Общество с ограниченной ответственностью Микрокредитная компания «Сибирская кредитно-сберегательная корпорация»

Введена в действие Приказом № 8-п от «25» июля 2019 г.

Председатель правления _____ М.Г. Четыркин

Политика безопасности персональных данных

Область бизнес-процессов:	Управление информационной безопасностью

№ текущей редакции документа:	**1**	**№ в Реестре:**	
Подразделение, ответственное за процесс:			

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ 2
1 ВВЕДЕНИЕ 3
2 ОСНОВНЫЕ ПОЛОЖЕНИЯ 3
3 КОНТРОЛЬ 6
4 ПОРЯДОК ПЕРЕСМОТРА 6

1 ВВЕДЕНИЕ

1.1 Назначение

Настоящая Политика безопасности персональных данных определяет основные принципы и требования Кредитного потребительского кооператива «Сибирская кредитно-сберегательная корпорация» (далее – «Компания») по защите персональных данных от актуальных угроз их безопасности.

Политика безопасности персональных данных является публичной и доводится до сведения всех заинтересованных сторон.

1.2 Цель

Целью принятия настоящей Политики является предотвращение ущерба бизнес-процессам Компании вследствие инцидентов при обработке персональных данных.

1.3 Область действия

Положения Политики распространяется на все подразделения Компании и на отношения Компании с контрагентами.

1.4 Нормативные ссылки

Настоящая Политика подготовлена в соответствии с положениями следующих нормативных документов:

№	Нормативные документы
1.	Федеральный Закон № 152-ФЗ от 27.07.2006 «О персональных данных»
2.	Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
3.	Постановление Правительства РФ от 15.09.2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"

2 ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1 В Компании допускаются к обработке персональные данные сотрудников Компании, её участников, партнёров и иных субъектов персональных данных, полученные как от самих субъектов персональных данных, так и из общедоступных источников информации.

2.2 В Компании не разрешается обрабатывать персональные данные, содержащие:

- специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;
- биометрические персональные данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

2.3 Под обработкой персональных данных в Компании понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием информационных систем или без использования таких систем, с персональными данными, включая:

- сбор,
- запись,
- систематизацию,
- накопление,
- хранение,
- уточнение (обновление, изменение),
- извлечение,
- использование,

- передачу (распространение, предоставление, доступ),
- обезличивание,
- блокирование,
- удаление и
- уничтожение.

2.4 Безопасность персональных данных в Компании обеспечивается созданием системы организационных и технических мер защиты, нейтрализующих актуальные угрозы, и созданных на основании действующего законодательства РФ и международных стандартов.

Под безопасностью персональных данных понимается обеспечение конфиденциальности, целостности и доступности персональных данных.

2.5 Актуальные угрозы безопасности персональных данных определяются в соответствии с действующими нормативными документами государственных органов, уполномоченных правительством РФ на контрольные функции в сфере защиты персональных данных, и отражаются в Модели угроз безопасности персональных данных Компании.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в Компании, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

2.6 Ответственность за безопасность персональных данных при их обработке несет сотрудник Компании, который обрабатывает персональные данные, или контрагент, осуществляющий обработку персональных данных по поручению Компании на основании заключаемого с этим контрагентом договора (далее – «Контрагент»). Договор между Компанией и Контрагентом должен предусматривать обязанность Контрагента обеспечить безопасность персональных данных при их обработке.

2.7 Лица, осуществляющие обработку персональных данных, сотрудники Компании и Контрагенты, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также регламентами Компании.

2.8 Для организации защиты персональных данных при их обработке в Компании и Контрагентами назначается должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в Компании.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационных системах Компании могут привлекаться на договорной основе внешние организации и лица, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

2.9 Защита персональных данных при их обработке в информационных системах Компании обеспечивается выполнением следующих организационных мер:

- организация режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими

служебных обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

2.10 В состав технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах Компании входят:
- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

2.11 Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обосабливаются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

2.12 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

2.13 При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, должны быть приняты меры по обеспечению раздельной обработки персональных данных.

2.14 Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

2.15 При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

2.16 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:
- типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, наименование и адрес Компании, источник получения персональных данных, сроки обработки персональных данных, общее описание используемых способов обработки персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

2.17. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного применения, например, для оформления разового пропуска на территорию Компании, должны соблюдаться следующие условия:

- ведение такого журнала (реестра, книги) должно быть оформлено распоряжением директора Компании;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза.

2.18 Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.19 Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

2.20 Состав и содержание конкретных мер по обеспечению безопасности персональных данных, отражается в Положении о порядке обработки персональных данных, должностных инструкциях сотрудников, договорах с Контрагентами, и иных регламентах Компании.

3 КОНТРОЛЬ

3.1. Контроль (аудит) обеспечения безопасности персональных данных проводится Компанией и её Контрагентами самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.2. Указанный контроль проводится не реже одного раза в три года.

4. ПОРЯДОК ПЕРЕСМОТРА

Пересмотр Политики безопасности персональных данных производится на регулярной основе не реже одного раза в три года. При внесении изменений учитываются:

- изменения законодательства РФ в области защиты персональных данных;
- результаты аудита;
- изменения бизнес-процессов Компании.