

УТВЕРЖДЕНО
Приказом директора
МКК «Фонд развития Приморского края»
от 01.09.2022г. № 67

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

***в Микрокредитной компании
«Фонд развития предпринимательства и
промышленности Приморского края»***

г.Владивосток
2022 год

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о защите персональных данных в МКК «Фонд развития предпринимательства и промышленности Приморского края» является локальным нормативным актом МКК «Фонд развития предпринимательства и промышленности Приморского края» (далее - Фонд), устанавливающим порядок получения, обработки, хранения, передачи и защиты персональных данных в Фонде.

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

1.3. В настоящем Положении используются следующие термины и определения:

Оператор – МКК «Фонд развития предпринимательства и промышленности Приморского края», вступившее в договорные отношения с работником, клиентом или контрагентом, организующее и осуществляющее в связи с этим обработку персональных данных.

Клиент – физическое лицо, официальный представитель – физическое лицо юридического лица и индивидуального предпринимателя, вступившее в договорные отношения по оказанию услуг с Фондом.

Контрагент – физическое лицо, физическое лицо – представитель юридического лица или индивидуального предпринимателя, вступившие с Фондом в договорные отношения.

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

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

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

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

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

Защита персональных данных – комплекс мер, принимаемых Фондом 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 Фонд принимает меры по защите от несанкционированного доступа третьих лиц, не имеющих право доступа к такой информации.

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

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

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

«Куки» (cookies) - общеотраслевая технология, которую вправе использовать Фонд в работе своего сайта, небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере, который использует Пользователь сайта, позволяющий Фонду сохранять персональные настройки и предпочтения Пользователя сайта, а также собирать неличную информацию о нём.

1.4. Настоящее Положение вступает в силу с момента его утверждения приказом руководителя Фонда.

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

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

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

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

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

2.1.3. Получение Фондом персональных данных может осуществляться как путем представления их самим субъектом персональных данных, так и путем получения их из иных источников, в том числе от других операторов персональных данных.

Фонд должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и юридическое последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку, если в соответствии с федеральным законом предоставление персональных данных и (или) получение Фондом согласия на обработку персональных данных являются обязательными.

Если персональные данные возможно получить только у третьей стороны, то третья сторона в данном случае выступает оператором персональных данных. Субъект персональных данных должен быть уведомлен оператором об этом заранее, и от субъекта персональных данных оператором должно быть получено письменное согласие. Ответственность при этом возлагается на третью сторону, выступающую в данном случае оператором персональных данных.

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

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

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

2.3. Персональные данные субъекта персональных данных не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном

происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено действующим законодательством Российской Федерации.

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

2.5. При идентификации клиента или контрагента Фонд может затребовать предъявления документов, удостоверяющих личность и подтверждающих полномочия представителя. При заключении договора, как и в ходе выполнения договора, Фонд может затребовать предоставление клиентом или контрагентом иных документов, содержащих информацию о нем.

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

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

2.7. Направление персональных данных посредством электронной почты допускается только с письменного согласия или поручения субъекта персональных данных.

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

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

3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ОСУЩЕСТВЛЕНИЯ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ, ПРЕДУСМОТРЕННОЙ УСТАВОМ ФОНДА

3.1. Фонд осуществляет обработку персональных данных в целях осуществления предпринимательской деятельности, предусмотренной Уставом Фонда, в том числе предоставление займов в порядке, установленном Федеральным законом «О потребительском кредите (займе)».

3.2. Для цели осуществления предпринимательской деятельности Фонд обрабатывает персональные данные у следующих категорий субъектов персональных данных:

- клиентов – физических лиц;
- представителей клиентов - юридических лиц;
- пользователей сайта.

3.2.1 Фонд запрашивает у клиентов – физических лиц следующие персональные данные:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- данные документа, удостоверяющего личность;
- 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.

3.2.2 Фонд запрашивает у представителей клиентов - юридических лиц следующие персональные данные:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- данные документа, удостоверяющего личность;
- телефон;
- адрес электронной почты.
- должность;

3.2.3 Фонд запрашивает у пользователей сайта следующие персональные данные:

- фамилия, имя, отчество;
- адрес электронной почты,
- телефон;

3.3. Фонд осуществляет обработку персональных данных следующими способами:

- Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
- Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
- Смешанная обработка персональных данных - обработка персональных данных, как с использованием средств автоматизации, так и без использования таких средств.

Фонд может использовать общеотраслевую технологию «куки» (cookies). В любое время пользователь сайта может изменить параметры в настройках своего браузера таким образом, чтобы браузер перестал сохранять все файлы cookie, а также оповещал их об отправке. В этом случае некоторые сервисы и функции сайта могут перестать работать или работать некорректно.

3.4. Обработка персональных данных начинается с момента поступления персональных данных в Фонд и прекращается:

- в случае выявления неправомерных действий с персональными данными;
- в случае достижения цели обработки персональных данных;

- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;
- в случае получения Фондом требования субъекта персональных данных о прекращении обработки персональных данных;
- в случае прекращения деятельности Фонда.

3.5. Хранение персональных данных осуществляется в Фонде:

- в течение пяти лет с момента фактического прекращения отношений с клиентом;
- не более 30 дней с даты достижения цели их обработки в случае если договор оказания услуг не заключен;
- в сейфе на бумажных носителях и на электронных носителях с ограниченным доступом;
- в электронном виде в информационной системе персональных данных сайта Фонда, а также в архивных копиях баз данных сайта Фонда.

3.6. Уничтожение персональных данных осуществляется комиссией, назначаемой приказом руководителя Фонда. Лицо, ответственное за организацию обработки персональных данных назначается председателем комиссии по уничтожению персональных данных.

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

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

3.7. Фонд не осуществляет трансграничную передачу персональных данных.

3.8. Биометрические персональные данные обрабатываются Фондом в следующих целях:

- противодействие коррупции;
- обеспечение личной безопасности работников и посетителей МКК «Фонд развития Приморского края»;
- с целью контроля за текущей трудовой деятельностью работников МКК «Фонд развития Приморского края»;

- с целью контроля количества и качества выполняемой работы работниками МКК «Фонд развития Приморского края»;
- с целью обеспечения сохранности имущества МКК «Фонд развития Приморского края»;
- с целью разрешения спорных ситуаций с заемщиками, поручителями, залогодателями, посетителями МКК «Фонд развития Приморского края».

К обрабатываемым Фондом биометрическим персональным данным относятся:

- голос, в том числе запись телефонных разговоров;
- видеозапись и видеоизображение лица, фигуры, голоса;
- фотография лица, фигуры.

Обработка Фондом биометрических персональных данных может производиться как с использованием средств автоматизации, так и без использования средств автоматизации.

3.9. Фондом не обрабатываются специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

4. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ЗАКЛЮЧЕНИЯ И ИСПОЛНЕНИЯ ГРАЖДАНСКО-ПРАВОВЫХ ДОГОВОРОВ

4.1 Фонд осуществляет обработку персональных данных в целях заключения и исполнения гражданско-правовых договоров с физическими, юридическими лицами, индивидуальными предпринимателями и иными лицами, в связи с осуществлением хозяйственной деятельности Фонда.

4.2 Для цели заключения и исполнения гражданско-правовых договоров Фонд обрабатывает персональные данные у следующих категорий субъектов персональных данных:

- контрагентов – физических лиц;
- представителей контрагентов - юридических лиц.

4.2.1. Фонд запрашивает у контрагентов - физических лиц следующие персональные данные:

- 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.

4.2.2. Фонд запрашивает у представителей контрагентов - юридических лиц следующие персональные данные:

- фамилия, имя, отчество;
- паспортные данные;
- телефон;
- адрес электронной почты.

- должность
- 4.3 Фонд осуществляет обработку персональных данных следующими способами:
- Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
 - Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
 - Смешанная обработка персональных данных - обработка персональных данных как с использованием средств автоматизации, так и без использования таких средств.
- 4.4 Обработка персональных данных начинается с момента поступления персональных данных в Фонд и прекращается:
- в случае выявления неправомерных действий с персональными данными;
 - в случае достижения цели обработки персональных данных;
 - в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;
 - в случае получения Фондом заявления субъекта персональных данных о прекращении обработки персональных данных;
 - в случае прекращения деятельности Фонда.
- 4.5 Хранение персональных данных осуществляется в Фонде:
- в течение пяти лет с момента фактического прекращения отношений с контрагентом;
 - не более 30 дней с даты достижения цели их обработки в случае если договор с контрагентом не был заключен;
 - в сейфе на бумажных носителях и на электронных носителях с ограниченным доступом;
 - в электронном виде в информационной системе персональных данных сайта Фонда, а также в архивных копиях баз данных сайта Фонда.
- 4.6 Уничтожение персональных данных контрагентов Фонда осуществляется комиссией, назначаемой приказом руководителя Фонда. Лицо, ответственное за организацию обработки персональных данных назначается председателем комиссии по уничтожению персональных данных.
- 4.6.1 При наступлении любого из событий, повлекших, необходимость уничтожения персональных данных контрагентов Фонда, в соответствии с законодательством Российской Федерации, лицо, ответственное за организацию обработки персональных данных обязано:
- уведомить членов комиссии о дате начала работ по уничтожению персональных данных;
 - определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);

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

4.7 Фонд не осуществляет трансграничную передачу персональных данных.

4.8. Биометрические персональные данные обрабатываются Фондом в следующих целях:

- противодействие коррупции;
- обеспечение личной безопасности работников и посетителей МКК «Фонд развития Приморского края»;
- с целью контроля за текущей трудовой деятельностью работников МКК «Фонд развития Приморского края»;
- с целью контроля количества и качества выполняемой работы работниками МКК «Фонд развития Приморского края»;
- с целью обеспечения сохранности имущества МКК «Фонд развития Приморского края»;
- с целью разрешения спорных ситуаций с заемщиками, поручителями, залогодателями, посетителями МКК «Фонд развития Приморского края».

К обрабатываемым Фондом биометрическим персональным данным относятся:

- голос, в том числе запись телефонных разговоров;
- видеозапись и видеоизображение лица, фигуры, голоса;
- фотография лица, фигуры.

Обработка Фондом биометрических персональных данных может производиться как с использованием средств автоматизации, так и без использования средств автоматизации.

4.9. Фондом не обрабатываются специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

5. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ОФОРМЛЕНИЯ ТРУДОВЫХ ОТНОШЕНИЙ

5.1. Фонд осуществляет обработку персональных данных в целях оформления трудовых отношений; исполнение обязательств по трудовым договорам; ведение кадрового делопроизводства; содействие работникам в обучении и продвижении по службе; исполнение требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе

доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение.

5.2. Для цели оформления трудовых отношений Фонд обрабатывает персональные данные у следующих категорий субъектов персональных данных:

- работников (в том числе уволенных);
- родственников работника;
- кандидатов на замещение вакантных должностей.

5.2.1 Фонд запрашивает у работников (в том числе уволенных) следующие персональные данные:

- 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 переподготовке 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;

5.2.2 Фонд запрашивает персональные данные родственников работника исключительно в целях заполнения личной карточки работника по унифицированной форме в следующем объеме:

- фамилия, имя, отчество;
- год, месяц, дата рождения;
- степень родства.

5.2.3 Фонд запрашивает кандидатов на замещение вакантных должностей следующие персональные данные:

- фамилия, имя, отчество;
- год, месяц, дата;

- адрес регистрации по месту жительства (почтовый адрес);
 - адрес фактического проживания (почтовый адрес фактического проживания);
 - семейное положение;
 - социальное положение;
 - адрес электронной почты, телефон;
 - сведения о стаже работы и о местах работы (город, название организации, должность, сроки работы);
 - сведения о наградах (поощрениях), почетных званиях;
 - сведения об образовании, повышении квалификации, профессиональной переподготовке и местах обучения (город, образовательное учреждение, сроки обучения, специальность, квалификация, профессия).
- 5.3. Фонд осуществляет обработку персональных данных следующими способами:
- Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
 - Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
 - Смешанная обработка персональных данных - обработка персональных данных как с использованием средств автоматизации, так и без использования таких средств.
- При заключении трудовых договоров Фонд принимает, снимает и хранит копии личных документов работника.
- 5.4. Обработка персональных данных начинается с момента поступления персональных данных в Фонд и прекращается:
- в случае выявления неправомерных действий с персональными данными;
 - в случае достижения цели обработки персональных данных;
 - в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;
 - в случае получения Фондом требования субъекта персональных данных о прекращении обработки персональных данных;
 - в случае прекращения деятельности Фонда.
- 5.5. Хранение персональных данных осуществляется в Фонде:
- в течение 50 лет после расторжения с работником трудового договора (делопроизводство по которым закончено до 01 января 2003 года) или в течение 75 лет после расторжения с работником трудового договора (делопроизводство по которым закончено после 01 января 2003 года);
 - не более 30 дней с даты достижения цели обработки персональных данных кандидатов на замещение вакантных должностей.
- 5.6. Уничтожение персональных данных работников Фонда осуществляется комиссией, назначаемой приказом руководителя Фонда. Лицо, ответственное за организацию обработки персональных данных назначается председателем комиссии по уничтожению персональных данных.

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

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

5.7. Фонд не осуществляет трансграничную передачу персональных данных.

5.8. Биометрические персональные данные обрабатываются Фондом в следующих целях:

- противодействие коррупции;
- обеспечение личной безопасности работников МКК «Фонд развития Приморского края»;
- с целью контроля за текущей трудовой деятельностью работников МКК «Фонд развития Приморского края»;
- с целью контроля количества и качества выполняемой работы работниками МКК «Фонд развития Приморского края»;
- с целью обеспечения сохранности имущества МКК «Фонд развития Приморского края»;
- с целью разрешения спорных ситуаций с заемщиками, поручителями, залогодателями, посетителями МКК «Фонд развития Приморского края».

К обрабатываемым Фондом биометрическим персональным данным относятся:

- голос, в том числе запись телефонных разговоров;
- видеозапись и видеоизображение лица, фигуры, голоса;
- фотография лица, фигуры.

Обработка Фондом биометрических персональных данных может производиться как с использованием средств автоматизации, так и без использования средств автоматизации.

5.9. Фондом не обрабатываются специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

6. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦОМ ПО ПОРУЧЕНИЮ ФОНДА

6.1. Фонд 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 органом или муниципальным органом соответствующего акта.

6.2. Лицо, осуществляющее обработку персональных данных по поручению Фонда, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

6.3. В поручении Фонда определяется перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели их обработки, и устанавливаются обязанности:

- соблюдать конфиденциальность персональных данных;
- принимать меры, направленные на обеспечение выполнения обязанностей, предусмотренных локально-нормативными актами Фонда;
- при сборе персональных данных в том числе посредством информационно-телекоммуникационной сети "Интернет", обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации;
- предоставлять Фонду документы и информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- уведомлять Фонд в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных.

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

6.5. 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.

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

7.1 Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

7.2 Фонд 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.

7.3 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 Фондом неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

7.4 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.

7.5 Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

7.6 Фонд 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.

7.7 Фонд в любое время по требованию субъекта персональных данных прекращает передачу (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения.

7.8 Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления Фонду требования, указанного п. 7.7 настоящего Положения.

8. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

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

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

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

При разработке системы защиты учитывалась обязанность Фонда 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».

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

- определение актуальных угроз безопасности персональных данных.

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

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 Фондом 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 также 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.

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

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

- проведение плановых и внезапных проверок на предмет соблюдения режима конфиденциальности в Фонде работниками Фонда;
 - принятие решений о необходимости отстранения от работы с конфиденциальной информацией работников Фонда, нарушающих режим конфиденциальности в Фонде;
 - рассмотрение иных вопросов обеспечения и соблюдения режима конфиденциальности.
- 8.10.4. Защите подлежат все персональные данные, определенные в разделе 2 настоящего Положения, в том числе:
- персональные данные субъекта, содержащиеся в копиях документов;
 - персональные данные субъекта, содержащиеся в документах, созданных Фондом;
 - 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.
- 8.11. Правовые меры защиты персональных данных.
- 8.11.1. К правовым мерам защиты персональных данных относится:
- 1) Разработка и утверждение локальных нормативных актов Фонда: Политики в отношении обработки и защиты персональных данных, Положения о защите персональных данных, иных документов, которыми регламентируется порядок организации системы защиты в Фонде (далее – Регламентирующие документы).
 - 2) Обязанность Фонда осуществлять мониторинг действующего законодательства.
- 8.11.2. Регламентирующие документы разрабатываются самим Фондом или с привлечением третьих лиц и утверждаются руководителем Фонда.
- 8.11.3. 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 Фонда 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.
- 8.12. Организационные меры защиты персональных данных.
- К организационным мерам защиты персональных данных относятся:
- 8.12.1. Определение правил доступа к информации, содержащей персональные данные.
- 8.12.1.1. К работе с информацией, содержащей персональные данные, могут быть допущены работники Фонда при одновременном выполнении следующих условий:
- должность работника указана в Реестре прав доступа;
 - работник ознакомлен под подпись с Реестром прав доступа и настоящим Положением;

- работником Фонда подписано Обязательство о неразглашении конфиденциальной информации.
- 8.12.1.2. Приказом руководителя Фонда 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 Фонд 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 Фонда содержит следующую информацию:
 - должности работников Фонда, 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 Фонда;
 - 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 Фонде, включая информацию, полученную от третьих лиц, обладает руководитель Фонда.
- 8.12.1.3. До начала работы с персональными данными работник должен подписать Обязательство о неразглашении конфиденциальной информации.
Обязательство о неразглашении конфиденциальной информации, подписанное работником Фонда, приобщается к личному делу работника.
- 8.12.1.4. Определение обязанностей для работников Фонда при работе с персональными данными. Работник Фонда, допущенный к работе с информацией, содержащей персональные данные, обязан:
- знать и выполнять требования настоящего Положения, иных внутренних документов по защите информации;
 - соблюдать ограничения, установленные Реестром прав доступа: работать только с теми сведениями и использовать только те ресурсы информационной системы, которые определены Реестром прав доступа;
 - соблюдать порядок работы и меры по защите ставших ему известными сведений конфиденциального характера;
 - соблюдать правила работы с носителями информации, содержащей персональные данные, порядок их учета и хранения, обеспечивать в процессе работы сохранность сведений, содержащихся в них от посторонних лиц;
 - незамедлительно в письменной форме, информировать руководителя Фонда 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.

8.12.1.5. Определение ограничений для работников Фонда 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 Фонда, 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 Фонда);
- выносить из служебных помещений документы и машинные носители с информацией, содержащей персональные данные.

8.12.2. Назначение лица, ответственного за информационную безопасность.

Приказом руководителя Фонда 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 Фонде определенных мер защиты информации, содержащей персональные данные;
- контроль за соблюдением работниками Фонда требований настоящего Положения;
- проведение обучений для работников Фонда в целях ознакомления с требованиями настоящего Положения;
- сбор и анализ статистических данных об Актуальных угрозах безопасности, характерных для Фонда;
- внесение предложений руководителю Фонда о необходимости проведения оценки достаточности принятых мер по защите информации, содержащей персональные данные, предложений по внесению изменений во внутренние документы Фонда, регламентирующие деятельность Фонда по защите информации, содержащей

персональные данные, предложений по иным вопросам, связанным с деятельностью Фонда по защите информации, содержащей персональные данные.

8.12.3. Определение порядка передачи персональных данных.

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

- по требованию органов государственной власти и местного самоуправления, государственных, надзорных и контролирующих органов, а также участников Фонда в соответствии с действующим законодательством;
- работникам Фонда в соответствии с учредительным документом Фонда;
- другим физическим и юридическим лицам на основании гражданско-правовых договоров, заключенных между ними и Фондом, при условии наличия в этих договорах обязательств по соблюдению режима конфиденциальности в отношении информации, ответственности за разглашение этой информации или заключения с ними отдельного договора о конфиденциальности.

2) При передаче персональных данных Фонд 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;

8.12.4. Обеспечение сохранности носителей информации.

8.12.4.1. Режим сохранности материальных носителей информации.

1) Доступ к материальным носителям информации, содержащей персональные данные, имеют только те работники Фонда, 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.

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

8.12.5. Установление режима использования Криптографических ключей.

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

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

8.12.5.3. Криптографические ключи должны использоваться Фондом в соответствии с технической документацией.

8.12.6. Установление режима обеспечения безопасности помещений.

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

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

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

8.12.7.1. Фонд 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.

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

- 8.12.7.3. 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.
- 8.12.7.4. 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.
- 8.12.7.5. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, с момента выявления такого инцидента самим Фондом или уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом, Фонд уведомляет уполномоченный орган по защите прав субъектов персональных данных:
- в течение 24 (двадцати четырех) часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о представителе Фонда, уполномоченном на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;
 - в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).
- 8.13. Технические меры по защите персональных данных:
- 8.13.1. 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 Фонда.
- 8.13.2. Создание учетных записей для работников Фонда. Каждому пользователю информационной системы Фонда, 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 Фонда. Пароль для входа в учетную запись не может передаваться третьим лицам, за исключением случаев, установленных настоящим Положением.
- 8.13.3. Установление режима защиты сетевого взаимодействия. Обмен данными между элементами информационной системы Фонда и другими компьютерами (рабочими станциями, серверами) должен быть организован через защищенные соединения,

- организованные с использованием протоколов IPSec с проверкой подлинности и шифрованием IP-пакетов.
- 8.13.4. Осуществление Резервного копирования информации, содержащей персональные данные.
- 8.13.5. Ограничение доступа к Информационно-коммуникационной сети Интернет.
- 8.13.6. Пользователям информационной системы Фонда (учетным записям пользователей), работающим с информацией, содержащей персональные данные, может быть ограничен доступ к сети Интернет и средствам электронной почты.
- 8.13.7. Применение технических средств, обеспечивающих восстановление модифицированной или уничтоженной вследствие несанкционированного доступа информации, содержащей персональные данные.
- 8.14. Проведение оценки эффективности принятых мер по защите информации, содержащей персональные данные.
- 8.6.1. Оценка эффективности принятых мер по защите информации, содержащей персональные данные, может проводиться Фондом самостоятельно или с привлечением сторонней организации.
- 8.6.2. Оценка эффективности принятых мер по защите информации, содержащей персональные данные, проводится по результатам внутренней проверки, проводимой лицом, ответственным за информационную безопасность.
- 8.6.3. Приказом руководителя утверждаются периодичность проведения проверок (но не реже одного раза в год), сроки проведения плановых проверок, а также их содержание.
- 8.6.4. 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 руководителю Фонда заключение о проведении оценки достаточности принятых мер по защите информации, содержащей персональные данные.
- 8.6.5. В случае подтверждения недостаточности принятых мер по защите информации, содержащей персональные данные, руководитель Фонда принимает решение о необходимости применения дополнительных мер по изменению системы защиты информации, содержащей персональные данные, в целях приведения ее к достаточному уровню.
- 8.15. Контроль за соблюдением работниками Фонда требований, предъявляемых к ним и установленных настоящим Положением, осуществляется лицом, ответственным за информационную безопасность.

9. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1 В целях защиты персональных данных, хранящихся у Фонда, субъект персональных данных имеет право на:

- требовать от Фонда уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются

необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

- требовать перечень своих персональных данных, обрабатываемых Фондом и информацию об источнике их получения;
- получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

9.2 Для реализации вышеуказанных прав субъект персональных данных, может в порядке, установленном ст. 14 Закона о персональных данных, обратиться в Фонд с соответствующим запросом. Для выполнения таких запросов представитель Фонда устанавливает личность субъекта персональных данных и при необходимости запрашивает дополнительную информацию.

9.3 Если субъект персональных данных считает, что Фонд осуществляет обработку его персональных данных с нарушением требований законодательства о персональных данных или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Фонда в порядке, предусмотренном законодательством Российской Федерации.

9.4 В целях обеспечения достоверности персональных данных субъект персональных данных обязан при заключении договора предоставить Фонду полные и достоверные данные о себе.

10. ПРАВА И ОБЯЗАННОСТИ ФОНДА КАК ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

10.9. Фонд в соответствии с Законом о персональных данных в том числе, но не исключительно, исполняет следующие обязанности:

- предоставляет субъекту персональных данных или его представителю по их просьбе информацию, предусмотренную Законом о персональных данных, в том числе о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с этими персональными данными;
- в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя дает в письменной форме мотивированный ответ, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа;
- разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку, если в соответствии с федеральным законом предоставление персональных данных и (или) получение Фондом согласия на обработку персональных данных являются обязательными;
- в случае получения персональных данных не от субъекта персональных данных предоставляет субъекту персональных данных (за исключением установленных Законом о персональных данных случаев) до начала обработки таких

персональных данных информацию, предусмотренную Законом о персональных данных;

- при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных;
 - вносит необходимые изменения в персональные данные в случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, а также уведомляет об этом субъекта персональных данных или его представителя и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;
 - уничтожает персональные данные в случае представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, а также уведомляет об этом субъекта персональных данных или его представителя и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;
 - прекращает обработку персональных данных при достижении целей их обработки.
- 10.10. Фонд в соответствии с Законом о персональных данных в том числе, но не исключительно имеет право:
- поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора;
 - продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных, в случае отзыва субъектом персональных данных согласия на обработку персональных данных;
 - мотивированно отказать субъекту персональных данных в выполнении повторного запроса на предоставление необходимой информации и ознакомления с обрабатываемыми персональными данными, не соответствующего условиям, предусмотренным Законом о персональных данных.

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

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

11.9.1. Дисциплинарная ответственность:

- а) Разглашение персональных данных субъекта персональных данных Фонда, то есть передача посторонним лицам, не имеющим к ним доступа; публичное раскрытие; утрата документов и иных носителей, содержащих персональные данные работника; иные нарушения обязанностей по их защите, обработке и хранению, установленных настоящим Положением, а также иными локальными нормативными

актами Фонда, лицом, ответственным за получение, обработку и защиту персональных данных работника, влекут наложение на него дисциплинарного взыскания - выговора, увольнения (пп. «в» п.6 ч. 1 ст. 81 Трудового кодекса РФ).

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

11.9.2. Административная ответственность:

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

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

11.9.3. Уголовная ответственность – за нарушение неприкосновенности частной жизни (в

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