«УТВЕРДЖАЮ»
Решением Общего собрания членов
Кредитного потребительского кооператива «Прогресс Сервис»
Протокол № 13 от « 31» июля 2018 г.

Председатель собрания Миневич О.Д.

Секретарь собрания Лашина Л.А.

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПОРЯДКЕ СОБЛЮДЕНИЯ ТАЙНЫ (РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ) В ОТНОШЕНИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОПЕРАЦИЙ, СОВЕРШАЕМЫХ ИМИ В КПК «ПРОГРЕСС СЕРВИС »

Г.Серов,
2018г.

Настоящее Положение о порядке соблюдения тайны (режима конфиденциальности) в отношении операций пайщиков КПК «Прогресс Сервис» (далее - Положение) разработано Кредитным потребительским кооперативом «Прогресс Сервис» (КПК «Прогресс Сервис»), являющийся членом Союза Саморегулируемой организации «Губернское кредитное содружество» (запись в Реестре членов Союза СРО «ГКС»№ 4), (далее - Займодавец) в целях определения порядка исполнения обязанности Займодавца гарантировать тайну об операциях своих заемщиков.

Настоящее положение входит в состав организационно-распорядительных документов Займодавца, регламентирующих работу с персональными данными и иной конфиденциальной информацией, и обязательно для соблюдения всеми работниками, а также иными лицами, имеющими доступ к такой информации.

1. Термины и определения

1.1. Займодавец – Кредитный потребительский кооператив «Прогресс Сервис»(КПК«Прогресс Сервис»), являющийся членом Союза Саморегулируемой организации «Губернское кредитное содружество» (запись в Реестре членов Союза СРО «ГКС»№ 4).

1.2. Заемщик – физическое или юридическое лицо, заключившее договор займа с Займодавцем.

1.3. Операция заемщика – любое действие заемщика, произведенное в целях заключения договора займа, исполнения обязательств по договору займа, включая подписание анкет, заявлений, согласий, договоров и платёжных документов в связи с заключением договора займа.

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

1.5. Безопасность персональных данных: Состояние защищенности ПДн от неправомерных действий, характеризуемое способностью пользователей, технических средств и информационных систем обеспечить конфиденциальность, целостность и доступность ПДн при их обработке, независимо от формы их представления.

1.6. Вредоносное программное обеспечение: Программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

1.7. Доступ к информации: Возможность получения и использования информации.

1.8. Доступность персональных данных: Возможность беспрепятственного получения санкционированного доступа к персональным данным лицами, имеющими право на такой доступ.

1.9. Информационная система персональных данных: Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.10. Конфиденциальность персональных данных: Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не допускать их распространения при отсутствии согласия субъекта ПДн или иного законного основания.

1.11. 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.

1.12. Пользователь персональных данных: Лицо, участвующее в процессах(е) обработки ПДн или использующее результаты такой обработки.

1.13. Процесс обработки персональных данных: Бизнес-процесс Займодавца, в рамках которого осуществляется обработка персональных данных.

1.14. Средство вычислительной техники: Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
1.15. Средство защиты информации: Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
1.16. 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.
1.17. Целостность персональных данных: Способность средства вычислительной техники или информационной системы обеспечивать неизменность персональных данных в условиях случайного и/или преднамеренного их искажения (разрушения).

2. Порядок установления и соблюдения режима тайны об операциях заемщиков

2.1. Все работники Займодавца обязаны соблюдать тайну об операциях заемщиков Займодавца.
2.2. Исполнение обязанности, указанной в п.2.1. настоящего Положения, обеспечивается путем принятия всеми работниками настоящего положения под роспись.
2.3. Принятие и исполнение данного Положения, подписание Обязательства о неразглашении признается необходимым и достаточным для соблюдения тайны об операциях заемщиков.
2.4. Обеспечения тайны об операциях заемщиков является частью исполнения обязанностей Займодавца по соблюдению режима конфиденциальности и иных требований законодательства в отношении обработки персональных данных.
2.5. Любые операции заемщика, попадающие под определение п. 1.3 настоящего положения признаются конфиденциальными.
2.6. Информация об операциях заемщика не может быть предоставлена никаким третьим лицам, за исключением случаев, предусмотренных законодательством или соглашением между Займодавцем и заемщиком.

3. Меры по обеспечению безопасности ПДн и соблюдения режима тайны операций заемщиков

3.1. Общие меры по обеспечению безопасности ПДн и соблюдения режима тайны операций заемщиков
3.1.1. При обработке ПДн Пользователи ПДн обязаны соблюдать следующие меры предосторожности:

- не предоставлять ПДн лицам, не имеющим права доступа к данной информации;
- не выносить носители ПДн за пределы территории Займодавца без согласования с непосредственным руководителем;
- не использовать ПДн в открытых публикациях (например, при написании статей, докладов и др.);
- не накапливать излишние ПДн (уничтожать документы и файлы по мере завершения работы с ними);
- осуществлять уничтожение документов средствами гарантированного уничтожения (шредер);
- не копировать и не печатать содержащие ПДн файлы без надобности (в том числе и на внешние съемные носители);
- не отправлять содержащие ПДн файлы на личную электронную почту, общедоступные файловые хранилища;
- не разглашать логины/пароли доступа к ресурсам Займодавца;

- не оставлять на рабочих местах носители ПДн без присмотра;
- не оставлять незапертыми после окончания работы шкафы, сейфы, помещения и хранилища с носителями ПДн;
- не обработывать ПДн в условиях, позволяющих осуществлять просмотр ПДн лицами, не имеющими к ним доступа, а также в условиях несоблюдения требований по эксплуатации рабочей станции;
- блокировать рабочую станцию при покидании рабочего места;
- не устанавливать самостоятельно программное обеспечение на рабочие станции;
- не подключать самостоятельно к рабочим станциям какие-либо устройства и не вносить изменения в состав, параметры конфигурации технических компонентов рабочих станций;
- не использовать программные и/или аппаратные компоненты ИСПДн в неслужебных целях;
- не использовать личные устройства для обработки ПДн (смартфоны, планшетные компьютеры и т.п.);
- соблюдать правила работы со СЗИ и установленный режим разграничения доступа к техническим компонентам ИСПДн и файлам, содержащим ПДн, при их обработке;
- присутствовать при работах по изменению аппаратно-программной конфигурации закрепленной за ним рабочей станции, а по завершении таких работ проверять ее работоспособность;
- хранить в тайне информацию о СЗПДн (о средствах, механизмах, процедурах и т.д.);
- предоставлять всю необходимую информацию и документы при расследовании инцидентов ИБ, связанных с обработкой и обеспечением безопасности ПДн, проведении внутренних контрольных мероприятий по защите ПДн, а также во время проверок со стороны регулирующих органов.

3.2. Обеспечение парольной защиты

3.2.1. При первичном доступе к ПДн Пользователю необходимо сформировать стойкий пароль для своей учетной записи. Пароль должен быть сформирован в соответствии со следующими рекомендациями:

- длина пароля составляет не менее 8-ми символов;
- длина пароля для привилегированных пользователей составляет не менее 10-ти символов;
- в составе символов пароля обязательно присутствуют буквы в верхнем и нижнем регистрах, цифры и специальные символы (“ ~ ! @ # $ % ^ & * ( ) - + _ = \ | / ? ,);
- при смене пароля новое значение отличается от предыдущего не менее чем в 4-ех позициях;
- пароль может повторяться не менее чем после использования 5-ти различных паролей;
- пароль не включает в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на знании информации о Пользователе.

3.2.2. В рамках обеспечения парольной защиты Пользователь ПДн обязан:

- хранить в тайне свои данные для аутентификации в системе (имя пользователя и пароль доступа);
- обновлять пароли не реже чем один раз в полгода;

- использовать разные пароли для разных систем.

3.3. Обеспечение антивирусной защиты

3.3.1. В рамках обеспечения антивирусной защиты Пользователь ПДн обязан:

- контролировать факт запуска антивирусного ПО после загрузки операционной системы;
- контролировать обновление антивирусных баз на своем ПК путем сравнения даты последнего обновления с датой на момент контроля (даты не должны отличаться более чем на 1 календарный день);
- осуществлять антивирусный контроль любой информации, получаемой по телекоммуникационным каналам;
- осуществлять антивирусный контроль съемных носителей информации (дискет, оптических дисков, USB flash-накопителей) при их подключении к рабочей станции.
- При возникновении подозрения на наличие вредоносного ПО (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь ПДн обязан сообщить об этом Ответственному за обеспечению безопасности ПДн, а также провести внеочередной антивирусный контроль своей рабочей станции (если это позволяют сделать его права доступа в системе).

3.4. Оповещение при нарушениях безопасности ПДн

3.4.1. С целью своевременного обнаружения событий безопасности, которые могут привести к нарушению конфиденциальности ПДн или нарушению процессов их обработки, Пользователь ПДн должен своевременно оповещать Ответственных за обеспечение безопасности ПДн в следующих случаях:

- заметного снижения производительности при работе с сетью Интернет, недоступности ресурсов;
- значительного увеличения времени отклика средств вычислительной техники, изменения дат обновления файлов, значительного возрастания размеров файлов, системных сбоев (включая случаи, когда операционная система перестает загружаться);
- получения по электронной почте подозрительных сообщений;
- получения сообщений от антивирусного ПО об обнаружении вредоносного ПО;
- присутствия незнакомых подозрительных лиц на территории Займодавца;
- утери личного пропуска на территорию Займодавца;
- повреждения, удаления или утраты доступа к файлам;
- обнаружения вскрытых шкафов, ящиков и прочих мест хранения носителей ПДн.

3.4.2. Пользователь ПДн должен своевременно оповещать своего непосредственного руководителя в следующих случаях:

- подозрения на неправомерность обработки ПДн;
- обращения субъекта ПДн по вопросам, связанным с обработкой или обеспечением безопасности ПДн;
- недоступности одного или нескольких информационных ресурсов;
- обнаружения вскрытых шкафов, ящиков и прочих мест хранения носителей ПДн;
- отправки ПДн на ошибочный адрес;
- утери документов, содержащих ПДн;
- подозрения на компрометацию личных ключей и паролей;
- нахождения документов, содержащих ПДн;
- обнаружения любых подозрительных событий, которые могут привести к разглашению ПДн или нарушению процессов обработки ПДн и обеспечения тайны операций заемщиков Займодавца;
- нарушения требований настоящего Положения.

4. Порядок получения доступа к обработке ПДн

4.1. Доступ к обработке ПДн предоставляется работникам при условиях:

4.1.1. Ознакомления с внутренними документами Займодавца, определяющими правила обработки и обеспечения безопасности ПДн;

4.1.2. прохождения инструктажа по правилам обработки и обеспечения безопасности ПДн.

4.1.3. По результатам изучения документов и прохождения инструктажа Пользователь ПДн обязан знать:

- штатные режимы работы и правила работы с техническими компонентами ИСПДн;
- правила парольной защиты;
- правила антивирусной защиты;
- способы выявления и последовательность действий в случае выявления нештатного функционирования технических компонентов ИСПДн;
- правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий от инцидентов ИБ.

4.1.4. Пользователь ПДн имеет право обратиться за консультацией:

- по общим вопросам обеспечения безопасности ПДн в Займодавца – к Ответственному за организацию обработки ПДн;
- по вопросам автоматизированной и неавтоматизированной обработки ПДн в рамках процесса обработки ПДн, в котором он принимает участие, к непосредственному руководителю или руководителю структурного подразделения, в компетенции которого находится данный процесс;
- по вопросам использования СЗИ и технических компонентов ИСПДн – к Ответственным за обеспечение безопасности ПДн.

5. Ответственность

5.1. За несоблюдение требований нормативных документов РФ в области обработки и защиты ПДн предусмотрена дисциплинарная, административная, гражданская и уголовная ответственность.

5.2. Пользователь ПДн несет ответственность в пределах, определенных действующими нормативными документами РФ, за:

- ненадлежащее выполнение требований настоящего Положения;
- сохранность ПДн (обеспечение их конфиденциальности, целостности и доступности);
- сохранность и работоспособность используемых им средств обработки и защиты ПДн.

5.3. Руководство Займодавца вправе применять к Пользователям ПДн предусмотренные Трудовым Кодексом РФ дисциплинарные взыскания.

6. Заключительные положения

6.1. Настоящее Положение действуют с момента его утверждения уполномоченным органом Займодавца, если в решении об их утверждении не указан иной срок, до момента одного из следующих событий, наступивших раньше: утверждение новой редакции Положения или его отмена, прекращение деятельности Займодавца, исключение Займодавца из реестра Союза Саморегулируемой организации «Губернское кредитное содружество».

6.2. Контроль исполнения требований настоящего Положения осуществляется лицом, ответственным за обработку персональных данных в Займодавце.

6.3. Во всем, не определенным настоящим Положением, Займодавец руководствуется положениями законодательства и иными внутренними организационно-распорядительными документами в области обработки ПДн, работы с коммерческой тайной и иной конфиденциальной информацией.