



Утверждено  
приказом Генерального директора  
№ 4/2017 от 01 января 2017 г.



Назаров Л.Д.

# **ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ**

*(в редакции от 01 января 2017 г.)*



## 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. Термины, используемые в настоящем Положении с заглавной буквы, значение которых не раскрыто в настоящей статье, имеют значение, присвоенное им в Правилах предоставления Микрозаймов, Правилах корпоративной информационной системы Mili.ru.
2. **персональные данные (ПДн)** - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому или юридическому лицу (субъекту персональных данных);
3. **оператор** - Общество с ограниченной ответственностью Микрофинансовая организация «МИЛИ» (ОГРН: 1117746872033; адрес: 125009, г. Москва, ул. Тверская, д. 9, стр. 7) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
4. **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;
5. **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
6. **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
7. **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
8. **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
9. **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;
10. **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
11. **информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
12. **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

## 2. ОБЩИЕ ПОЛОЖЕНИЯ



2.1. Настоящие Положение (далее - Положение) об обработке персональных данных клиентов ООО Микрофинансовая организация «МИЛИ» разработаны в соответствии с:

2.1.1. Федеральный закон от 12.12.2005 г. №160 «О ратификации конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

2.1.2. Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных».

2.1.3. Постановление Правительства Российской Федерации от 17.11.2007 г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

2.1.4. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.1.5. Постановление Правительства Российской Федерации от 06.07.2008 г. №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

2.1.6. Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г. №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

2.1.7. Приказ Федеральной службы по техническому и экспортному контролю №58 от 5.02.2010 г. «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

2.1.8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

2.1.9. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.

2.1.10. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/5-144.

2.1.11. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при обработке в информационных системах персональных данных. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6-622.

2.2. 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.



2.3. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

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

2.5. 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 закрепления наработанной Оператором практики операций с ПДн.

### **3. ОБРАБОТКА И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ**

3.1. Обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме Электронного документа, подписанного Электронной подписью.

3.2. Обработка ПДн субъекта ПДн включает в себя сбор; запись; систематизацию; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; обезличивание; блокирование; удаление; уничтожение; передачу (распространение, предоставление, доступ) и (или) поручение их обработки в пределах территории РФ и на территорию любых иностранных государств (трансграничную передачу), в частности, США, Ирландии, иных иностранных государств как обеспечивающих, так и не обеспечивающих адекватную защиту прав субъектов персональных данных, а также передачу иным третьим лицам, которым может потребоваться передача ПДн в соответствии с целями их обработки.

То есть, совокупность действий, которые предусмотрены и необходимы для предоставления финансовых услуг, контроля за оплатой и выполнением договорных обязательств.

3.3. Персональные данные субъекта ПДн относятся к категории конфиденциальной информации.

3.4. В целях обеспечения прав и свобод человека и гражданина Оператор и его представители при обработке ПДн субъектов ПДн соблюдают следующие общие требования:

3.4.1. Обработка ПДн субъектов ПДн осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия выполнения договорных обязательств в соответствии с законодательством Российской Федерации.

3.4.2. При определении объема и содержания, обрабатываемых ПДн субъектов ПДн Оператор руководствуется законодательством Российской Федерации.

3.4.3. Все ПДн субъект ПДн предоставляет Оператору самостоятельно в форме электронного документа в момент подачи Заявления о предоставлении микрозайма.

3.4.4. Обработка ПДн, полученных от третьих лиц, возможна только при уведомлении субъекта ПДн об этом заранее.



#### **4. СУБЪЕКТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

4.1. Оператором осуществляется обработка персональных данных следующих категорий субъектов персональных данных:

- Клиенты ООО Микрофинансовая организация «МИЛИ».

#### **5. ЦЕЛЬ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

5.1. Целью обработки ПДн является обеспечение защиты прав и свобод клиента при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определяет и устанавливает ответственность должностных лиц, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн, оценка платежеспособности клиента, а также реализация положений нормативных правовых актов и иных документов по защите ПДн.

5.2. Основными целями обеспечения безопасности персональных данных являются:

- предотвращение нарушений прав субъекта ПДн на сохранение конфиденциальности информации, обрабатываемой в ИСПДн Оператора;
- предотвращение искажения или несанкционированной модификации информации, содержащей персональные данные, обрабатываемой в ИСПДн Оператора;
- предотвращение несанкционированных действий в отношении информации, содержащей персональные данные.

5.3. Настоящее Положение является обязательным для исполнения всеми сотрудниками Оператора и распространяются на:

- автоматизированные системы Оператора;
- средства телекоммуникаций;
- информационные ресурсы и носители информации;
- помещения.

#### **6. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

6.1. Обработка персональных данных осуществляется на основе принципов:

6.1.1. законности целей и способов обработки ПДн и добросовестности;

6.1.2. соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Оператора;

6.1.3. соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;

6.1.4. достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;

6.1.5. недопустимости объединения, созданных для несовместимых между собой целей баз данных информационных систем ПДн.

#### **7. СПОСОБЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

7.1. Оператор может осуществлять обработку ПДн с использованием средств автоматизации, а также без использования таких средств.

#### **8. ПЕРЕЧЕНЬ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

8.1. Сведениями, составляющими ПДн клиента, является любая информация, относящаяся к прямо или косвенно определенному, или определяемому клиенту Оператора (субъекту ПДн) - физическому лицу, в том числе:



8.1.1. **ПДн специальной категории** - сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья клиентов.

8.1.2. **Биометрические ПДн** - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Оператором для установления личности клиента. К числу таких данных могут относиться среди прочего аудио и видеозаписи, ксерокопии с документов, удостоверяющих личность и имеющих фотографию владельца – клиента Оператора. Обязательным условием отнесения указанных данных к разряду биометрических ПДн является условие их использование Оператором для установления личности человека.

8.1.3. **ПДн общей категории**, за исключением ПДн, относящихся к специальной категории и к обезличенным, общедоступным, биометрическим ПДн:

- Фамилия, имя, отчество;
- дата и место рождения;
- Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство;
- Адрес места жительства (по паспорту и фактический);
- Номера телефонов (мобильного и домашнего);
- Сведения об образовании;
- Сведения о квалификации;
- Сведения о трудовой деятельности (данные о трудовой занятости на текущее время);
- Сведения о заработной плате.
- Сведения о семейном положении;
- Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.
- Сведения об идентификационном номере налогоплательщика.

8.1.4. **Общедоступные ПДн:**

- Фамилия, имя, отчество;
- Дата и место рождения;
- Номера телефонов (мобильного и домашнего);
- IP-адреса устройств, с которых клиент осуществляет доступ к Корпоративно-информационной системе Оператора;
- Номер клиента или иной уникальный идентификатор клиента;
- Иные сведения, являющиеся общедоступными или сделанные таковыми с письменного согласия клиента.

## **9. ОРГАНИЗАЦИЯ РАБОТЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

9.1. Организация работ по обеспечению безопасности ПДн осуществляется Генеральным директором.

9.2. Для разработки и осуществления мероприятий по обеспечению безопасности ПДн при их обработке в информационных системах Оператора, приказом Генерального директора назначаться, ответственное лицо за обеспечение безопасности ПДн.

9.3. Разработка и осуществление мероприятий по обеспечению безопасности ПДн может осуществляться также сторонними организациями на договорной основе, имеющими лицензии на право проведения соответствующих работ.





9.4. Приказом Генерального директора Оператора назначаются ответственные лица по работе с ПДн.

9.5. Лица, доступ которых к ПДн, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании утвержденного списка.

## **10. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ**

10.1. Система защиты персональных данных:

10.1.1. Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

10.1.2. При обработке ПДн в информационных системах Оператора должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности ПДн.

10.2. Перечень мероприятий по обеспечению безопасности персональных данных

10.2.1. Мероприятия по обеспечению безопасности ПДн при их обработке в информационных системах включают в себя:

- определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;
- учет лиц, допущенных к работе с ПДн в информационной системе;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;



- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
  - описание системы защиты персональных данных.
- 10.3. Классификация информационных систем персональных данных.
- 10.3.1. Информационные системы ПДн Оператора подлежат обязательной классификации.
- 10.3.2. Для проведения классификации информационных систем персональных данных (ИСПДн) Оператора назначается комиссия.
- 10.3.3. Результаты классификации оформляются соответствующим актом.
- 10.4. Помещения, в которых ведется обработка персональных данных.
- 10.4.1. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

## **11. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

11.1. Сроки обработки ПДн определяются в соответствии со ст. 21 Федерального закона «О персональных данных». Обработка ПДн начинается с момента поступления персональных данных в ИСПДн и прекращается:

- в случае выявления неправомерных действий с ПДн в срок, не превышающий трех рабочих дней с даты такого выявления, Оператор устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, уничтожает ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Оператор уведомляет субъекта ПДн, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, Оператор уведомляет также указанный орган;
- в случае достижения цели обработки ПДн Оператор незамедлительно прекращает обработку ПДн и уничтожает соответствующие ПДн в срок, не превышающий трех рабочих дней с даты достижения цели обработки ПДн, и уведомляет об этом субъекта ПДн, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, Оператор уведомляет также указанный орган;
- в случае отзыва субъектом ПДн согласия на обработку своих ПДн Оператор прекращает обработку ПДн и уничтожает ПДн в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении ПДн Оператор уведомляет субъекта ПДн.
- в случае прекращения деятельности Оператора.

## **12. ХРАНЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**





12.1. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

12.2. Для уничтожения персональных данных, приказом Генерального директора назначается комиссия по уничтожению ПДн.

12.3. Уничтожение ПДн оформляется актом.

12.4. Места хранения материальных носителей ПДн утверждаются приказом Генерального директора.

### **13. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ПРОДВИЖЕНИЯ ТОВАРОВ, РАБОТ, УСЛУГ**

13.1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только при условии предварительного согласия субъекта персональных данных.

### **14. ПОРУЧЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬЕМУ ЛИЦУ**

14.1. Оператор вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, на основании заключаемого с этим лицом договора.

14.2. Лицо, осуществляющее обработку ПДн по поручению Оператора, соблюдает принципы и правила обработки ПДн, предусмотренные Федеральным законом «О персональных данных».

Контроль выполнения настоящего требования осуществляет Генеральный директор Оператора.

14.3. Лицо, осуществляющее обработку ПДн по поручению оператора, не обязано получать согласие субъекта ПДн на обработку его ПДн.

### **15. ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ**

15.1. Оператор может осуществлять трансграничную передачу ПДн.

15.2. Для осуществления трансграничной передачи ПДн необходимо получить согласие субъекта ПДн в письменной форме.

15.3. Трансграничная передача ПДн может осуществляться без согласия субъекта ПДн в случаях:

15.3.1. исполнения договора, стороной которого является субъект ПДн;

15.3.2. защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта ПДн.

### **16. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕГО ПОЛОЖЕНИЯ.**

16.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном законодательством РФ.

### **17. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

17.1. Настоящее Положение вступает в силу с момента его утверждения приказом Генерального директора Оператора.



17.2. Настоящее Положение доводится до сведения всех Работников Оператора, персонально под роспись.