

Приказом № 13

Омаров К.М



об обработке и защите персональных данных клиентов
НКО «Фонд содействия кредитованию субъектов малого и среднего
предпринимательства Республики Дагестан»

1.1. Настоящее положение является локальным правовым актом некоммерческой организация «Фонд содействия кредитованию субъектов малого и среднего предпринимательства Республики Дагестан» (сокращенно Гарантийный фонд РД), являющейся в соответствии с действующим законодательством Российской Федерации Оператором персональных данных.

1.2. Настоящее положение определяет политику Организации в отношении обработки персональных данных клиентов Организации, в том числе устанавливает порядок обработки персональных данных, основные цели, принципы обработки и требования к безопасности персональных данных клиентов Организации.

1.3. Настоящее положение разработано в целях регулирования порядка сбора, систематизации, хранения, передачи и уничтожения персональных данных клиентов на основании полномочий Организации. Обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защита прав неприкосновенности частной жизни, личной, семейной тайны, а так же установления ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.4. Понятия и термины, используемые в настоящем Положении:

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

Персональные данные, разрешенные субъектом (клиентом) персональных данных для распространения - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном законодательством РФ;

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;

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

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

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

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

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

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

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Конфиденциальность персональных данных (конфиденциальность) — строгое соблюдение работником, владеющим доступом к персональным данным, требований не распространять их без получения разрешения субъекта этой информации или его законных представителей.

Клиент/контрагент (субъект персональных данных) — физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Оператор персональных данных (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;

Организация считается Оператором в соответствии с данным Положением.

1.5. Настоящее положение разработано в соответствии с Конституцией Российской Федерации, ФЗ от 27.07.2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных), Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 1 ноября 2012 г. N 1119, и иными нормативными актами в области защиты персональных данных, действующими на территории Российской Федерации, Уставом организации.

1.6. Целями обрабатывания персональных данных являются:

- установление процедуры обработки личных сведений каждого Клиента Организации, чьи данные необходимо обрабатывать;
- защита прав, свобод человека во время выполнения операций с его персональными данными, определение ответственности работников Организации, владеющих доступом к персональным данным, в случае невыполнения ими законодательства по обработке и защите персональных данных.
- реализации прав и законных интересов Организации в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Организации;

1.7. Основным инфраструктурным ресурсом Организации для осуществления операций с персональными данными являются информационные системы, представляющие собой:

- комплексы автоматизированной обработки персональных данных (позволяющих осуществлять операции с персональными данными в виде файлов, доступ к которым

регулируется в соответствии с положениями локальных правовых актов Организации, федеральных, региональных и муниципальных нормативно-правовых актов);

– документацию на бумажных носителях (доступ к которым также осуществляется в соответствии с положениями локальных правовых актов и законодательства РФ).

2. Персональные данные

2.1. К персональным данным клиента относятся:

- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения и др.);
- паспортные данные;
- гражданство;
- адрес регистрации;
- адрес места жительства;
- номер телефона;
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
- сведения об идентификационном номере налогоплательщика;
- семейное, социальное, имущественное положение, образование, профессия, доходы и иная информация, прямо или косвенно относящаяся к личности и месту работы клиента.

2.2. Указанные сведения являются конфиденциальными. Организация как Оператор персональных данных не вправе распространять персональные данные без согласия клиента, если иное не предусмотрено федеральным законом.

2.3. Организация наделена правом создания, сбора, хранения таких данных, также и на электронных носителях, в которых содержатся сведения о Клиенте, касающиеся:

- анкетной (адресной) информации о Клиенте;
- договоров и приложений к ним;
- документов клиента, подтверждающих его личность (в копиях), прочей документации, предоставляемой клиентом, в которых указаны его персональные данные;
- переписки в электронном виде, записи ведения переговоров по телефону.

3. Обработка персональных данных и гарантии их защиты

3.1. В целях обеспечения прав и свобод человека и гражданина организация при обработке персональных данных клиента Организация соблюдает следующие общие требования:

– обработка персональных данных клиента осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов;

– при определении объема и содержания обрабатываемых персональных данных клиента Организация руководствуется Конституцией РФ, Федеральным законом от 27.07.2006г. N 152-ФЗ "О персональных данных" и иными Федеральными законами регулирующих использование персональных данных.

3.2. Обработка персональных данных осуществляется Организацией с согласия клиента на обработку его персональных данных, а также с соблюдением принципов и правил, предусмотренных Законом о персональных данных.

3.3. Клиенты Организации принимают решение о предоставлении его персональных данных и дают согласие в письменной форме на их обработку свободно, своей волей и в своем интересе.

3.4. Согласие клиента на обработку его персональных данных предоставляется в соответствии с требованиями ст. 9 Закона о персональных данных (Приложение 1) и должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а так же порядок его отзыва

3.5. Обработка персональных данных клиентов без согласия допускается в случаях предусмотренных ст. 6 Закона о персональных данных, а именно:

- обработка персональных данных осуществляется на основании действующего законодательства, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а так же определяющего полномочия работодателя;
- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья работника и их обработка необходима для его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия Клиента невозможно;
- обработка персональных данных осуществляется в целях для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- по требованию полномочных государственных органов в случаях, предусмотренных действующим законодательством РФ.

3.6. Согласие на обработку персональных данных может быть отозвано клиентом. В случае отзыва согласия на обработку персональных данных Организация вправе продолжить обработку персональных данных без согласия клиента при наличии оснований, указанных в п. 2 - 11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Закона о персональных данных.

3.7. Согласие клиента на обработку персональных данных, разрешенных для распространения, оформляется отдельно от иных согласий клиента на обработку его персональных данных и предоставляется в соответствии с требованиями ст. 10.1 Закона о персональных данных (Приложение 2)

3.8. Защита персональных данных клиента от неправомерного их использования или утраты обеспечивается организацией за счет ее средств в порядке, установленном Федеральными законами и настоящим Положением.

3.9. Организация при обработке персональных данных принимает необходимые правовые, организационные и технические меры и (или) обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.10. Организация осуществляет внутренний контроль соответствия обработки персональных данных Закону о персональных данных, требованиям к защите персональных данных, настоящему Положению.

3.11. Организация обеспечивает безопасность персональных данных клиента следующими способами:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3.12. Обработке подлежат персональные данные, которые отвечают целям их обработки в соответствии со ст. 5 Закона о персональных данных.

3.13. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.14. Цель обработки персональных данных клиента указывается в каждом отдельном согласии на обработку персональных данных.

3.15. Не подлежат обработке персональные данные о клиенте, касающиеся его расовой, национальной принадлежности, сексуальной ориентации, политических взглядов, религии, философских убеждений, здоровья, а также биометрические персональные данные (фото, видео, отпечатки пальцев).

3.16. Организация обрабатывает в информационных системах с использованием средств автоматизации персональные данные клиента, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных.

3.17. Организация при обработке персональных данных клиента на бумажных носителях в целях обеспечения их защиты:

- назначает должностное лицо (работника), ответственного за обработку персональных данных;
- ограничивает доступ в помещения, в которых хранятся документы, содержащие персональные данные клиентов.

3.18. В целях обеспечения конфиденциальности документы, содержащие персональные данные клиентов на бумажных носителях, оформляются, ведутся и хранятся у ответственного сотрудника.

3.19. Работники, допущенные к персональным данным клиентов, подписывают обязательство о неразглашении персональных данных. В противном случае до обработки персональных данных клиентов не допускаются.

3.20. Персональные данные клиентов в электронном виде хранятся в локальной компьютерной сети организации, в электронных папках и файлах в персональных компьютерах руководителя организации и работников, допущенных к обработке персональных данных клиентов.

3.21. Обработка персональных данных начинается с получения достоверных персональных данных клиента. Доступ к этим сведениям имеют только работники организации, которым предоставлено такое право после подписания Соглашения о неразглашении персональных данных клиента.

3.22. Доступ к персональным данным клиентов в Организации имеют:

- руководитель организации;
- сотрудники, выполняющие бухгалтерские операции;

- сотрудники отдела по работе с заемщиками;
- сотрудники юридического отдела;
- сотрудники информационного подразделения (ИТ);
- клиент – субъект персональных данных.

3.23. Общая защита персональных данных клиента возложена на руководителя организации.

4. Передача персональных данных

4.1. При передаче персональных данных клиента организация соблюдает следующие требования:

- не сообщать персональные данные клиента третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью клиента, а также в других случаях, установленных федеральными законами;
- не сообщать персональные данные клиента в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные клиента, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные клиента, обязаны соблюдать режим секретности (конфиденциальности);
- разрешать доступ к персональным данным клиентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные клиентов, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья клиентов.

4.2. Все сведения о передаче персональных данных клиента учитываются для контроля правомерности использования данной информации лицами, ее получившими.

4.3. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия клиента на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

4.4. Передача информации, содержащей сведения о персональных данных клиента, по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

4.5. Согласие на обработку персональных данных, разрешенных для распространения, оформляется отдельно от иных согласий клиента на обработку его персональных данных. Организация обеспечивает клиенту возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных им для распространения.

4.6. В согласии на обработку персональных данных, разрешенных клиентом для распространения, он вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных организацией неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

4.7. Передача (распространение, предоставление, доступ) персональных данных, разрешенных клиентом для распространения, должна быть прекращена в любое время по его требованию. Указанные в данном требовании персональные данные могут обрабатываться только организацией.

5. Порядок уничтожения персональных данных

5.1. В случае выявления неправомерной обработки персональных данных при обращении клиента организация осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому клиенту, с момента такого обращения на период проверки.

5.2. В случае выявления неточных персональных данных при обращении клиента организация осуществляет блокирование персональных данных, относящихся к этому клиенту, с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы клиента, или третьих лиц.

5.3. В случае подтверждения факта неточности персональных данных организация на основании сведений, представленных клиентом, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

5.4. В случае выявления неправомерной обработки персональных данных, осуществляемой организацией, организация в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.

5.5. В случае если обеспечить правомерность обработки персональных данных невозможно, организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

5.6. Об устранении допущенных нарушений или об уничтожении персональных данных организация уведомляет клиента.

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

- в течение 24 (двадцати четырех) часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав клиента, и предполагаемом вреде, нанесенном правам клиента, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном организацией на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- в течение 72 (семидесяти двух) часов о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5.8. В случае достижения цели обработки персональных данных организация прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

5.9. В случае отзыва клиентом согласия на обработку его персональных данных организация прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

5.10. В случае обращения клиента в организацию с требованием о прекращении обработки персональных данных организация в срок, не превышающий 10 (десяти) рабочих дней с даты получения им соответствующего требования, прекращает их обработку, за исключением случаев, предусмотренных Законом о персональных данных.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления организацией в адрес клиента мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

5.11. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 5.4-5.10 настоящего положения, организация осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных

данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.12. После истечения срока нормативного хранения документов, содержащих персональные данные клиента, или при наступлении иных законных оснований документы подлежат уничтожению.

5.13. Организация для этих целей создает экспертную комиссию и проводит экспертизу ценности документов.

5.14. По результатам экспертизы документы, содержащие персональные данные клиента подлежащие уничтожению:

- на бумажном носителе - уничтожаются путем измельчения в шредере;
- в электронном виде - стираются с информационных носителей либо физически уничтожаются сами носители, на которых хранится информация.

6. Права клиентов в целях обеспечения защиты персональных данных

6.1. В целях обеспечения защиты персональных данных, хранящихся в организации, клиенты имеют право на:

— полную информацию об их персональных данных и обработке этих данных, в том числе содержащую:

- подтверждение факта обработки персональных данных организацией;
- правовые основания и цели обработки персональных данных;
- цели и применяемые организацией способы обработки персональных данных;
- сроки обработки персональных данных, в том числе сроки их хранения;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- информацию о способах исполнения организацией обязанностей, установленных статьей 18.1 Закона о персональных данных;

— свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные клиента, за исключением случаев, предусмотренных федеральным законом;

— определение своих представителей для защиты своих персональных данных;

— требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Закона о персональных данных. При отказе организации исключить или исправить персональные данные клиента он имеет право заявить в письменной форме организации о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера клиент имеет право дополнить заявлением, выражающим его собственную точку зрения;

— требование об извещении организацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные клиента, обо всех произведенных в них исключениях, исправлениях или дополнениях;

— обжалование в суд любых неправомерных действий или бездействия организации при обработке и защите персональных данных.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных клиентов организации, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном федеральными законами РФ, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7.2. Моральный вред, причиненный клиенту вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральным

законодательством, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных клиентом убытков.

8. Заключительные положения

8.1. Организация обеспечивает неограниченный доступ клиентов к настоящему документу.

8.2. Настоящее положение является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным клиента, и доводится до их сведения персонально под роспись.

8.3. Настоящее Положение вступает в силу с даты его утверждения уполномоченным органом управления Организации, вводится в действие приказом руководителя организации и действует бессрочно до замены новым локальным правовым актом аналогичного назначения.

8.4. Настоящее Положение может быть дополнено и изменено решением уполномоченного органа управления.