УТВЕРЖДЕНО

Приказом Генерального директора
№ 1-ПД от «19» октября 2017 года

_____ / Оплачко В.А /

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ, КЛИЕНТОВ И КОНТРАГЕНТОВ ООО МКК «ЦЕНТРАЛЬНЫЙ ЗАЛОГОВЫЙ ДОМ»

г. Кемерово
2017 год

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о защите персональных данных работников, клиентов и контрагентов ООО МКК «ЦЕНТРАЛЬНЫЙ ЗАЛОГОВЫЙ ДОМ» является локальным нормативным актом Общества с ограниченной ответственностью Микрокредитная компания «ЦЕНТРАЛЬНЫЙ ЗАЛОГОВЫЙ ДОМ», устанавливающим порядок получения, обработки, хранения, передачи и защиты персональных данных в Обществе.

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Главой 14 Трудового кодекса Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» иными нормативными правовыми актами, регулирующими отношения, связанные с обработкой и защитой персональных данных.

1.3. В настоящем Положении используются следующие термины и определения:

Оператор – ООО МКК «ЦЕНТРАЛЬНЫЙ ЗАЛОГОВЫЙ ДОМ», вступившее в договорные отношения с работником, клиентом или контрагентом, организующее и осуществляющее в связи с этим обработку персональных данных.

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

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

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

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

Субъект персональных данных – работник, клиент, контрагент.

Защита персональных данных – комплекс мер, принимаемых Обществом для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

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

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

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

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

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

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

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

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные - информация, необходимая в целях исполнения Обществом обязательств, возникших из трудовых отношений с работниками, из гражданско-правовых отношений с клиентами и контрагентами. Под информацией понимаются сведения о фактах, событиях и обстоятельствах жизни субъекта персональных данных, позволяющие идентифицировать его личность.

2.2. В состав персональных данных работника входят:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес регистрации по месту жительства (почтовый адрес);
- адрес фактического проживания (почтовый адрес фактического проживания);
- семейное положение;
- паспортные данные;
- социальное положение;
- адрес электронной почты, телефон;
- данные свидетельства о заключении брака;
- данные свидетельства о расторжении брака;
- данные свидетельства о рождении детей;
- сведения о стаже работы и о местах работы (город, название организации, должность, сроки работы);
- сведения о наградах (поощрениях), почетных званиях;
- данные страхового свидетельства государственного пенсионного страхования (СНИЛС);
- данные свидетельства о постановке на учет в налоговом органе физического лица (ИНН);
- данные полиса медицинского страхования;
- сведения об образовании, повышении квалификации, профессиональной переподготовки и местах обучения (город, образовательное учреждение, сроки обучения, специальность, квалификация, профессия);
- сведения о наличии льгот и гарантий, предоставляемых в соответствии с действующим законодательством;
- сведения о доходах;
- данные документов воинского учета – для военнообязанных и лиц, подлежащих призыву на воинскую службу;
- сведения медицинского характера.

2.3. В состав персональных данных клиентов входят:

- фамилия, имя, отчество;

- год, месяц, дата и место рождения;
- адрес;
- паспортные данные;
- данные страхового свидетельства государственного пенсионного страхования (СНИЛС);
- данные свидетельства о постановке на учет в налоговом органе физического лица (ИНН);
- образование;
- место работы или учебы;
- занимаемая должность;
- сведения о трудовом стаже;
- сведения о доходах;
- семейное положение;
- телефон;
- адрес электронной почты.

2.4. В состав персональных данных контрагентов входят:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- паспортные данные;
- данные страхового свидетельства государственного пенсионного страхования (СНИЛС);
- данные свидетельства о постановке на учет в налоговом органе физического лица (ИНН);
- адрес электронной почты;
- телефон.

3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

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

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

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

3.1.3. Получение Обществом персональных данных может осуществляться как путем представления их самим субъектом персональных данных, так и путем получения их из иных источников. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Общество должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

3.1.4. Общество не имеет права получать и обрабатывать персональные данные работника, клиента, контрагента о его политических, религиозных и иных убеждениях, о частной жизни. В необходимых случаях данные о частной жизни работника или клиента (информация о семейных, бытовых, личных отношениях) могут быть получены и обработаны Обществом только с его письменного согласия.

3.1.5. Общество не имеет право получать и обрабатывать персональные данные работника, клиента, контрагента об их членстве в общественных объединениях или их профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

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

3.3. 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 действующим законодательством Российской Федерации.

3.4. При принятии решений, затрагивающих интересы работника, клиента или контрагента, Общество не имеет права основываться на персональных данных работника, клиента или контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.

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

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

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

3.7. Передача персональных данных возможна только с согласия работника, клиента, контрагента или в случаях, прямо предусмотренных законодательством Российской Федерации.

3.7.1. При передаче персональных данных Общество должно соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия работника, клиента, контрагента за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, клиента, контрагента, а также в случаях, установленных законодательством Российской Федерации;
- предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они получены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

- 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 Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.8. Все меры конфиденциальности при обработке персональных данных распространяются как на бумажные, так и на электронные носители информации.

3.9. Не допускается отвечать на вопросы, связанные с предоставлением персональных данных по телефону или факсу.

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

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

3.12. Обработка персональных данных начинается с момента поступления персональных данных в Общество и прекращается:

- в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления;
- в случае достижения цели обработки персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;
- в случае прекращения деятельности Общества.

3.13. Общество вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта. Лицо, осуществляющее обработку персональных данных по поручению Общества, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В поручении Общества должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

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

3.15. В случае, если Общество поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Общество. Лицо, осуществляющее обработку персональных данных по поручению Общества, несет ответственность перед Обществом.

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1. К обработке, передаче и хранению персональных данных могут иметь доступ:
- Руководитель Общества;
- Руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);
- другие работники Общества при выполнении ими своих должностных обязанностей.

4.2. Перечень должностей, на которых работники имеют доступ к персональным данным работников, клиентов и контрагентов, и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение правил обработки персональных данных, определяется и утверждается руководителем Общества. Доступ к персональным данным предоставляется только лицам, замещающим должности из Перечня.

4.3. Работники Общества имеют доступ к персональным данным и выполняют действия по обработке персональных данных в пределах, определенных должностными обязанностями.

4.4. Работники, получившие доступ к персональным данным, должны использовать эти данные лишь в целях, для которых они обрабатываются, соблюдать режим конфиденциальности, информировать Общество об утечке персональных данных, о фактах нарушения порядка обращения с ними и о попытках несанкционированного доступа к персональным данным.

4.5. Внешний доступ.

4.5.1. Сообщение сведений о персональных данных другим организациям и гражданам разрешается при наличии письменного согласия работника или контрагента и заявления подписанного руководителем организации либо гражданином, запросившим такие сведения.

4.5.2. К лицам, которым могут быть переданы персональные данные вне организации, при условии соблюдения законодательства относятся:
- правоохранительные органы;
- налоговые органы;
- судебные органы;
- отделения Пенсионного фонда РФ;
- отделения Фонда социального страхования;
- отделения Фонда обязательного медицинского страхования;
- федеральная инспекция труда;
- военкоматы;
- иные органы и организации в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

4.5.3. Надзорные и контрольные органы имеют доступ к информации только в пределах своей компетенции.

5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Защите подлежат:
- персональные данные работника, клиента, контрагента, содержащиеся в копиях документов;
- персональные данные работника, клиента, контрагента, содержащиеся в документах, созданных Обществом;
- персональные данные работника, клиента, контрагента, занесенные в учетные формы;

- записи, содержащие персональные данные работника, клиента, контрагента;
- персональные данные работника, клиента, контрагента, содержащиеся на электронных носителях.

5.2. Общество принимает необходимые правовые, организационные и технические меры 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 в соответствии со статьей 19 Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных».

5.2.1. Обществом принимаются следующие правовые и организационные меры:

1) Разработаны и утверждены локальные нормативные акты Общества: Политика в отношении обработки и защиты персональных данных, Положение о защите персональных данных работников, клиентов и контрагентов, которыми регламентируется порядок получения, обработки, хранения, передачи и защиты персональных данных в Обществе.
2) Определен перечень должностей, на которых работники имеют доступ к персональным данным.
3) Установлен обязательный порядок ознакомления работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Общества в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.
4) Все лица, в обязанности которых входит непосредственное осуществление обработки персональных данных, при приеме на работу обязаны подписывать обязательство о неразглашении персональных данных.
5) Приказом директора Общества назначено ответственное лицо за организацию обработки персональных данных.
6) Обеспечен неограниченный доступ к Политике в отношении обработки и защиты персональных данных.
7) Бесконтрольное использование защищаемой информации обеспечивается тем, что:
   - рабочие места работников размещаются таким образом, чтобы исключить возможность обозрения находящихся на столе документов, а также мониторов компьютеров посторонними лицами;
   - документы, содержащие персональные данные, хранятся в запираемых шкафах, а также в металлическом запираемом сейфе;
   - персональные данные, обработка, которых осуществляется в различных целях, хранятся раздельно.

5.2.2. Технические меры:

8) Помещение, в котором осуществляется обработка персональных данных, должно быть оборудовано охранной сигнализацией.
9) Кабинеты, в котором осуществляется обработка персональных данных и(или) хранение, опечатывается. Право доступа в кабинет имеют лица, допущенные к обработке персональных данных на основании приказа директора Общества.
10) Персональные компьютеры работников Общества, непосредственно осуществляющих обработку персональных данных, защищаются паролями, которые известны этим

работникам соответственно. Пароли должны изменяться не реже одного раза в два месяца. На указанных персональных компьютерах также имеется антивирусная защита.

5.3. Общество осуществляет внутренний контроль и аудит соответствия порядка обработки персональных данных Федеральному закону от 27.07.2006 года №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных.

6. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ.

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

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

- уведомить членов комиссии о работах по уничтожению персональных данных;
- определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);
- установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению (и/или материальные носители персональных данных);
- определить технологию (приём, способ) уничтожения персональных данных (и/или материальных носителей персональных данных);
- определить технические (материальные, программные и иные) средства, посредством которых будет произведено уничтожение персональных данных;
- руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных);
- оформить соответствующий Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) и представить Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) на утверждение руководителю;
- в случае необходимости уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

7. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В целях защиты персональных данных, хранящихся у Общества, субъект персональных данных имеет право на:

7.1.1. Предоставление полной информации о составе персональных данных и их обработке.

7.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации.

7.1.3. Определение представителей для защиты своих персональных данных.

7.1.4. Требование об исключении или исправлении неверных, или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Общества

персональных данных. При отказе Общества исключить или исправить персональные данные субъект персональных данных имеет право заявить в письменной форме Обществу о своем несогласии с соответствующим обоснованием такого несогласия.

7.1.5. Требование об извещении Обществом всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

7.1.6. Обжалование в суд любых неправомерных действий или бездействия Общества при обработке и защите его персональных данных.

7.2. В целях обеспечения достоверности персональных данных субъект персональных данных обязан:

7.2.1. При заключении договора предоставить Обществу полные и достоверные данные о себе.

7.2.2. В случае изменения сведений, составляющих персональные данные, незамедлительно, но не позднее пяти рабочих дней, предоставить данную информацию Обществу.

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

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

8.2. Дисциплинарная ответственность:

a) Разглашение персональных данных работника, клиента, контрагента Общества, то есть передача посторонним лицам, не имеющим к ним доступа; публичное раскрытие; утрата документов и иных носителей, содержащих персональные данные работника; иные нарушения обязанностей по их защите, обработке и хранению, установленных настоящим Положением, а также иными локальными нормативными актами Общества, лицом, ответственным за получение, обработку и защиту персональных данных работника, влекут наложение на него дисциплинарного взыскания - выговора, увольнения (пп. «в» п.6 ч. 1 ст. 81 Трудового кодекса РФ).

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

8.3. Административная ответственность:

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

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

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