер Фонда.
- сотрудник кадровой службы (на основании договора аутсорсинга от 01.04.2022 года с Фондом развития предпринимательства Челябинской области – Центр «Мой бизнес»).
5.6. Внутренний доступ (доступ внутри Фонда) к персональным данным Клиентов/ Контрагентов имеют работники Фонда, внесенные в список лиц, допущенных к обработке персональных данных, утвержденный приказом директора Фонда.
5.7. Хранение персональных данных Клиента/Контрагента должно осуществляться в форме, позволяющей определить Клиента/Контрагента, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является Клиент/Контрагент. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Сроки хранения документов, содержащих персональные данные Клиента/Контрагента/Работника, определяются в соответствие со сроком действия договора с Клиентом/Контрагентом/Работника, сроком исковой давности, а также иными требованиями законодательства Российской Федерации.
5.8. Период хранения и обработки персональных данных определяется в соответствии с Федеральным законом № 152-ФЗ.
5.9. При хранении персональных данных Фонд обеспечивает:
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных или на бумажные документы, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.
5.10. Хранимые персональные данные подлежат защите от несанкционированного доступа и копирования. Безопасность персональных данных при их хранении обеспечивается с

помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.
5.11. Хранение персональных данных Клиентов/Контрагентов Фонда осуществляется Фондом по следующим адресам:
- Челябинская область, город Челябинск, Российская улица, дом 110, стр1, неж. пом. 6.
- Челябинская область, город Челябинск, Российская улица, дом 110, стр1, неж.пом. №001.
Хранение персональных данных Работников Фонда осуществляется Фондом развития предпринимательства Челябинской области – Центр «Мой бизнес» по следующему адресу: Челябинская область, город Челябинск, Российская улица, дом 110, стр1, неж.пом. №308. Данные помещения используются на основании договора аренды.

VI. Передача персональных данных

6.1. При передаче персональных данных Клиента/Контрагента/Работника Оператор соблюдает следующие требования:
6.1.1. Не сообщает персональные данные Клиента/Контрагента/Работника третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях», при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов, а также в случаях, предусмотренных иными федеральными законами. Оператор в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено на получение персональных данных Клиента/Контрагента/Работника, либо отсутствует письменное согласие Клиента/Контрагента/Работника на предоставление его персональных сведений, либо, по мнению Оператора, присутствует угроза жизни или здоровью Клиента или Контрагента, Фонд обязан отказать в предоставлении персональных данных такому лицу. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.
6.1.2. Не сообщает персональные данные Клиента/Контрагента/Работника в коммерческих целях без его письменного согласия.
6.1.3. Предупреждает лиц, получающих персональные данные Клиента/Контрагента/Работника, 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 Клиента/Контрагента, обязаны соблюдать требования конфиденциальности.
6.1.4. Осуществляет передачу персональных данных Клиента/Контрагента/Работника в пределах своей организации или иным лицам на основании заключенного договора в соответствии с настоящим Положением.
6.1.5. Разрешает доступ к персональным данным Клиентов/Контрагентов/Работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные Клиента/Контрагента, которые необходимы для выполнения их конкретных функций. Лица, получающие персональные данные Клиента/Контрагента, обязаны соблюдать требования конфиденциальности.
6.1.6. Не запрашивает информацию о состоянии здоровья Клиента/Контрагента/Работников, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Клиентом/Контрагентов/Работников своих представительских функций;
6.1.7. Передает персональные данные Клиента/Контрагента/Работника его представителям в порядке, установленном законодательством Российской Федерации, и ограничивает эту информацию только теми персональными данными Клиента/Контрагента, которые необходимы для выполнения указанными представителями их функций.

6.2. В случае если Оператору оказываются услуги юридическими или физическими лицами на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным Клиентов/Контрагентов/Работников, то соответствующие данные предоставляются Оператором только после подписания с ними соглашения о конфиденциальности (неразглашении конфиденциальной информации).

VII. Обязанности Оператора, Клиента/Контрагента/Работника

7.1. В целях обеспечения достоверности персональных данных Клиент/Контрагент/Работник обязан:
7.1.1. При заключении договора предоставить Оператору полные и достоверные данные о себе.
7.1.2. В случае изменения сведений, составляющих персональные данные Клиента/ Контрагента, незамедлительно, но не позднее 5 (Пяти) рабочих дней, предоставить данную информацию Оператору.
7.2. Оператор обязан:
7.2.1. Обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации и настоящим Положением;
7.2.2. Предоставить возможность Клиенту/Контрагенту или их представителям ознакомиться с настоящим Положением и его правами в области защиты персональных данных;
7.2.3. Обеспечить хранение первичной учетной документации. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.
7.2.4. В случае реорганизации или ликвидации Оператора учет и сохранность документов, порядок передачи их на государственное хранение осуществлять в соответствии с правилами, предусмотренными учредительными документами и действующим законодательством Российской Федерации.
7.2.5. Вести журнал учета обращений субъектов персональных данных (приложение №5 к настоящему Положению).
7.2.6. Осуществлять передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации.
7.2.7. По требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.
7.3. Анализ угроз.
Обеспечение безопасности персональных данных, а также разработка и внедрение средств защиты персональных данных основывается на анализе угроз безопасности персональных данных. Фонд, при возникновении необходимости разрабатывает и поддерживает частную модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - Частная модель угроз). Частная модель угроз отражает актуальное состояние защищенности информационных системах персональных данных и актуальные угрозы безопасности персональных данных. Разработка Частной модели угроз осуществляется на основании анализа существующих угроз безопасности и возможности их реализации в обследуемой информационных системах персональных данных.
7.4. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Фонд обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов

персональных данных Фонд обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

7.5. В случае подтверждения факта неточности персональных данных Фонд на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7.6. В случае выявления неправомерной обработки персональных данных, осуществляемой Фондом или лицом, действующим по поручению Фонда, Фонд в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, Фонд в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Фонд обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

7.7. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Фонд обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение 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 предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

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

7.8. В случае достижения цели обработки персональных данных Фонд обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если Фонд не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством РФ.

7.9. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Фонд обязан прекратить их обработку или обеспечить прекращение

такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если Фонд не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством РФ.

7.10. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона №152-ФЗ. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

7.11. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5.1 статьи 21 Федерального закона №152-ФЗ, Фонд осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Фонда) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7.12. Подтверждение уничтожения персональных данных в случаях, предусмотренных статьей 21 Федерального закона №152-ФЗ, осуществляется Фондом в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.

VIII. Порядок уничтожения персональных данных

8.1. Основания для уничтожения персональных данных Клиента/Контрагента/Работника:

- получение Фондом требования Клиента/Контрагента/Работника об прекращении обработки и уничтожении персональных данных;
- получение Фондом отзыва субъектом персональных данных согласия на обработку его персональных данных;
- достижение цели обработки персональных данных;
- получение Фондом решения суда или органа по защите прав субъектов персональных данных о прекращении и уничтожении обработки персональных данных;
- выявление Фондом неправомерной обработки персональных данных.

8.2. Ответственным за уничтожение персональных данных является уполномоченное лицо или Комиссия, назначаемое Приказом директора Фонда.

8.3. Директор Фонда является председателем комиссии Фонда по уничтожению персональных данных.

8.4. При наступлении любого из событий, повлекших, согласно законодательства Российской Федерации, необходимость уничтожения персональных данных, уполномоченное лицо/Комиссия обязано приказом (приложение №3 к настоящему Положению):

- уведомить членов комиссии о работах 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 персональных данных, подлежащие уничтожению (и/или материальные носители персональных данных);
- определить технологию (приём, способ) уничтожения персональных данных (и/или материальных носителей персональных данных);
- определить технические (материальные, программные и иные) средства, посредством которых будет произведено уничтожение персональных данных;
- руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных);
- оформить соответствующий Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) и представить Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) на утверждение директору (приложение №4 к настоящему Положению);
- в случае необходимости уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

IX. Права Клиентов/Контрагентов/Работников в целях защиты персональных данных

9.1. В целях обеспечения защиты персональных данных, хранящихся у Оператора, Клиенты/Контрагенты/Работники имеют право на:
9.1.1. Полную информацию о составе персональных данных и их обработке, в частности Клиент/Контрагент/Работник имеет право знать, кто и в каких целях использует или использовал информацию о его персональных данных.
9.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Клиента/Контрагента/Работника, за исключением случаев, предусмотренных законодательством Российской Федерации.
9.1.3. Определение своих представителей для защиты своих персональных данных.
9.1.4. 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/Контрагента/Работника он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия.
9.1.5. Требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные Клиента/Контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях.
9.1.6. Обжалование в суд любых неправомерных действий или бездействия Оператора при обработке и защите его персональных данных.
9.1.7. Клиент имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;

- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом №152-ФЗ или другими федеральными законами.

X. Ответственность за нарушение норм, регулирующих получение, обработку, передачу и защиту персональных данных

10.1. Лица, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

10.2. Фонд, допустивший нарушение порядка обращения с персональными данными, возмещает клиенту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные об этом Клиенте/Контрагенте/Работнике.

XI. Заключительные положения

11.1 Настоящее Положение вступает в силу с момента его утверждения приказом Директора Фонда.

11.2 Настоящее Положение доводится до сведения всех работников Фонда персонально под роспись.

11.3. Изменения в настоящее Положение вносятся по мере необходимости, либо в соответствии с требованиями законодательства Российской Федерации.

Приложение №1

ИНСТРУКЦИЯ
по организации парольной защиты

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в информационных системах (далее – ИС) Фонда финансирования промышленности и предпринимательства - центр «Мой бизнес» (микрокредитная компания) (далее – Фонд), а также контроль над действиями пользователей при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.2. **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

2.3. **Пароль** – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.4. **Пользователь** – работник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

2.5. **Компрометация пароля** – раскрытие, обнаружение или утеря пароля.

III. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

3.1. Правила формирования паролей:

3.1.1. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

3.1.1.1. длина пароля должна быть не менее 6 символов;

3.1.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

3.1.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

3.1.1.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях;

3.1.2. Пользователям допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

3.1.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения

возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах.

3.2. Порядок смены личных паролей:

3.2.1. Смена паролей должна проводиться регулярно, не реже одного раза в 4 месяца (120 дней).

3.2.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

3.2.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за обеспечение безопасности персональных данных в информационных системах, администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

3.2.4. Ответственный за обеспечение безопасности персональных данных в информационных системах ведёт Журнал учёта работ в информационных системах, в котором он отмечает факт смены паролей пользователей.

3.2.4.1. Временный пароль, заданный ответственным за обеспечение безопасности персональных данных в информационных системах при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

3.3. В ИС должна обеспечиваться защита аутентификационной информации в процессе ее ввода от возможного использования лицами, не имеющими на это полномочий. Защита обеспечивается отображением вводимых символов условными знаками «*», «•» или иными знаками, вместо действительной информации.

3.4. Действия в случае утери и компрометации пароля:

3.4.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

IV. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

4.1. Правила формирования паролей:

4.1.1. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

4.1.1.1. длина пароля должна быть не менее 6 символов;

4.1.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

4.1.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

4.1.1.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

4.1.2. Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

4.1.3. Для обеспечения возможности использования имён и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей ответственному за обеспечение безопасности персональных данных в информационных системах в запечатанном конверте или опечатанном пенале.

4.2. Порядок ввода пароля:

4.2.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4.3. Порядок смены личных паролей:

4.3.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца, самостоятельно каждым пользователем.

4.3.2. Временный пароль, заданный ответственным за обеспечение безопасности персональных данных в информационных системах при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

4.4. Хранение пароля:

4.4.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах, и носителях информации.

4.4.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

4.4.3. Запрещается регистрировать других пользователей в ИС со своим личным паролем, запрещается входить в ИС под учётной записью и паролем другого пользователя.

4.5. Действия в случае утери и компрометации пароля:

4.5.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователь должен немедленно обратиться к ответственному за обеспечение безопасности персональных данных в информационных системах с целью смены личного пароля.

V. ОТВЕТСТВЕННОСТЬ

5.1. Работники несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обеспечению безопасности информации и за все действия, совершенные от имени их учётных записей в ИС, если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. Работники при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

5.3. Разглашение информации (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) Фонда, влечет наложение на работника, имеющего доступ к защищаемой информации, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Фонда, имеющий доступ к информации и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Фонду (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

5.3.1. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях РФ.

5.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

Приложение №2

ИНСТРУКЦИЯ

по организации антивирусной защиты

ОБЩИЕ ПОЛОЖЕНИЯ

Данная инструкция определяет требования к организации защиты информационной системы Фонда финансирования промышленности и предпринимательства Челябинской области – Центр «Мой бизнес» (микрокредитная компания) (далее – Фонд) вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность пользователей ИС, ответственного за обеспечение безопасности персональных данных в информационных системах и других должностных лиц, за выполнение указанных требований.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Антивирусная база – это база, которая содержит уникальные данные о каждом конкретном вирусе.

Антивирусная защита – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.

Средство антивирусной защиты – программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

Информация – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации

Программное обеспечение – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993)

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

К использованию в Фонде допускаются только сертифицированные и лицензионные средства антивирусной защиты, закупленные у разработчиков или поставщиков данных средств.

Установка средств антивирусного контроля на автоматизированных рабочих местах и серверах ИС Фонда осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты информации.

Антивирусный контроль должен быть настроен в режиме постоянной антивирусной защиты.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ,

передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после её приёма. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

Процедура обновления баз средства антивирусной защиты должна проводиться в автоматическом режиме не реже 1 (одного) раза в день на всех АРМ ИС, работающих в сети, не реже 1 (одного) раза в неделю для всех АРМ ИС, работающих автономно.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено ответственным за обеспечение безопасности персональных данных в информационных системах на предмет отсутствия вредоносного программного обеспечения (далее – ПО).

Подключаемые к компьютеру внешние устройства и носители информации должны проверяться антивирусным ПО непосредственно после подключения.

Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИС Фонда, осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах, пользователями ИС и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИС Фонда.

ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) пользователь ИС обязан самостоятельно или вместе с ответственным за обеспечение безопасности персональных данных в информационных системах провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах ответственного за обеспечение безопасности персональных данных в информационных системах для определения им факта наличия или отсутствия вредоносного программного обеспечения.

В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения пользователь ИС обязан:

- приостановить обработку данных;
- немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения ответственного за обеспечение безопасности информации, владельца заражённых файлов, а также всех работников, использующих эти файлы в работе;
- совместно с владельцем файлов, заражённых вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;
- произвести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за обеспечение безопасности персональных данных в информационных системах).

ОТВЕТСТВЕННОСТЬ

Работники Фонда несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени их учётных записей в ИС, если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

Работники Фонда при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата

документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) Фонда, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Фонда, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Фонду (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях РФ.

В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

Приложение №3

Приказ N ____

г. _____ "___" _____ ___ г.

Об уничтожении персональных данных

В целях исполнения требований Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных», а также руководствуясь Приказом директора Фонда №5 от 22.05.2023 года

ПРИКАЗЫВАЮ:

1. Комиссии в составе:

1) _____ (председатель комиссии);
(Ф.И.О., должность)

2) _____ (член комиссии);
(Ф.И.О., должность)

3) _____ (член комиссии).
(Ф.И.О., должность)

4) _____ (член комиссии).
(Ф.И.О., должность)

2. В срок до "___"_____ ___ г. провести уничтожение документов и информации, составляющих персональные данные Клиентов/Контрагентов/Работников Фонда.

2.2. В срок до "___"_____ ___ г. представить на утверждение Комиссии Акт об уничтожении персональных данных Клиентов/Контрагентов/Работников Фонда.

2.3. В срок до "___"_____ ___ г. уничтожить с применением уничтожителя бумаг, а также путем удаления информации с электронного носителя документы и информацию согласно Акту об уничтожении персональных данных.

3. Контроль за исполнением настоящего приказа оставляю за собой (вариант: возложить на _____).
(указать должность и Ф.И.О.)

Руководитель _____ _____/_____
(подпись) (Ф.И.О.)

С приказом ознакомлены: "___"_____ ___ г. _____/_____
(подпись) (Ф.И.О.)

Приложение №4

Акт
об уничтожении персональных данных

г. Челябинск «___» _____ _____г.

Комиссия, созданная приказом директора Фонда финансирования промышленности и предпринимательства Челябинской области – Центр «Мой бизнес» (микрокредитная компания) от 22.05.2023 года № 5, в составе председателя комиссии - _____, членов комиссии - _____, _____, _____в соответствии со ст. 21 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» составила настоящий Акт об уничтожении персональных данных субъектов персональных данных, обрабатываемых, Фондом финансирования промышленности и предпринимательства Челябинской области – Центр «Мой бизнес» (микрокредитная компания), находящимся по адресу: 454904, Россия, Челябинская область, г. Челябинск, ул. Российская, д. 110, корп.1, неж.пом. 6.

Ф.И.О. субъектов, чьи персональные данные были уничтожены	**Перечень категорий уничтоженных персональных данных**	**Наименование носителя, из которого были уничтожены персональные данные**	**Способ уничтожения персональных данных**	**Причина уничтожения персональных данных**	**Дата уничтожения персональных данных**

Настоящий Акт подлежит хранению до «____» _____ _____ г.

Председатель комиссии: _____
Члены комиссии: _____
_____

Приложение №5

Журнал
учета обращений субъектов персональных данных

№ п/п	Наименование/ФИО/ИНН субъекта персональных данных	Дата обращения субъекта персональных данных	Тема обращения субъекта персональных данных	Лицо, принявшее обращение субъекта персональных данных

С положением ознакомлены

1. Карпова О.В.
2. Соболь В.Г.
3. Курочкин А.А.
4. Матвеева М.В.
5. Кронина Т.П.
6. Ситникова С.В.
7. Пугачев
8. Кремлева В.В.
9. Никитин А.А.
10. Усачева О.С.
11. Захаров А.О.
12. Кудрявцева А.С.