

Микрокредитная компания,
некоммерческая организация
«Фонд поддержки малого и
среднего предпринимательства
Республики Алтай»



«Алтай Республиканын кичүү ле
орто аргачылыгы јәмөбүр фонд»
деп микрофинанс организация,
коммерческый эмес организация

649000, Республика Алтай, г. Горно-Алтайск, ул. Черес-Туркина, 27 телефоны: (38822) 4-72-21; 2-31-55 fond-ra@ya.ru

УТВЕРЖДАЮ

Директор МКК, НКО

«Фонд поддержки МСП РА»

Н.В. Еядокимова

«26» *Июль* 2019 г.

ПОЛИТИКА
обеспечения безопасности персональных данных
при их обработке в МКК, НКО «Фонд поддержки
малого и среднего предпринимательства
Республики Алтай»

г. Горно-Алтайск
2019 г.

1. Общие положения

Политика обеспечения безопасности персональных данных при их обработке в Микрокредитной компании, некоммерческой организации «Фонд поддержки малого и среднего предпринимательства Республики Алтай» (далее - Политика) разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и применяется ко всем персональным данным, обрабатываемым в Микрокредитной компании, некоммерческой организации «Фонд поддержки малого и среднего предпринимательства Республики Алтай» (далее - Фонд).

Цель Политики состоит в определении объема обрабатываемых персональных данных, принципов обработки персональных данных, а также способов и мер их защиты.

Публикация Политики на сайте Фонда осуществляется для доведения до клиентов и лиц, желающих воспользоваться услугами Фонда, необходимой информацией, позволяющей понять, какие персональные данные и с какой целью собираются Фондом, каким образом они обрабатываются, какие требования к обеспечению их безопасности реализуются.

Предоставление клиентам Фонда услуг требует сбора и дальнейшей обработки персональных данных, позволяющих идентифицировать клиентов Фонда, их представителей и (или) выгодоприобретателей, бенефициарных владельцев и осуществлять их обслуживание. Состав и объем требуемых сведений определяются действующим законодательством РФ и внутренними нормативными документами Фонда. В случае непредставления указанными лицами требуемой информации Фонд имеет право отказать им в обслуживании.

Действуя в своих интересах, клиенты Фонда имеют право привлекать третьих лиц к участию в своих отношениях с Фондом. В этом случае они обязаны обеспечить предоставление требуемой информации указанными лицами.

В случае, когда обработка персональных данных, содержание и объем которых соответствует требованиям законодательства РФ, или обработки персональных данных необходима 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 будет являться выгодоприобретателем или поручителем, а так же в иных случаях, предусмотренными законодательством РФ осуществляется без письменного согласия.

В остальных случаях обработка ПДн в Фонде осуществляется после получения письменного согласия субъекта ПДн.

Фонд оставляет за собой право вносить необходимые изменения в Политику при изменении действующего законодательства РФ и условий своей деятельности.

Действующая редакция Политики подлежит размещению на информационном стенде, в сети Интернет на официальном сайте Фонда www.binkra.ru, в целях обеспечения неограниченного доступа к сведениям о реализуемых требованиях защиты персональных данных.

1.1. Основные понятия, используемые в Политике:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) 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;

- 4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
- 5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- 8) 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;
- 9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- 10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- 11) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Правовые основы и цели обработки персональных данных

Фонд осуществляет обработку персональных данных в целях осуществления возложенных на Фонд законодательством Российской Федерации функций в соответствии с Трудовым и Налоговым кодексами Российской Федерации, федеральным законом от 24.07.2007 № 209 - ФЗ «О развитии малого и среднего предпринимательства в РФ», Федеральным законом от 30.12.2004 № 218 – ФЗ «О кредитных историях», Федеральным законом от 01.04.1996 № 27 -ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», ФЗ от 27.07.2006 № 152 – ФЗ «О персональных данных», Уставом и правовыми актами Фонда.

Целью настоящей Политики является обеспечение безопасности объектов персональных данных от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональным данным.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

3. Сфера действия настоящей Политики

Требования настоящей Политики распространяются на всех клиентов и сотрудников Фонда, в том числе штатных, временных, оказывающих услуги по гражданско - правовому договору и т.п., а также всех прочих лиц (аудиторы, программисты и т.п.)

4. Перечень обрабатываемых персональных данных

Под персональными данными понимается любая информация, относящиеся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). В процессе своей деятельности Фонд осуществляет обработку следующих персональных данных:

- фамилия, имя, отчество (в том числе прежние), пол, дата и место рождения;

- копии паспортов, паспортные данные, данные других документов, удостоверяющих личность (серия, номер, дата выдачи, код подразделения и наименование органа, выдавшего документ) и гражданство¹;
- адрес места жительства (по регистрации и фактический) и дата регистрации по месту жительства или по месту пребывания;
- идентификационный номер налогоплательщика (при наличии);
- номера контактных телефонов, адрес электронной почты;
- информация о предоставленных услугах, в том числе информация о счетах и операциях по ним;
- информация о платежеспособности, составе семьи и имущественных правах лиц, изъявивших желание воспользоваться услугами Фонда;
- сведения о трудовых отношениях субъектов персональных данных;
- сведения, собираемые в целях исполнения требований действующего законодательства РФ при рассмотрении вопросов присма на работу, обеспечения необходимых условий работы и профессионального роста, а также полученные в результате осуществления трудовых отношений с работниками Фонда.

5. Лица, имеющие доступ к персональным данным

К обрабатываемым персональным данным имеют доступ сотрудники Фонда и лица, оказывающие услуги по гражданско-правовым договорам, которые в соответствии с их должностными обязанностями наделены такими полномочиями.

Доступ иных лиц к персональным данным, обрабатываемым Фондом, может быть предоставлен исключительно в предусмотренных законом случаях, либо с согласия субъекта персональных данных.

Существенным условием договора, заключаемого Фондом с лицом, которому предоставляется доступ к персональным данным, является обязанность соблюдения указанным лицом конфиденциальности и обеспечения безопасности персональных данных при их обработке.

При принятии нового работника ответственное лицо за обработку персональных данных обязано организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных систем по обработке персональных данных.

6. Способы обработки Фондом персональных данных

В целях исполнения требований действующего законодательства РФ и своих договорных обязательств Фонд использует как автоматизированную обработку персональных данных, так и неавтоматизированную обработку с использованием бумажного документооборота.

Совокупность операций обработки включает сбор, запись, систематизацию, хранение, уточнение, извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, уничтожение персональных данных.

Принятие решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, на основании исключительно автоматизированной обработки персональных данных Фондом не производится.

7. Сроки обработки персональных данных

Сроки обработки персональных данных, указанных в разделе 3 Политики, определяются исходя из целей обработки персональных данных в соответствии со сроком действия договора с субъектом ПДн, сроком исковой давности, сроками хранения документов, установленными приказом Министерства культуры Российской Федерации от 25.08.2010 г. № 558 «Об утверждении «Перечня типовых управленческих документов, образующихся в процессе деятельности государственных органов, органов местного

¹ Иностранцами гражданами и лицами без гражданства дополнительно предоставляются данные миграционной карты и документа, подтверждающего право иностранного гражданина на пребывание (проживание) в Российской Федерации.

самоуправления и организаций, с указанием сроков хранения», иными требованиями законодательства РФ, а так же сроком предоставленного субъектом персональных данных согласия на обработку персональных данных, в случаях, когда такое согласие должно быть предоставлено в соответствии с требованиями законодательства.

8. Реализуемые Фондом требования к защите персональных данных

Все работники Фонда и лица, оказывающие услуги по гражданско-правовым договорам обязаны обеспечивать защиту персональных данных его клиентов. Безопасность персональных данных при их обработке в информационных системах Фонда обеспечивается с помощью системы защиты информации ограниченного доступа, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Размещение информационных систем, специального оборудования и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях, обеспечивает сохранность носителей персональных данных и средств защиты информации, а также исключает возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

При обработке персональных данных в информационных системах Фонда обеспечивается:

- надлежащая защита оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица;
- 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, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение установления посторонних программных обеспечений, подключения личных мобильных устройств и носителей информации, а так же записывать на них защищаемую информацию;
- постоянный контроль уровня защищенности.

9. Ответственность работников при обработке персональных данных

Ответственность сотрудников, при обработке персональных данных в информационных системах Фонда, наступает в соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

При нарушениях сотрудниками Фонда, пользователей информационной системы обработки персональных данных, правил, связанных с безопасностью персональных данных, они несут ответственность, установленную действующим законодательством Российской Федерации.

1. Положение об обработке персональных данных клиентов в Микрокредитной компании, некоммерческой организации «Фонд поддержки малого и среднего предпринимательства Республики Алтай» (Приложение № 1 к настоящей политике) ;

2. Положение об обработке персональных данных работников Микрокредитной компании, некоммерческой организации «Фонд поддержки малого и среднего предпринимательства Республики Алтай» (Приложение № 2 к настоящей политике)

ПОЛОЖЕНИЕ

**об обработке персональных данных клиентов
в Микрокредитной компании, некоммерческой
организации «Фонд поддержки малого и среднего
предпринимательства Республики Алтай»**

1. Общие положения

Настоящее Положение об обработке персональных данных клиентов (далее – Положение) устанавливает порядок и условия проведения работ по обработке персональных данных (далее – ПДн) клиентов – представителей юридических лиц, индивидуальных предпринимателей и физических лиц (далее – клиенты) МКК, НКО «Фонд поддержки малого и среднего предпринимательства Республики Алтай» (далее – Фонд) с использованием средств автоматизации и без использования таких средств.

Положение разработано с целью обеспечения защиты прав и свобод субъекта персональных данных (далее – субъект ПДн) при обработке его ПДн, а также с целью установления ответственности должностных лиц Фонда, имеющих доступ к ПДн его клиентов, за невыполнение требований и норм, регулирующих обработку ПДн.

Данное Положение разработано в соответствии с требованиями:

- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";
- Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Настоящее Положение вступает в силу с момента его утверждения директором Фонда и действует бессрочно до замены его новым Положением или до наступления иных случаев, предусмотренных законодательством.

Настоящее Положение является обязательным для исполнения всеми сотрудниками Фонда, имеющими доступ к ПДн клиентов – субъектов ПДн. Все сотрудники Фонда, связанные с обработкой ПДн и имеющие доступ к ПДн клиентов, должны быть ознакомлены с настоящим Положением под роспись.

Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля (надзора), а также в целях закрепленияработанной Фондом практики операций с ПДн.

Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм настоящего Положения возлагается на назначаемого приказом по Фонду сотрудника, ответственного за организацию обработки ПДн.

При появлении новых типов ПДн допускается разграничение доступа к ним на основании приказа директора Фонда.

Фонд учитывает требования настоящего Положения при разработке и утверждении любых внутренних документов Фонда, связанных с обработкой ПДн.

2. Основные понятия и определения

В Положении применяются термины и определения в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

«Положении об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденном Постановлением Правительства РФ от 15 сентября 2008 года № 687, другими нормативно-правовыми актами, регулирующими защиту прав субъектов ПДн и обеспечение безопасности ПДн.

3. Состав ПДн

ПДн клиентов Фонда – это любая информация, относящаяся к прямо или косвенно определенному или определяемому клиенту Фонда (субъекту ПДн) – физическому лицу (индивидуальному предпринимателю). Перечень ПДн, обрабатываемых в Фонде (далее – Перечень ПДн), приведен в Приложении 1.

В ходе осуществления Фондом своих функций Перечень ПДн может быть изменен.

При получении ПДн, не указанных в Перечне ПДн, указанные данные подлежат немедленному уничтожению лицом, непреднамеренно получившим указанные данные.

4. Специальные категории ПДн

Запрещается обрабатывать ПДн о политических, религиозных и философских убеждениях, а также об интимной жизни клиента Фонда. Указанные специальные категории ПДн в деятельности Фонда не используются и не обрабатываются.

Фонд не вправе производить обработку данных о судимости клиента, за исключением в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Сведения о расовой и национальной принадлежности клиентов Фонда не обрабатываются. Фотографии, находящиеся в документах, удостоверяющих личность клиента Фонда, и иные аналогичные данные не относятся к сведениям о расовой и национальной принадлежности.

В случае если обработка специальных категорий ПДн клиента Фонда необходима по действующему законодательству или для осуществления деятельности Фонда, то такая обработка осуществляется с

письменного согласия клиента, за исключением случаев, предусмотренных законодательством Российской Федерации в области ПДн.

5. Биометрические ПДн

Фонд не обрабатывает сведения, которые характеризуют физиологические особенности клиентов и на основе которых можно установить их личность. В соответствии с требованиями ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Данные изображения лица» система охранного видеонаблюдения, используемая в Фонде, не обрабатывает биометрические ПДн, на основании которых возможно идентифицировать личность клиента Фонда.

Сканирование фотографий в документах, идентифицирующих личность клиентов (например, в паспортах), в Фонде не осуществляется. Передаваемые в рамках договоров с определенными третьими лицами паспорта клиентов не соответствуют требованиям, предъявляемым к форматам записи изображений, установленными ГОСТ Р ИСО/МЭК 19794-5-2006.

В случае если обработка биометрических ПДн клиента Фонда необходима по действующему законодательству или для осуществления деятельности Фонда, то такая обработка осуществляется с письменного согласия клиента, за исключением случаев, предусмотренных законодательством Российской Федерации в области ПДн.

6. Общедоступные ПДн

В целях информационного обеспечения могут создаваться общедоступные источники ПДн (в том числе справочники, адресные книги). В общедоступные источники ПДн с письменного согласия клиента могут включаться его фамилия, имя, отчество, год и место рождения, адрес, включая адрес электронной почты, клиентский номер, IP-адрес, сведения о профессии и иные ПДн, сообщаемые субъектом ПДн или находящиеся в Перечне ПДн.

Сведения о клиенте Фонда должны быть в любое время исключены из общедоступных источников ПДн по запросу клиента либо по решению суда или иных уполномоченных государственных органов.

В случае обработки общедоступных ПДн клиента обязанность доказывания того, что обрабатываемые ПДн являются общедоступными, возлагается на Фонд.

7. Цели и сроки обработки ПДн

Фонд обрабатывает ПДн с целью осуществления возложенных на Фонд законодательством Российской Федерации функций в соответствии с (в том числе, но не ограничиваясь), Гражданским кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности, «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О несостоятельности (банкротстве) кредитных организаций», «О персональных данных», «О бухгалтерском учете», принятыми в их исполнение нормативными актами Правительства России, а также в соответствии с нормативными актами Банка России и в иных целях в рамках действующего законодательства. Фонд собирает ПДн только в объеме, необходимом для достижения названных целей.

Допускаются иные цели обработки ПДн в случае, если указанные действия не противоречат действующему законодательству, деятельности Фонда и на проведение указанной обработки получено согласие клиента Фонда.

Хранение ПДн осуществляется в соответствии с согласием субъектов ПДн и в течение срока, указанного в согласии с учетом требований законодательства.

В случае отсутствия в указанных нормативно-правовых актах сроков хранения отдельных видов ПДн, указанные ПДн подлежат хранению в течение срока, указанного в согласии соответствующего субъекта ПДн.

8. Обработка ПДн

Фонд осуществляет обработку ПДн в целях соблюдения законодательных и нормативных актов, минимизации финансовых рисков (включая сохранность активов и ресурсов Фонда), зависящих от ПДн клиента.

Обработку ПДн осуществляют сотрудники Фонда, уполномоченные на то должностными инструкциями, иными внутренними документами Фонда или организационно-распорядительными документами по Фонду.

Сотрудники Фонда имеют право получать только те ПДн, которые необходимы им для выполнения конкретных должностных обязанностей.

Сотрудники Фонда, осуществляющие обработку ПДн клиентов, должны быть проинформированы о факте такой обработки, об особенностях и правилах такой обработки, установленных нормативно-правовыми актами и внутренними документами Фонда.

В рамках информирования сотрудников Фонда о факте обработки ПДн, Фонд обязывает сотрудников Фонда самостоятельно изучать и соблюдать внутренние нормативные документы, регламентирующие как общий порядок работы с ПДн, так и специальные нормы, касающиеся совершения отдельных действий, связанных с обработкой ПДн клиентов Фонда.

9. Согласие на обработку ПДн

Обработка ПДн клиентов осуществляется с их согласия на обработку их ПДн, а также в иных случаях, предусмотренных статьей 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Согласие на обработку ПДн может быть дано клиентом или его законным представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя клиента полномочия данного представителя проверяются Фондом. Форма согласия может быть в письменной, конклюдентной или иной форме, предусмотренной действующим законодательством.

При недееспособности клиента письменное согласие на обработку его данных дает его законный представитель.

Фонд обязан иметь доказательство получения согласия клиента на обработку его ПДн (в том случае, если такое согласие является необходимым).

9.1. Письменная форма согласия

В случаях, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта персональных данных:

- Обработка специальных категорий ПДн,
- Обработка биометрических ПДн,
- Трансграничная передача ПДн в страны, не обеспечивающие адекватной защиты прав субъекта ПДн,
- Включение в общедоступные источники ПДн,
- Принятие решений на основании исключительно автоматизированной обработки ПДн.

Согласие клиента на обработку его ПДн в Фонде должно включать в себя сведения и информацию, требующуюся для включения в согласие в соответствии с действующим законодательством и внутренними документами Фонда.

9.2. Конклюдентная форма согласия

В соответствии со статьей 158 Гражданского кодекса Российской Федерации конклюдентное или подразумеваемое согласие – это действие лица, выражающее его волю установить правоотношение (например, совершить сделку), но не в форме устного или письменного волеизъявления, а поведением, по которому можно сделать заключение о таком намерении.

Клиенты Фонда дают конклюдентное согласие на обработку их ПДн в случаях, описанных в Таблица 1.

Таблица 1. Случаи обработки ПДн на основании конклюдентного согласия

Вид обработки ПДн	Цель обработки	Обрабатываемые ПДн
Заполнение анкет, в т.ч. и на Web-сайте Фонда.	Изучение возможностей по получению и обслуживанию кредита.	п.2.1.3 Перечня ПДн
Регистрация на Web-сайте и мероприятиях, проводимых Фондом	Уведомление о мероприятиях, акциях, предоставляемых скидках	Фамилия, имя, отчество, контактная информация.
Участие в опросах, проводимых Фондом.	Проведение опросов и исследований в области финансовых услуг, проведения маркетинговых программ, статистических исследований.	п.2.1.3 Перечня ПДн.

9.3. Отзыв согласия

Клиент Фонда может в любой момент отозвать свое согласие на обработку ПДн при условии, что подобная процедура не нарушает требований законодательства РФ и допускается условиями договора, одной из сторон по которому является Фонд, а клиент является либо другой стороной по договору, либо выгодоприобретателем, либо поручителем, либо залогодателем.

В случае отзыва клиентом Фонда согласия на обработку ПДн Фонд вправе продолжить обработку ПДн без согласия клиента при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9.4. Обработка ПДн без согласия

В соответствии с пунктами 2 - 11 части 1 статьи 6, а также пунктом 4 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» обработка ПДн может осуществляться без согласия. В Фонде к таким ситуациям относятся те, которые указаны в Таблице 2.

Таблица 2. Случаи обработки ПДн без согласия (по состоянию законодательства на дату утверждения Положения)

Вид обработки ПДн	Основание
Заключение договора с клиентом	Ст.6.1.5 ФЗ-152
Взаимодействие с Пенсионным фондом РФ	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с налоговыми органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с таможенными органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с Федеральной службой финансового мониторинга	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1

Взаимодействие с Банком России	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с органами предварительного следствия	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с органами внутренних дел	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с судебными органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие со Счетной палатой Российской Федерации	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с Федеральным органом исполнительной власти в области финансовых рынков	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с Фондом социального страхования Российской Федерации	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с органами принудительного исполнения судебных актов, актов других органов и должностных лиц	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с организациями, осуществляющими функции по обязательному страхованию вкладов	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с лицами, указанными клиентом Фонда в завещательном распоряжении	Ст.6.1.1 ФЗ-152, ст.26 ФЗ ФЗ- 395-1 и ст.1128 ГК РФ
Взаимодействие с нотариальными конторами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с иностранными консульскими учреждениями	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Заполнение анкет и заявок на получение займов	Ст.6.1.5 ФЗ-152
Оформление договоров аренды, лизинга, доверительного управления, в которых клиент Фонда указан как выгодоприобретатель	Ст.6.1.5 ФЗ-152
Идентификация клиентов в рамках законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма	Ст.6.1.1 ФЗ-152 и ФЗ-115
Расчет платежными поручениями	Ст.6.1.1 ФЗ-152 и ст.863 ГК РФ, а также Положения

10. Порядок обработки ПДн с использованием средств автоматизации

Обработка ПДн в Фонде может проводиться с использованием средств автоматизации (информационных систем) и без таковых. Конкретный способ обработки ПДн определяется на основании процедур использования данных, определенных внутренними документами Фонда.

Обработка ПДн в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и методических документов ФСТЭК и ФСБ России по защите информации.

Фонд осуществляет обработку ПДн в ИСПДн структурных подразделений Фонда. К ИСПДн Фонда относятся информационные системы, поддерживающие выполнение возложенных на Фонд законодательством РФ функций, в которых обрабатываются ПДн, содержащиеся в Перечне ПДн.

Список информационных систем, в которых обрабатываются ПДн, их классификация, требования по обеспечению безопасности обрабатываемых в них ПДн клиентов Фонда описаны в отдельных нормативных документах Фонда.

Контроль за соответствием обработки ПДн заявленным целям возлагается на лицо, ответственное за обработку ПДн в Фонде, и на руководителей соответствующих подразделений.

Необходимость доступа работников Фонда к ПДн, обрабатываемым в ИСПДн Фонда, документально определена в их должностных инструкциях.

10.1. Исключительно автоматизированная обработка ПДн

Исключительно автоматизированная обработка ПДн в Фонде не осуществляется. Во всех процессах обработки ПДн клиентов с использованием средств автоматизации принимают участие ответственные сотрудники Фонда.

10.2. Порядок обработки ПДн без использования средств автоматизации

Обработка ПДн без использования средств автоматизации (далее – неавтоматизированная обработка ПДн) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, база данных) на электронных носителях информации.

При неавтоматизированной обработке ПДн на бумажных носителях:

- не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы;

- ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие ПДн, формируются в дела в зависимости от цели обработки ПДн;

- дела с документами, содержащими ПДн, должны иметь внутренние описи документов с указанием цели обработки и категории ПДн.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовые формы), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, регистры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес оператора и лиц, которым оператором поручена обработка ПДн, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;

- типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, - при необходимости получения письменного согласия на обработку ПДн;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

- типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

Неавтоматизированная обработка ПДн в электронном виде осуществляется на внешних электронных носителях информации. При отсутствии технологической возможности осуществления неавтоматизированной обработки ПДн в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка соответствующих средств защиты информации), исключая возможность несанкционированного доступа к ПДн лиц, не допущенных к их обработке.

Электронные носители информации, содержащие ПДн, учитываются в журнале учета электронных носителей ПДн. К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории ПДн.

При несовместимости целей неавтоматизированной обработки ПДн, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

Документы и внешние электронные носители информации, содержащие ПДн, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

11. Получение/сбор ПДн

Источниками ПДн клиентов в Фонде являются:

- Анкеты,

- Договоры,

- Формы,

- Сайт Фонда,

- Заявки/заявления,

- Телефон,

- Копии предоставляемых документов,

- иные источники в соответствии с действующим законодательством Российской Федерации.

Клиент обязан предоставлять Фонду достоверные сведения о себе и одновременно сообщать Фонду об изменении своих ПДн. Фонд имеет право проверять достоверность сведений, предоставленных субъектом, сверяя данные, предоставленные субъектом, с имеющимися у Фонда документами.

12. Получение ПДн не напрямую от клиента Фонда

Фонд получает ПДн клиента от него самого или от третьих лиц при условии наличия согласия на обработку и/или оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». В ряде случаев Фонд

получает персональные данные от третьих лиц, получающих ПДн у субъектов, в том числе в качестве представителей Фонда на основании доверенности, а также имеющих договорные отношения с субъектом ПДн либо с Фондом. В качестве таких третьих лиц могут выступать страховые организации и другие лица. В данном случае, в соответствии с частью 4 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Фонд не обязан получать согласие субъекта ПДн на обработку его ПДн если ПДн получены не от субъекта ПДн и их обработка не поручена Фонду оператором, Фонд до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» права субъекта ПДн;
- источник получения ПДн.

Фонд освобождается от обязанности предоставить субъекту ПДн указанные сведения в случаях, если: ПДн получены Фондом на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является клиент Фонда.

ПДн сделаны общедоступными клиентом Фонда или получены из общедоступного источника.

Фонд осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы клиента Фонда.

Предоставление клиенту Фонда сведений, предусмотренных ч. 3 ст. 18 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», нарушает права и законные интересы третьих лиц.

13. Использование ПДн

Доступ к ПДн субъекта имеют сотрудники Фонда, которым ПДн необходимы в связи с исполнением ими трудовых обязанностей. Перечень сотрудников, имеющих доступ к ПДн, утверждается приказом директора Фонда.

Доступ сотрудников, не включенных в вышеуказанный перечень, осуществляется на основании приказа директора Фонда, подготовленного на основании служебной записки руководителя сотрудника с положительной резолюцией ответственного за обработку ПДн в Фонде.

В случае если Фонду оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к ПДн клиентов Фонда, то соответствующие данные предоставляются Фондом только после подписания с лицами, осуществляющими обработку ПДн по поручению Фонда, соответствующего соглашения, в котором должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Использование и хранение биометрических и специальных категорий ПДн вне информационных систем ПДн может осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

14. Использование ПДн с целью идентификации клиентов

В ходе выполнения функций кредитной организации, связанных с необходимостью идентификации состоящих на обслуживании клиентов, Фонд в соответствии с Федеральным законом №115-ФЗ от 07.08.2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путем» обязан обрабатывать следующие персональные данные клиентов:

- фамилия, имя, отчество;
- полная дата и место рождения;
- паспортные данные;
- место жительства, прописки;
- гражданство;
- идентификационный номер налогоплательщика (если имеется);
- номера контактных телефонов и факсов (если имеются).

Письменное согласие на обработку указанной информации от субъекта ПДн не требуется на основании пункта 3 части 1 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» в силу того, что обработка осуществляется в соответствии с Федеральным законом №115-ФЗ от 07.08.2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путем».

15. Использование ПДн с целью выдачи займов

В ходе выполнения функций кредитной организации, связанных с проведением операций по выдаче и погашению гарантий, кредитов и займов, Фонд также обрабатывает ПДн клиента, указанные в Приложении 1 к настоящему Положению. Среди них в том числе:

- образование, данные об ученых степенях;
- финансовое положение (доходы, долги, владение имуществом, денежные вклады, полученные гарантии и субсидии и др.);

- факты биографии и трудовая деятельность (место работы, размер заработка, судимость, служба в вооруженных силах, работа на выборных должностях, на государственной службе, участие в профессиональных объединениях и профсоюзах и др.).

В случае если указанные данные предоставлены на этапе рассмотрения заявки на предоставление займа, и договор займа не был заключен, то их обработка завершается, а данные уничтожаются в течение 4 (четырёх) лет от даты их предоставления. В случае же если кредитный либо иной подобный договор был заключен, обработка ПДн завершается в течение срока, указанного в согласии на обработку.

Согласие на обработку указанных ПДн получается у потенциального заемщика до заключения кредитного договора и начала обработки таких данных.

16. Использование ПДн субъекта в целях продвижения товаров, работ, услуг

Клиент Фонда даст свое согласие на обработку его ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с клиентом Фонда с помощью средств связи, включая, но, не ограничиваясь: почтовая рассылка, рассылка SMS-сообщений, электронная почта, телефон (включая мобильный), факсимильная связь, сеть Интернет, только при следующих условиях:

- Действие данного согласия распространяется только на
 - проведение опросов и исследований в области финансовых услуг;
 - проведение маркетинговых программ;
 - проведение статистических исследований;
 - уведомления о мероприятиях, акциях, предоставляемых скидках.

Действие данного согласия распространяется только на взаимоотношения, возникающие в рамках исполнения Фондом обязательств по заключенным с клиентом договорам, а также продвижения своих услуг и услуг своих партнеров.

Действие данного согласия распространяется на следующие операции по обработке ПДн: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Данное согласие действует в течение срока, указанного в таком согласии.

В остальных случаях обработка ПДн в целях продвижения работ и услуг на рынке путем прямых контактов с клиентом Фонда с помощью средств связи допускается только с его предварительного согласия. Бремя доказывания наличия согласия лежит на Фонде.

Фонд обязан немедленно прекратить по требованию клиента обработку его ПДн, если это не противоречит действующему законодательству.

17. Передача ПДн третьим лицам

Передача ПДн третьим лицам (исключая надзорные органы) возможна только в случаях, прямо предусмотренных законодательными и нормативными актами, либо в случае согласия субъекта ПДн.

В случае если обязанность либо возможность предоставления имеющихся в распоряжении Фонда ПДн иным лицам (включая органы государственной и муниципальной власти) установлена законодательством, Фонд обязан предоставить указанные данные в составе, виде и сроки, указанные в законодательных или нормативных актах.

Если обязанность предоставления ПДн фиксируется соответствующим запросом (ходатайством) уполномоченного лица, запрос подлежит обязательной проверке в целях контроля над обоснованностью предоставления запроса. При обоснованности подобного запроса, юрист информирует об этом подразделение, которое осуществляет обработку запрошенных данных, которое в свою очередь формирует ответ на запрос (при необходимости – организует деятельность иных подразделений по подготовке ответа). При необоснованности запроса, юрист информирует об этом подразделение, которое осуществляет обработку запрошенных данных, которое в свою очередь направляет отправителю запроса письменное уведомление об отказе в предоставлении ПДн.

Любые запросы на раскрытие ПДн от третьих лиц, не являющихся субъектами раскрываемых ПДн, подлежат обязательному рассмотрению на предмет обоснованности.

При передаче ПДн третьим лицам Фонд обязан уведомлять лиц, получивших ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие ПДн, обязаны соблюдать их конфиденциальность и безопасность. Данное требование не распространяется на обмен ПДн в порядке, установленном законодательством.

Третьи лица и цели передачи им ПДн клиентов ФБР указаны в Таблица 3, а также в разделе «Передача ПДн третьим лицам без согласия».

Таблица 3. Перечень третьих лиц, которым возможна передача ПДн клиента

п/п	Тип третьего лица	Цель передачи
Бюро кредитных историй	Формирование, обработка и хранение кредитных историй клиентов ФБР, а также предоставление кредитных отчетов о клиентах ФБР	

Банковские платёжные агенты и субагенты, принимающие платежи клиентов ФБР в соответствии с действующим законодательством, и т.ч. банки-партнёры

Операции по выдаче и погашению гарантий, кредитов и займов

Передача ПДн третьим лицам осуществляется только с согласия клиента за исключением случаев, предусмотренных действующим законодательством.

18. Передача ПДн третьим лицам без согласия

Фонд вправе осуществлять передачу ПДн в соответствующих целях запроса объемах без согласия субъекта ПДн следующим третьим лицам:

Пенсионный фонд РФ,
Налоговые органы,
Таможенные органы,
Федеральную службу финансового мониторинга,
Банк России,
Органы предварительного следствия (при наличии согласия руководителя следственного органа),
Органы внутренних дел,
Судебные органы,
Счетную палату Российской Федерации,
Федеральный орган исполнительной власти в области финансовых рынков,
Фонд социального страхования Российской Федерации,
Органы принудительного исполнения судебных актов, актов других органов и должностных лиц в случаях, предусмотренных законодательными актами об их деятельности,
Нотариальным конторам (по находящимся в их производстве наследственным делам),
а также другим третьим лицам в случаях, предусмотренных законодательными актами об их деятельности.

19. Трансграничная передача ПДн

Трансграничная передача ПДн осуществляется Фондом при осуществлении расчетной деятельности в порядке направления разъяснений в рамках исполнения требований национального законодательства о противодействии отмыванию доходов, полученных преступным путем и финансированию терроризма.

Трансграничная передача ПДн также может быть осуществлена в адрес организаций, зарегистрированных в иных странах, при условии, что законодательство указанных стран позволяет сделать вывод об адекватной защите ПДн. Оценку возможности подобной передачи осуществляет уполномоченный по обработке ПДн в Фонде в рамках действующего законодательства.

Иная трансграничная передача осуществляется исключительно с письменного согласия субъекта ПДн.

20. Передача ПДн в государственные органы

В соответствии с действующим законодательством Фонд вправе осуществлять передачу ПДн государственным органам, указанным в разделе «Передача ПДн третьим лицам без согласия», а также другим государственным органам и должностным лицам в случаях, предусмотренных законодательными актами об их деятельности.

21. Уточнение ПДн

Уточнение ПДн Клиента производится путем обновления или изменения данных в информационной системе или на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн клиента.

Уточнение ПДн производится в рамках действующей в Фонде системы документооборота с соблюдением принципов, изложенных в настоящем Положении.

22. Блокирование ПДн

Блокирование ПДн представляет собой деятельность Фонда по временному прекращению обработки ПДн Клиентов (за исключением случаев, если обработка необходима для уточнения ПДн). Блокирование осуществляется в случае, если клиентом Фонда или его законным представителем, либо уполномоченным органом по защите прав субъектов ПДн выявлена недостоверность ПДн при условии, что такое блокирование не нарушает права и законные интересы клиента или третьих лиц.

В случае подтверждения факта неточности ПДн Фонд на основании сведений, представленных клиентом Фонда или его законным представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов, обязан уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Фонда) в течение 7 (семи) рабочих дней со дня представления таких сведений и снять блокирование ПДн.

Блокирование осуществляется руководителем подразделения Фонда, осуществляющего обработку ПДн клиентов при условии уведомления соответствующих подразделений Фонда, контролирующих правильность процесса блокирования.

Если обработка ПДн осуществляется другим лицом, действующим по поручению Фонда, то Фонд обязан обеспечить их блокирование с момента получения обращения от клиента Фонда или его законного

представителя или получения запроса от уполномоченного органа по защите прав субъектов ПДн на период проверки.

Блокирование ПДн в информационных системах Фонда может быть осуществлено путем установления специальных прав доступа к ПДн либо путем копирования данных на специальное рабочее место с ограниченным доступом с одновременным удалением данных из первоначального места хранения.

Блокирование ПДн на материальных носителях производится путем их изъятия и хранения у уполномоченного лица Фонда в защищенном месте, исключающем возможность несанкционированного доступа к нему посторонних лиц.

Блокирование материального носителя информации содержащего ПДн как подлежащие, так и не подлежащие блокированию, осуществляется путем копирования материального носителя способом, исключающим совместное копирование определенных типов информации (удаление, вымарывание блокированного фрагмента). В дальнейшей деятельности используется копированный материальный носитель, не содержащий блокированной информации. Блокированный материальный носитель передается на хранение уполномоченному лицу Фонда.

Снятие блокирования осуществляется после уточнения ПДн на основании информации, переданной клиентом Фонда или его законным представителем, либо уполномоченным органом по защите прав субъектов ПДн.

Снятие блокирования сопровождается уведомлением уполномоченного лица Фонда, ответственного за хранение блокированных ПДн, о снятии блокирования после уточнения ПДн. Блокированные ПДн в информационных системах подлежат разблокировке и уточнению. Блокированные документы на материальных носителях подлежат возврату в подразделение, передавшее персональные данные для блокирования.

23. Хранение ПДн

Хранение ПДн клиентов должно осуществляться в форме, позволяющей определить клиента, не дольше, чем этого требуют цели и сроки обработки ПДн, указанные в разделе «Цели и сроки обработки персональных данных» данного Положения. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Хранение ПДн клиентов, цели обработки которых различны, должно осуществляться раздельно в рамках информационной системы или, при условии хранения на материальных носителях, в рамках структуры дел соответствующего подразделения Фонда.

Сотрудник Фонда, имеющий доступ к ПДн клиентов в связи с исполнением трудовых обязанностей:

Обеспечивает хранение информации, содержащей ПДн клиента, исключая доступ к ним третьих лиц.

В отсутствие сотрудника на его рабочем месте не должно находиться документов, содержащих ПДн клиентов.

При уходе в отпуск, служебную командировку и иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие ПДн клиентов лицу, на которое локальным актом Фонда будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, то документы и иные носители, содержащие ПДн клиентов, передаются другому сотруднику, имеющему доступ к ПДн клиентов по указанию руководителя структурного подразделения.

При увольнении сотрудника, имеющего доступ к ПДн клиентов, документы и иные носители, содержащие ПДн клиентов, передаются другому сотруднику, имеющему доступ к ПДн клиентов по указанию руководителя структурного подразделения и с уведомлением лица, ответственного за обработку ПДн в Фонде.

24. Архивирование ПДн

ПДн, неиспользуемые в операционной деятельности Фонда и цель обработки которых не достигнута, могут быть переведены на архивное хранение с соблюдением всех необходимых требований, предусмотренных Федеральным законом от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации» и иными нормативными актами в сфере организации хранения, комплектования, учета и использования архивных документов независимо от их формы собственности.

Архивирование ПДн производится в рамках действующих в Фонде систем документооборота и работы с архивными документами с соблюдением принципов, изложенных в настоящем Положении. Обязательным условием архивирования ПДн является обеспечение их конфиденциальности и безопасности.

Подразделения Фонда, хранящие архивные ПДн на бумажных носителях, обязаны обеспечить ограничение доступа к указанным данным только тех сотрудников, деятельность которых непосредственно связана с обработкой хранимого типа архивных ПДн. Доступ к архивным ПДн, хранение которых осуществляется на электронных носителях, должен быть ограничен исходя из требований информационной безопасности, указанных в данном Положении и отдельных локальных нормативных актах Фонда.

25. Обезличивание ПДн

С целью уменьшения объема ПДн, подлежащих защите в соответствии с требованиями 152-ФЗ, подзаконных актов и методических указаний, а также в целях снижения нагрузки и бремени на Фонд, приводящих к дополнительным затратам без повышения уровня защищенности ПДн и прав клиентов Фонда, может быть произведено обезличивание ПДн клиентов Фонда. Также обезличивание производится в целях предоставления статистической отчетности, агрегированной информации о деятельности Фонда, а также в иных целях, предусмотренных действующим законодательством, например, по достижении целей их

обработки или в случае утраты необходимости в достижении этих целей в соответствии со статьей 5 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Обезличенные ПДн должны представлять собой информацию на бумажном или магнитном носителе, принадлежность которой к конкретному физическому лицу невозможно определить без использования дополнительной информации в силу произведенных при обработке ПДн действий. Применяемые в Фонде механизмы обезличивания приведены в Таблица 4.

Таблица 4. Механизмы обезличивания ПДн

Алгоритм обезличивания	Описание	Примечание
Абстрагирование ПДн	Сделать ПДн менее точными путем группирования общих или непрерывных характеристик, т.е. не позволяющими отличить с помощью данного атрибута одного субъекта ПДн от других	Например, вместо указания конкретного возраста использовать кодификаторы (18-25 лет – 2, 26-33 года – 3 и т.д.).
Скрытие ПДн	Удалить всю или часть записи ПДн, не требуемые для деятельности организации	Применяется в том случае, если Фонд уже хранит неиспользуемые ПДн.
Внесение шума в ПДн		Добавить небольшое количество посторонней информации в ПДн
Замена ПДн		Переставить поля одной записи ПДн с теми же самыми полями другой аналогичной записи
Замена данных средним значением		Заменить выбранные данные средним значением для группы ПДн
Разделение ПДн на части	Использование перекрестных ссылок	Например, вместо одной таблицы использовать две – одна с ФИО и идентификатором субъекта ПДн, вторая – с тем же идентификатором субъекта ПДн и остальной частью ПДн.
Использование специальных алгоритмов	Маскирование ПДн или подмена определенных символов другими	Отдельные корпоративные СУБД могут быть оснащены специальными функциями маскирования (data masking pack).
Использование алгоритмов криптографического преобразования	Хэширование или шифрование	Использование средств криптографической защиты регулируется отдельным законодательством.

Лицо, ответственное за обработку ПДн клиентов обладает правом самостоятельного обезличивания ПДн клиентов. При необходимости получения иных обезличенных ПДн, сотрудники Фонда обязаны направить соответствующему лицу, ответственному за обработку ПДн клиентов, служебную записку с запросом соответствующих данных, если предоставление таких данных не осуществляется в рамках должностных обязанностей и внутрифондовых регламентов.

26. Уничтожение ПДн

Уничтожение ПДн производится Фондом:

при выявлении неустраиваемых неправомерных действий с ПДн клиентов;
по достижении целей обработки ПДн (при условии невозможности обезличивания ПДн);
при получении от клиента отзыва согласия на обработку ПДн (при условии, что такой отзыв не противоречит обязанностям Фонда продолжать обработку ПДн в соответствии с действующим законодательством);

по требованию клиента или уполномоченного органа по защите прав субъектов ПДн – если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Уничтожению подлежат все требуемые к уничтожению ПДн, зафиксированные на материальных носителях или хранящихся в информационных системах. Уничтожение ПДн на материальных носителях производится в соответствии со стандартными внутрифондовскими процедурами. Уничтожение ПДн в информационных системах производится должностным лицом, использовавшим указанные данные. Ответственный за обработку ПДн Фонда контролирует полноту уничтожения указанных данных в информационных системах Фонда.

Если обработка ПДн осуществляется другим лицом, действующим по поручению Фонда, то Фонд обязан обеспечить их уничтожение в соответствии с данным Положением.

Решение об уничтожении ПДн принимается лицом, ответственным за обработку ПДн в Фонде, по представлению руководителя подразделения, ответственного за обработку соответствующих ПДн клиентов, признанных необходимыми к уничтожению. Решение об уничтожении должно быть принято в срок, не превышающий 3 (трих) рабочих дней с даты появления оснований к уничтожению ПДн.

После принятия решения об уничтожении руководитель подразделения, ответственного за обработку ПДн, обязан уведомить об этом ответственного за обработку ПДн Фонда, который назначает комиссию по уничтожению ПДн.

Данная комиссия получает (для данных, хранящихся на материальных носителях) полную информацию обо всех местах хранения соответствующих ПДн. Если хранение осуществлялось на материальном носителе, то руководитель соответствующего подразделения обязан передать комиссии указанный материальный носитель ПДн, подлежащих уничтожению.

Уничтожение ПДн производится руководителем подразделения (для данных, хранящихся в электронной форме) либо комиссией Фонда по уничтожению ПДн (для документов на материальных носителях) в срок

не превышающий 10 (десяти) рабочих дней с даты выявления неустраняемых неправомерных действий с ПДн,

не превышающий 30 (тридцати) календарных дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» или другими федеральными законами.

Не превышающий 30 (тридцати) календарных дней с даты поступления от клиента отзыва согласия на обработку его ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» или другими федеральными законами.

В случае отсутствия возможности уничтожения ПДн в течение срока, указанного выше, Фонд осуществляет уничтожение или обеспечивает уничтожение ПДн в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

В случае если согласно имеющейся у Фонда информации, ПДн клиентов были направлены третьим лицам, руководитель подразделения, осуществляющего обработку соответствующих ПДн, обязан потребовать у указанных третьих лиц в письменной форме уничтожения ПДн с изложением оснований для подобного уничтожения.

При необходимости уничтожения ПДн, являющихся частью материального носителя, содержащего ПДн, не подлежащие уничтожению, комиссией осуществляется вымарывание либо иное физическое удаление данных с условием сохранения данных, не подлежащих уничтожению. Скорректированные подобным образом документ подлежит возврату в соответствующее подразделение.

После уничтожения данных председатель комиссии обязан уведомить о данной операции подразделение, передавшее информацию на уничтожение.

При получении информации об уничтожении либо после самостоятельного уничтожения, подразделение, осуществляющее обработку ПДн, обязано уведомить о факте уничтожения клиента и, в случае если уничтожение произведено по запросу уполномоченного органа по защите персональной информации, указанный орган.

Уведомление должно содержать перечень мер, предпринятых Фондом по результатам обнаружения случаев неправомерной обработки ПДн.

Ответственный за обработку ПДн в Фонде в рамках проверок по направлениям деятельности контролирует своевременность и полноту уничтожения ПДн руководителями подразделений.

27. Права и обязанности клиента Фонда

В целях обеспечения защиты ПДн клиенты Фонда вправе:

получать полную информацию о своих ПДн и способе обработки этих данных (в том числе автоматизированной);

осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, за исключением случаев, предусмотренных Федеральным законом «О персональных данных». Физический доступ клиентов Фонда на территорию Фонда осуществляется в соответствии с внутренними документами Фонда;

требовать внесения необходимых изменений, уничтожения или блокирования соответствующих ПДн, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействие) уполномоченных должностных лиц Фонда.

Субъект ПДн вправе обратиться в Фонд с составленным с соблюдением требования законодательства запросом об обработке ПДн Фондом. Запрос должен быть зарегистрирован и обработан в соответствии с Регламентом реагирования на запросы субъектов ПДн. В данном запросе может быть уточнена следующая информация:

1) подтверждение факта обработки ПДн Фондом;

- 2) правовые основания и цели обработки ПДн;
- 3) цели и применяемые Фондом способы обработки ПДн;
- 4) наименование и место нахождения Фонда, сведения о лицах (за исключением работников Фонда), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Фондом или на основании федерального закона;
- 5) обрабатываемые ПДн, относящиеся к соответствующему Клиенту, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки ПДн, в том числе сроки их хранения;
- 7) порядок осуществления клиентом прав, предусмотренных федеральным законом;
- 8) информация об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Фонда, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные федеральным законодательством.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе если обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма или если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

Сведения, указанные выше, предоставляются клиенту или его представителю оператором при обращении либо при получении запроса клиента или его уполномоченного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность клиента или его уполномоченного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие клиента в отношениях с Фондом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Фондом, подпись клиента или его уполномоченного представителя.

В случае, если сведения, указанные выше, а также обрабатываемые ПДн были предоставлены для ознакомления клиенту по его запросу, клиент вправе обратиться повторно к Фонду или направить ему повторный запрос в целях получения сведений, указанных выше, и ознакомления с такими ПДн не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является клиент.

Клиент вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных выше, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в предыдущем абзаце, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

28. Права и обязанности Фонда в отношении обработки ПДн

Необходимость доступа работников Фонда к ПДн субъектов ПДн, обрабатываемым в Фонде, документально определена в соответствующих должностных инструкциях.

Обработка и защита ПДн в структурных подразделениях Фонда осуществляется в документально определенном порядке, исключая несанкционированный доступ к ПДн.

В Фонде документально определен перечень лиц, осуществляющих обработку ПДн. Лица, осуществляющие такую обработку, проинформированы о факте обработки ими ПДн, об особенностях и правилах осуществления такой обработки, а также об ответственности за нарушение действующего законодательства в области ПДн. Лица, осуществляющие обработку ПДн, ознакомлены под роспись с настоящими требованиями и подписали обязательство о соблюдении конфиденциальности ПДн и соблюдении правил обработки ПДн.

В Фонде документально определен перечень помещений, в которых ведется обработка ПДн, а также перечень лиц, имеющих доступ в помещения, в которых проводится обработка ПДн.

Передача ПДн между структурными подразделениями Фонда осуществляется только между сотрудниками, имеющими доступ к ПДн.

Фонд не вправе заставлять клиентов к предоставлению ПДн, однако вправе требовать этого, если подобные обязательства прямо вытекают из договорных отношений с клиентами или требований нормативных и законодательных актов.

Фонд обязан обеспечивать субъекту ПДн возможность ознакомления в доступной форме с документами и материалами, непосредственно к нему относящимися (если подобный запрет прямо не установлен действующим законодательством) при получении запроса, соответствующего требованиям статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и раздела «Права и обязанности клиентов Фонда» данного Положения.

Если сбор ПДн осуществляется во исполнение требований федерального закона, сотрудники Фонда, осуществляющие сбор ПДн, обязаны разъяснить субъекту ПДн юридические последствия отказа предоставить ПДн.

Фонд обязан сообщать в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение 30 (тридцати) календарных дней с даты получения такого запроса.

29. Уведомление уполномоченного органа по защите прав субъектов ПДн

В случаях, установленных Федеральным законом «О персональных данных», Фонд направляет уведомление в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор).

30. Обеспечение безопасности ПДн

Фонд при обработке ПДн клиентов принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн. Указанные меры, включая их перечень и описание, а также порядок их принятия установлены в Положении об обеспечении безопасности ПДн.

Обеспечение безопасности ПДн в Фонде достигается, в частности:

- 1) определением угроз безопасности ПДн при их обработке в информационных системах ПДн;
- 2) применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- 4) оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;
- 5) учетом машинных носителей ПДн;
- 6) обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
- 7) восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 8) установлением правил доступа к ПДн, обрабатываемым в информационной системе ПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в информационной системе ПДн;
- 9) контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности информационных систем ПДн.

Фонд не должен обеспечивать безопасность и конфиденциальность ПДн клиентов в следующих случаях:

- ПДн обезличены;
- ПДн являются общедоступными или включены в источники общедоступных данных.

31. Ответственность за нарушение требований настоящего Положения

Сотрудники Фонда, обрабатывающие ПДн Клиентов, и лица, которым Фонд поручает обработку ПДн клиентов, несут гражданскую, уголовную, административную и иную предусмотренную законодательством Российской Федерации ответственность за нарушение режима защиты, обработки и порядка использования этих ПДн.

За неисполнение или ненадлежащее исполнение уполномоченными сотрудниками Фонда по его вине возложенных на него обязанностей по соблюдению установленного порядка работы с ПДн Фонд вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

Административная ответственность также предусмотрена в случаях неправомерного отказа уполномоченными лицами Фонда в предоставлении собранных в установленном порядке документов, в случаях несвоевременного предоставления таких документов, либо в случаях предоставления неполной или заведомо ложной информации.

Руководитель подразделения, предоставляющий доступ сотруднику Фонда к обрабатываемым ПДн, несет персональную ответственность за данное разрешение.

Сотрудники Фонда, получающие доступ к обрабатываемым ПДн, несут персональную ответственность за конфиденциальность полученной информации.

ПЕРЕЧЕНЬ
ПДн клиентов обрабатываемых в МКК, НКО
«Фонд поддержки МСП РА»

1.1. Перечень (далее – Перечень) ПДн клиентов, подлежащих защите в Фонде, разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и внутренними документами Фонда.

2. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

2.1. В Фонде сведениями, составляющими персональные данные (далее – ПДн) клиента, является любая информация, относящаяся к прямо или косвенно определенному или определяемому клиенту Фонда (субъекту ПДн) – физическому лицу, в том числе:

2.1.1. ПДн специальной (первой) категории.

2.1.1.1. Сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья клиентов Фонда.

2.1.2. Биометрические ПДн (второй категории).

2.1.2.1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Фондом для установления личности клиента Фонда. К числу таких данных *могут* относиться среди прочего видеозаписи внутренних систем охранного телевидения, данные в устройствах, использующих для идентификации биометрические данные человека, кодеркопии с документов, удостоверяющих личность и имеющих фотографию владельца – клиента Фонда. Обязательным условием отнесения указанных данных к разряду биометрических ПДн является условие их использование Фондом для установления личности человека.

2.1.3. ПДн общей (третьей) категории, за исключением ПДн, относящихся к специальной категории и к обозначенным, общедоступным, биометрическим ПДн.

2.1.3.1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.1.3.2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.

2.1.3.3. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.

2.1.3.4. Номера телефонов (мобильного, рабочего и домашнего), в случае их регистрации на клиента Фонда или по адресу его места жительства (по паспорту).

2.1.3.5. Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения).

2.1.3.6. Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения).

2.1.3.7. Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и ее наименования, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях).

2.1.3.8. Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней.

2.1.3.9. Содержание и реквизиты гражданско-правового договора с клиентом Фонда, в котором он является стороной по договору, выгодоприобретателем, поручителем или залогодателем.

2.1.3.10. Сведения о заработной плате.

2.1.3.11. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет).

2.1.3.12. Сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2НДФЛ супруга(и), данные документов по долгам обязательствам, степень родства, фамилия, имена, отчества и даты рождения других членов семьи, иждивенцев).

2.1.3.13. Сведения об имуществе (имущественном положении):

- автотранспорт (государственные номера и другие данные из свидетельства о регистрации транспортных средств и из паспортов транспортных средств);

- недвижимое имущество (полные адреса размещения объектов недвижимости и его реквизиты);

- банковские вклады (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов);

- кредиты (займы), банковские счета (в том числе спецкартсчета), денежные средства и ценные бумаги, в том числе в доверительном управлении и на доверительном хранении (данные договоров с клиентами, в том числе номера счетов, спецкартсчетов, номера банковских карт, кодовая информация по банковским картам, коды кредитных историй, адреса приобретаемых объектов недвижимости).

2.1.3.14. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования, а также сведения, содержащиеся в справках формы СЗВ-6-1 и СЗВ-6-2.

2.1.3.15. Сведения об идентификационном номере налогоплательщика.

2.1.3.16. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).

2.1.4. Общедоступные ПДн (четвертой категории).

2.1.4.1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.1.4.2. Номера телефонов (мобильного и домашнего), в случае их регистрации на клиента Фонда или по адресу его места жительства (по паспорту).

2.1.4.3. IP-адреса устройств, с которых клиент Фонда осуществляет доступ к информационным системам Фонда.

2.1.4.4. Номер клиента или иной уникальный идентификатор клиента.

2.1.4.5. иные сведения, являющиеся общедоступными или сделанные таковыми с письменного согласия клиента.

Приложение №2 к
ПОЛИТИКЕ обеспечения
безопасности персональных данных
при их обработке в МКК, НКО «Фонд
поддержки малого и среднего
предпринимательства Республики
Алтай»

ПОЛОЖЕНИЕ

**об обработке персональных данных работников
Микрокредитной компании, некоммерческой организации
«Фонд поддержки малого и среднего предпринимательства
Республики Алтай»**

1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников МКК, НКО «Фонд поддержки малого и среднего предпринимательства Республики Алтай» (далее - Фонд) от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, а также Федерального закона «Об информации, информатизации и защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие приказом директора и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

2. Понятие и состав персональных данных

2.1. Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. В состав персональных данных работника входят:

- анкетные и биографические данные;
- наименование структурного подразделения;
- занимаемая должность;
- сведения о текущем должностном окладе;
- паспортные данные;
- биометрические данные;
- адрес прописки;
- ИНН;
- номер страхового свидетельства;
- данные об образовании;
- данные о детях;
- данные о семейном положении;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным проверкам;
- копии отчетов, направляемые в органы статистики.

2.3. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3. Обработка персональных данных

3.1. Под обработкой персональных данных работника понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

3.2.3. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.

3.2.4. Персональные данные следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях предполагаемых источников и способах получения персональных данных, а так же о характере подлежащих

получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

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

3.2.6. Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:

- Заместитель директора Фонда;
- Главный бухгалтер Фонда;
- юрист Фонда;

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

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

3.5. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные 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 работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

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

3.5.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные носители информации.

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

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

3.9. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).

4.1.1. Право доступа к персональным данным сотрудника имеют:

- директор организации;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
- сам работник, носитель данных;
- другие сотрудники организации при выполнении ими своих служебных обязанностей.

4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом директора организации.

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.2.4. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывших супругов (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

5. Защита персональных данных

5.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоупотребленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

5.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

5.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

5.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

5.5. «Внутренняя защита».

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

5.5.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;

- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору, инспектору по кадрам и в исключительных случаях, по письменному разрешению директора, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

5.5.3. Запрет персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается ответственному за обработку персональных данных.

5.6. «Внешняя защита».

5.6.1. Для запрета конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности организации, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов инспектора-делопроизводителя.

5.6.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

5.8. По возможности персональные данные обезличиваются.

5.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. Права и обязанности работника

6.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

6.2. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

6.3. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

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

6.4. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

- своевременно сообщать работодателю об изменении своих персональных данных

6.5. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

6.6. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность — одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и запоту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации — влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собиране или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.