

УТВЕРЖДЕНО
Приказом генерального директора ООО
МКК «Генезис групп»
№ 07/11/19-4 от 07.11.2019 г.

**ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ
ПЕРСОНАЛЬНЫХ ДАННЫХ
ООО МКК «Генезис групп»**

**Москва
2019 год**

1. Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон о ПДн) и является основополагающим внутренним регулятивным документом Общества с ограниченной ответственностью Микрокредитной компании «Генезис групп» (далее - Общество), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее — ПДн) работников, клиентов, контрагентов Общества, оператором которых является Общество.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на защиту прав и свобод человека и гражданина при обработке его ПДн в Обществе, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Политика действует в отношении всех ПДн, которые Общество может получить от субъектов ПДн - работников Общества в связи с оформлением трудовых отношений, клиентов и контрагентов Общества в связи с осуществлением Обществом уставной деятельности.

1.4. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Обществом как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.5. Если в отношениях с Обществом участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Общество становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние регулятивные документы Общества распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних регулятивных документах прямо не упоминаются, но фактически участвуют в правоотношениях с Обществом.

1.6. В целях обеспечения неограниченного доступа к настоящей Политике документ размещается на информационных стендах в офисах и на сайте Общества.

2. Принципы обеспечения безопасности персональных данных

2.1. Основной задачей обеспечения безопасности ПДн при их обработке в Обществе является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

2.2. Для обеспечения безопасности ПДн Общество руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн в Обществе осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Общества (далее - ИС) и других имеющихся в Обществе систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

6) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Обществе с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

7) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8) минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

9) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Общества предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Общества;

10) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются;

11) целеориентированность обработки ПДн: обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн, объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой, получение избыточных ПДн по отношению к заявленным целям их обработки;

12) срочность обработки ПДн: 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.

3. Основания обработки и состав персональных данных

3.1. Обработка ПДн в Обществе осуществляется в связи с выполнением законодательно возложенных на Общество функций, определяемых такими документами как:

1) Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";

2) "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ;

3) "Налоговый кодекс Российской Федерации (часть первая)" от 31.07.1998 N 146-ФЗ и "Налоговый кодекс Российской Федерации (часть вторая)" от 05.08.2000 N 117-ФЗ;

4) Федеральный закон от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма";

5) Федеральный закон от 01.04.1996 N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования";

6) Федеральный закон от 02.07.2010 N 151 -ФЗ "О микрофинансовой деятельности и микрофинансовых организациях";

7) "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ, "Гражданский кодекс Российской Федерации (часть вторая)" от 26.01.1996 N 14-ФЗ, "Гражданский кодекс Российской Федерации (часть третья)" от 26.11.2001 N 146-ФЗ, "Гражданский кодекс Российской Федерации (часть четвертая)" от 18.12.2006 N 230-ФЗ;

8) Федеральный закон от 30.12.2004 N 218-ФЗ "О кредитных историях";

9) Федеральный закон от 08.02.1998 N 14-ФЗ "Об обществах с ограниченной ответственностью"¹;

10) Федеральный закон от 21.12.2013 N 353-ФЗ "О потребительском кредите (займе)";

11) иными нормативными правовыми актами Российской Федерации.

3.2. В связи с реализацией трудовых отношений Общество обрабатывает следующие категории ПДн:

- фамилия, имя, отчество;

- образование;

- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные или данные иного документа, удостоверяющего личность;
- сведения о воинском учете;
- ИНН;
- СНИЛС;
- налоговый статус (резидент/нерезидент);
- сведения о заработной плате;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- адрес места жительства;
- личный телефон, адрес электронной почты;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание (условия) трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- иную, не указанную выше информацию, содержащуюся в личных делах и трудовых книжках сотрудников;
- информацию, содержащуюся в приказах по личному составу и по основной деятельности, затрагивающих субъекта ПДн;
- информацию, содержащуюся в страховом свидетельстве обязательного пенсионного страхования, свидетельстве о постановке на учет в налоговом органе субъекта ПДн по месту жительства, страховом медицинском полисе обязательного медицинского страхования граждан, медицинском заключении установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на работу в Общество, листке нетрудоспособности;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- иные данные, представленные субъектом ПДн.

В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых Общество выступает в качестве работодателя, обрабатываются ПДн лиц, претендующих на трудоустройство в Общество, работников Общества (далее - Работники) и бывших Работников.

3.3. В связи с реализацией своих прав и обязанностей как юридического лица, Обществом обрабатываются ПДн физических лиц, являющихся контрагентами (возможными контрагентами) Общества по гражданско-правовым договорам, ПДн руководителей, членов коллегиальных исполнительных органов и представителей юридических лиц, ПДн иных лиц, ПДн которые могут использоваться для осуществления пропускного режима в занимаемых Обществом помещениях, а также граждан, письменно обращающихся в Общество по вопросам его деятельности. В целях осуществления уставной деятельности Общество обрабатывает следующие категории ПДн:

- фамилия, имя, отчество;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- место работы субъекта или место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- паспортные данные;
- телефон, адрес электронной почты;
- сведения о заработной плате, доходах;
- занимаемая должность;
- специальность;
- ИНН;
- СНИЛС;

- налоговый статус (резидент/нерезидент);
- адрес места жительства;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- иные данные, представленные субъектом ПДн.

3.4. ПДн получают и обрабатываются Обществом на основании федеральных законов и иных нормативных правовых актов Российской Федерации, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.

3.5. В целях исполнения возложенных на Общество функций Общество в установленном порядке вправе поручить обработку ПДн третьим лицам.

В договоры с лицами, которым Общество поручает обработку ПДн, включаются условия, обязывающие таких лиц соблюдать предусмотренные законодательством требования к обработке и защите ПДн.

3.6. Общество предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

3.7. В Обществе не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Обществе, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Обществом ПДн уничтожаются или обезличиваются.

3.8. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Общество принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

4. Цели сбора и обработки персональных данных

4.1. Общество осуществляет обработку персональных данных в следующих целях:

- осуществление предпринимательской деятельности, предусмотренной уставом Общества, а именно, предоставление потребительских займов в порядке, установленном Федеральным законом «О потребительском кредите (займе)»;
- заключение и исполнение гражданско-правовых договоров с физическими, юридическими лицами, индивидуальными предпринимателями и иными лицами, в связи с осуществлением хозяйственной деятельности Общества;
- оформление трудовых отношений; исполнение обязательств по трудовым и гражданско- правовым договорам; ведение кадрового делопроизводства; содействие работникам в обучении и продвижении по службе; исполнение требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение; осуществление воинского учета;
- выполнение иных требований законодательства.

4.2. С согласия субъекта персональных данных, Общество может использовать персональные данные клиентов и контрагентов в следующих целях:

- для связи с клиентами и контрагентами в случае необходимости, в том числе для направления уведомлений, информации и запросов, связанных с оказанием услуг, а также обработки заявлений, запросов и заявок клиентов;
- для улучшения качества услуг, оказываемых Обществом;
- для продвижения услуг на рынке путем осуществления прямых контактов с клиентами и контрагентами;

- для проведения статистических и иных исследований на основе обезличенных персональных данных.

5, Реализуемые меры по защите персональных данных

5.1. Общество принимает организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Законом о ПДн и принятыми в соответствии с ним нормативными правовыми актами, в том числе:

- Постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных;

- Приказом ФСТЭК России от 18 февраля 2013 г. N 21 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах Пдн";

- Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

- постановления Правительства Российской Федерации РФ 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".

5.2. Обработка ПДн субъекта персональных данных осуществляется Обществом с согласия субъектов ПДн, за исключением случаев, перечисленных в п. 2. ст. 6 Закона о ПДн. Письменное согласие составляется в виде отдельного документа или включается в состав иных документов, подписываемых субъектом персональных данных.

5.3. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше чем этого требуют цели обработки ПДн, если срок хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

5.4. Обществом осуществляется ознакомление работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн, в том числе требованиями к защите ПДн, Политикой и иными внутренними регулятивными документами по вопросам обработки ПДн, и (или) обучение указанных работников по вопросам обработки и защиты ПДн.

5.5. При обработке ПДн с использованием средств автоматизации Общества, в частности, применяются следующие меры:

1) назначается Ответственный за обработку ПДн;

2) утверждаются (издаются) внутренние регулятивные документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

3) осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн Закону о ПДн и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике и внутренним регулятивным документам Общества;

4) проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона о ПДн, определяется соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение исполнения обязанностей, предусмотренных Законом о ПДн.

5.6. Обеспечение безопасности ПДн в организации при их обработке в информационных системах ПДн (далее- ИСПДн) достигается в Обществе, в частности, путем:

1) назначения Ответственного за обеспечение безопасности ПДн в ИСПДн;

2) определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

3) определения в установленном порядке состава и содержания мер по обеспечению

безопасности ПДн, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности Обществом могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в ходе разработки средств защиты ПДн (далее- СЗПДн) проводится обоснование применения компенсирующих мер для обеспечения безопасности ПДн;

4) применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз.

В Обществе, в том числе, осуществляются:

оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

обеспечение сохранности машинных носителей ПДн;

обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;

резервирование, восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установление правил доступа к обрабатываемым ПДн, а также обеспечение регистрации и учета действий, совершаемых с ПДн;

организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

контроль за принимаемыми мерами по обеспечению безопасности ПДн, уровня защищенности ИСПДн.

5.7. Обеспечение защиты ПДн в Обществе при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

1) обособления ПДн от иной информации;

2) недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;

3) использования отдельных материальных носителей для обработки каждой категории ПДн;

4) принятия мер по обеспечению отдельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн;

5) соблюдения требований:

к отдельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;

уточнению ПДн;

уничтожению или обезличиванию части ПДн;

использованию типовых форм документов, характер информации в которых предполагается или допускается включение в них ПДн;

ведению журналов, содержащих ПДн;

хранению ПДн, в том числе к обеспечению отдельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

6. Передача персональных данных

6.1. Общество не представляет и не раскрывает сведения, содержащие ПДн данные работников, клиентов и контрагентов третьей стороне без письменного согласия субъекта ПДн, за исключением случаев, установленных федеральными законами.

6.2. По мотивированному запросу исключительно для выполнения возложенных законодательством функций и полномочий данные субъекта ПДн без его согласия могут быть

направлены:

- в судебные органы в связи с осуществлением правосудия;
- в органы государственной безопасности;
- в органы прокуратуры;
- в органы полиции;
- в следственные органы;
- в иные органы и организации в случаях, установленных нормативными правовыми актами,

обязательными для исполнения.

6.3. Работники Общества, осуществляющие обработку ПДн, не передают сведения, содержащие ПДн, по телефону или факсу.

7. Сроки обработки и хранения персональных данных

7.1. Период обработки и хранения ПДн определяется в соответствии с законом о ПДн.

7.2. Обработка ПДн начинается с момента поступления ПДн в Общество и прекращается в следующих случаях:

- в случае выявления неправомерной обработки ПДн в срок, не превышающий трех рабочих дней с даты такого выявления. В случае, если обеспечить правомерность обработки ПДн невозможно, Общество в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязано уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Общество уведомляет субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также в указанный орган.

- в случае достижения цели обработки ПДн. В срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, иным соглашением между Обществом и субъектом персональных данных либо если Общество не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных действующим законодательством, Общество прекращает обработку ПДн или обеспечивает ее прекращение и уничтожение.

в случае отзыва субъектом ПДн согласия на обработку его ПДн Общество прекращает их обработку или обеспечивает прекращение такой обработки и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожает ПДн или обеспечивает их уничтожение в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, иным соглашением между Обществом и субъектом ПДн либо если Общество не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных действующим законодательством. В случае отзыва субъектом ПДн согласия на обработку его ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи Общество прекращает обработку его ПДн немедленно.

7.3. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если иной срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

7.4. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством.

7.5. В случае получения согласия клиента (или контрагента) на обработку ПДн в целях продвижения услуг Общества на рынке путем осуществления прямых контактов с помощью средств связи, данные клиента (или контрагента) хранятся бессрочно (до отзыва субъектом ПДн согласия на обработку его ПДн).

8. Права субъектов персональных данных

Субъект ПДн вправе:

- 8.1. получать информацию, касающуюся обработки его ПДн, включая сроки их обработки и хранения;
- 8.2. требовать от Общества уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- 8.3. защищать свои права и законные интересы, обжаловать действия или бездействия Общества.

В целях реализации прав, предусмотренных п. 8.1.-8.2. Политики, субъект ПДн может обратиться с запросом в Общество в порядке, определенном ч. 3 ст. 14 Закона о ПДн.

В случае, если субъект ПДн считает, что Общество осуществляет обработку его ПДн с нарушением требований Закона о ПДн или иным образом нарушает его права и свободы, субъект вправе обжаловать действие или бездействие Общества в порядке, предусмотренном действующим законодательством РФ.

9. Конфиденциальность персональных данных.

9.1. Информация, относящаяся к ПДн, ставшая известной в связи с реализацией трудовых отношений, оказанием услуг клиентам Общества, взаимодействия с контрагентами является конфиденциальной информацией и охраняется законом.

9.2. Лица, получившие доступ к обрабатываемым Обществом ПДн, предупреждаются, а в случае нарушения привлекаются к дисциплинарной, административной, гражданско- правовой или уголовной ответственности за нарушения требований законодательства РФ в области обработки и защиты ПДн .

9.3. Общество обязуется не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законом и настоящей Политики.

9.4. Внутренний контроль за соблюдением положений Политики осуществляют лица, ответственные за обработку и защиту информации.

10. Заключительные положения

10.1. Настоящая Политика вступает в силу с момента утверждения и действует до ее отмены.

10.2. Все изменения и дополнения, вносимые в настоящую Политику, утверждаются приказом генерального директора Общества.

10.3. Текст настоящей Политики с изменениями и дополнениями (при наличии) размещается в офисе Общества и в информационно-телекоммуникационной сети «Интернет» на официальном сайте Общества www.kiva.ru.