Приложение
УТВЕРЖДЕНО
приказом МКК ТОФПМП
от «23» июля 2020 г. № 19/3

ПОЛОЖЕНИЕ

по обеспечению безопасности персональных данных в Микрокредитной компании Тульский областной фонд поддержки малого предпринимательства

1. Термины и определения

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

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

Использование персональных данных - действия (операции) с персональными данными, совершаемые Оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других
ЛИЦ.

Конфиденциальность персональных данных - обязательное для соблюдения Оператором требование не допускать распространения персональных данных без согласия субъекта персональных данных или наличия иного законного основания.

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
ДЕННЫХ.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

Оператор персональных данных (далее 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. В рамках настоящего Положения Оператором является МКК ТОФПМП.

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

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

Сотрудник (работник) - физическое лицо, состоящее в трудовых отношениях с МКК ТОФПМП.

Субъект - физическое лицо, обладатель собственных персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2. Общие положения

2.1 Назначение документа

2.1.1. Целью настоящего «Положения по обеспечению безопасности персональных данных» (далее - Положение) является регламентация технологического и организационного процесса защиты персональных данных в МКК ТОФПМП.

2.1.2. Положение разработано в соответствии с частью 1 статьи 23, статьи 24 Конституции Российской Федерации, главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников» от 30.12.2001 № 197-ФЗ, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2.2. Вступление в силу документа

2.2.1. Настоящее Положение вступает в силу с момента его утверждения руководителем МКК ТОФПМП и действует бессрочно.

2.2.2. Действие настоящего Положения может быть отменено приказом руководителя МКК ТОФПМП в связи с утратой актуальности, либо по иным причинам.

2.2.3. Все изменения настоящего Положения утверждаются приказом руководителя МКК ТОФПМП.

2.2.4. Все работники МКК ТОФПМП, допущенные к обработке персональных данных, должны быть ознакомлены с настоящим Положением под роспись в течение одного месяца с момента принятия настоящего Положения, а так же, в аналогичный срок с момента принятия изменений вносимых в настоящее Положение.

2.2.5. Все вновь принимаемые на работу в МКК ТОФПМП сотрудники, для исполнения должностных обязанностей которых необходим допуск к обработке персональных данных, должны быть ознакомлены (под роспись) с настоящим Положением до начала исполнения этих обязанностей.

3. Принципы защиты персональных данных субъектов

3.1. В целях защиты персональных данных субъектов создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение персональными данными. Целью и результатом несанкционированного доступа к персональным данным субъектов может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внедрение вредоносных программ, фальсификация содержания реквизитов документа и др.

3.2. Основным источником несанкционированного доступа к персональным данным является персонал, работающий с документами, содержащими персональные данные.

3.3. Посторонние лица не должны знать информацию о распределении функций, рабочих процессах, технологии составления, оформления, ведения и хранения документов, дел и рабочих материалов в информационных системах персональных данных. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности МКК ТОФПМП, например посетители, работники других организационных структур.

3.4. Для обеспечения защиты персональных данных необходимо соблюдать следующие организационно-технические меры:

а) регламентация состава работников, функциональные обязанности которых требуют доступа к персональным данным, и процесса предоставления такого доступа;

б) регламентация порядка приёма, учёта и контроля деятельности посетителей;

в) поддержания порядка охраны зданий и помещений;

г) периодический контроль обеспечения защищённости персональных данных

субъектов;

д) соблюдение требований к защите персональных данных субъектов при интервьюировании и собеседованиях.

3.5. В случаях обнаружения несоблюдения условий хранения носителей ПДн и/или несоблюдения использования средств защиты информации, а так же в случае обнаружения нарушения порядка предоставления персональных данных, должно производиться разбирательство и составляться заключение по выявленным фактам.

4. Перечень мер по защите персональных данных при их автоматизированной обработке

4.1. Для обеспечения защиты персональных данных при их обработке в информационных системах должны приниматься следующие меры:

а) определение угроз безопасности персональным данным при их обработке, формирование на их основе модели угроз;

б) разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учёт лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4.2. Порядок доступа в помещения МКК ТОФПМП, в которых ведётся обработка персональных данных представлен в документе «Порядок доступа в помещения Микрокредитной компании Тульский областной фонд поддержки малого предпринимательства, в которых ведётся обработка персональных данных».

5. Перечень мер по защите персональных данных, обрабатываемых без использования средств автоматизации

5.1. Для обеспечения защиты материальных носителей, содержащих персональные данные субъектов, обрабатываемых в МКК ТОФПМП, Оператор обязан:

5.1.1. Довести до сотрудников, осуществляющих обработку персональных данных субъектов на материальных носителях, информацию об особенностях и правилах осуществления такой обработки.

5.1.2. Запретить вынос за пределы МКК ТОФПМП носителей, содержащих персональные данные субъектов, за исключением случаев, установленных законодательством.

5.1.3. Хранить носители, содержащие персональные данные, только в сейфах

(шкафах), с надёжными средствами защиты, предотвращающими неконтролируемый доступ к ним. Места хранения носителей определяются приказом руководителя МКК ТОФПМП «Об утверждении мест хранения носителей персональных данных».

5.1.4. Обеспечить учёт материальных носителей, содержащих персональные данные. Система учёта должна предоставлять возможность контроля над местонахождением каждого материального носителя.

5.1.5. Организационно исключить необоснованное ознакомление с персональными данными лиц, не имеющих соответствующих полномочий.

5.1.6. Обеспечить защиту от несанкционированного доступа и копирования персональных данных на материальных носителях, согласно организационным и распорядительным документам, принятым в МКК ТОФПМП.

6. Контроль защищённости персональных данных субъектов

6.1. Необходимо производить периодический контроль выполнения организационно-технических мер, а также контроль защищённости информационных ресурсов, содержащих персональные данные.

6.2. Виды контроля состояния защищённости персональных данных субъектов, обрабатываемые МКК ТОФПМГ1:

а) предварительный контроль (оценочная проверка обоснованности мер защиты персональных данных до начала их обработки). Осуществляется с целью своевременного выявления и предотвращения предпосылок возможных нарушений требований или норм защиты персональных данных;

б) текущий контроль (проверка в процессе обработки персональных данных). Осуществляется с целью своевременного выявления возникающих трудностей и недостатков реализации, принятых мер защиты персональных данных и выработки мероприятий по их устранению. Текущий контроль может быть периодическим, повседневным или непрерывным;

в) контроль устранения недостатков (проверка, проводимая после устранения ранее допущенных нарушений норм и требований защиты персональных данных, вследствие которых были приостановлены или ограничены работы с защищаемыми персональными данными субъектов). Осуществляется с целью выдачи разрешения на продолжение обработки персональных данных субъектов;

г) внутренний контроль. Проводится силами уполномоченных работников МКК ТОФПМП;

д) организационный контроль. Подразумевает проверку состояния полноты и обоснованности мероприятий, по защите защищаемых информационных ресурсов требованиям соответствующих руководящих и нормативных документов;

е) контроль эффективности. Проводится с целью проверки соответствия количественных или качественных показателей эффективности мероприятий по защите персональных данных установленным требованиям или нормам эффективности защиты;

ж) технический контроль. Обеспечивает проверку эффективности защиты персональных данных с использованием технических и (или) программных средств контроля и в дальнейшем получение наиболее объективной и достоверной информации о состоянии объектов контроля.

7. Организационная структура и обязанности ответственных лиц

7.1. Приказом руководителя МКК ТОФПМП назначается лицо, ответственное за обработку персональных данных (ответственное лицо), администратор информационной системы персональных данных (ИСПДн) и администратор безопасности ИСПДн, которые проводят мероприятия по защите персональных данных субъектов. При необходимости дополнительно назначаются лица, ответственные за обработку персональных данных в структурных подразделениях.

7.2. Лицо, ответственное за организацию обработки персональных данных:

а) осуществляет внутренний контроль над соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

б) доводит до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

в) организует приём и обработку обращений и запросов субъектов персональных данных или их представителей и осуществляет контроль за приёмом и обработкой таких обращений и запросов.

7.3 Администратор ИСПДн отвечает за обеспечение работоспособности элементов ИСПДн и средств защиты персональных данных.

7.4 Администратор безопасности ИСПДн отвечает за обеспечение необходимого уровня состояния защиты ИСПДн, правильность настройки средств защиты, организацию выдачи, хранения и уничтожения материальных носителей персональных данных.

8. Обязанности Оператора и субъектов персональных данных

8.1. Сотрудники МКК ТОФПМП использовать персональные данные только в соответствии с целями обработки, определившими их получение.

8.2. Сотрудники МКК ТОФПМП обязаны не отвечать на запросы, связанные с передачей персональных данных, по телефону или факсу.

8.3. Для защиты персональных данных субъектов МКК ТОФПМП обязано:

а) за свой счёт, в порядке, установленном законодательством РФ, обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты;

б) ознакомить сотрудника с настоящим Положением под расписку;

в) по запросу ознакомить субъекта персональных данных, не являющегося сотрудником, или в случае недееспособности либо несовершеннолетия субъекта, его законного представителя с настоящим Положением под расписку;

г) осуществлять передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;

д) предоставлять персональные данные субъекта только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим Положением и законодательством Российской Федерации;

е) по требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и порядке обработки этих данных.

8.4. При обнаружении нарушений порядка предоставления персональных данных сотрудники МКК ТОФПМП обязаны незамедлительно приостановить предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

8.5 Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности.

9. Права субъектов персональных данных

9.1. Субъекты персональных данных имеют право:

9.2. На получение информации, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных оператором;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые оператором способы обработки персональных данных;

г) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на

основании федерального закона;

д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

е) сроки обработки персональных данных, в том числе сроки их хранения;

ж) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

з) информацию об осуществлённой или о предполагаемой трансграничной передаче данных;

и) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

к) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

9.3. Получать доступ к своим персональным данным, включая право получать копии любой записи, содержащей собственные персональные данные, за исключением случаев, предусмотренных федеральным законом;

9.4. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;

9.5. При отказе Оператора или уполномоченного им лица исключить или исправить персональные данные субъекта - заявить в письменной форме о своём несогласии, представив соответствующее обоснование;

9.6. Требовать от Оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них изменениях.

9.7. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

а) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

б) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

в) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма;

г) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

д) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

10. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных сотрудника

10.1. Руководитель, разрешающий доступ сотрудника к конфиденциальному

документу, содержащему персональные данные, несёт персональную ответственность за данное разрешение.

10.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, материальную, административную, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации.

10.3. Каждый сотрудник несёт единоличную ответственность за сохранность и конфиденциальность полученных в процессе работы персональных данных субъектов.

10.4. За неисполнение или ненадлежащее исполнение сотрудником возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера руководство Оператора вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

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