

Информационная безопасность

**Положение о защите персональных данных
Банк «СКС» (ООО)
(Выписка)**

Конфиденциальная информация Банк «СКС» (ООО)

Вся информация, содержащаяся в данном документе, является собственностью Банк «СКС» (ООО) и не может быть полностью или частично воспроизведена, разглашена или использована без письменного разрешения.

Управление документацией

История изменений

Версия	Дата	Автор	Причина внесения изменений
1.0			Новый документ

Оглавление

1.	ОБЩИЕ ПОЛОЖЕНИЯ.....	4
2.	СОСТАВ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ	4
3.	ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	6
4.	КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	7
5.	ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	7
6.	ПОЛУЧЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ БАНКА	8
7.	ХРАНЕНИЕ И ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ.....	8
8.	ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ.....	9
9.	ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТА.....	10
10.	ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.....	10
	Приложение № 1	12

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее «Положение о защите персональных данных» (далее по тексту – Положение), разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных», Федеральным законом «Об информатизации, информации и защите информации», Федеральным законом «О банках и банковской деятельности» и Федеральным Законом «О коммерческой тайне» в целях урегулирования процесса получения, хранения, комбинирования, передачи или другого вида использования персональных данных, обрабатываемых в Банк «СКС» (ООО) (далее по тексту - Банк).

1.2. Персональные данные (далее – ПДн) являются информацией конфиденциального характера. Перечень сведений, составляющих персональные данные, их обработка, обеспечение сохранности и контроля доступа, а также требования по защите персональных данных определяются законодательством Российской Федерации, нормативными актами Банка России и настоящим Положением.

1.3. Обработка персональных данных осуществляется в целях обеспечения соблюдения законов и иных нормативных правовых актов, при обеспечении Банком обслуживания клиентов (далее – субъекты ПДн).

1.4. Лица, виновные в нарушении норм, регулирующих получение, обработку, хранение и защиту персональных данных, несут дисциплинарную, административную, гражданскую или уголовную ответственность в соответствии с федеральными законами, в том числе за сохранность, достоверность и полноту данной информации, обеспечение ее конфиденциальности, в том числе при передаче по системе телекоммуникаций, за правильность оформления учетной документации, а также за обеспечение беспрепятственного доступа субъектов ПДн к своим персональным данным.

1.5. Запрещается раскрытие и передача персональных данных третьим лицам без письменного согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья субъекта ПДн, а также в случаях, установленных действующим законодательством РФ.

1.6. Требования настоящего Положения обязательны для исполнения всеми сотрудниками Банк «СКС» (ООО).

2. СОСТАВ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Сведениями, составляющими ПДн в Банке является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн) в том числе:

- Фамилия, имя, отчество (в т. ч. прежние), дата и место рождения;
- Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ), и гражданство. Характеристики, идентифицирующие физиологические особенности человека и, на основе которых можно установить его личность;
- Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
- Номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта ПДн или по адресу его места жительства (по паспорту);
- Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения);

- Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения);
- Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса и телефона организации, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения);
- Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
- Содержание и реквизиты трудового договора с работником Банка или гражданско-правового договора с гражданином;
- Сведения о заработной плате (номера счетов, данные зарплатных договоров с клиентами, в том числе номера их спецкартсчетов, данные по окладу, надбавкам, налогам и другие сведения);
- Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии/снятии на(с) учет(а) и другие сведения);
- Сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2НДФЛ супруга(и), данные документов по долговым обязательствам, степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения);
- Сведения об имуществе (имущественном положении):
 - автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств),
 - недвижимое имущество (вид, тип, способ получения, общие характеристики, стоимость, полные адреса размещения объектов недвижимости и другие сведения),
 - банковские вклады (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов, вид, срок размещения, сумма, условия вклада и другие сведения),
 - кредиты (займы), банковские счета (в том числе спецкартсчета), денежные средства и ценные бумаги, в том числе в доверительном управлении и на доверительном хранении (данные договоров с клиентами, в том числе номера счетов, спецкартсчетов, номера банковских карт, кодовая информация по банковским картам, коды кредитных историй, адреса приобретаемых объектов недвижимости, сумма и валюта кредита или займа, цель кредитования, условия кредитования, сведения о залоге, сведения о приобретаемом объекте, данные по ценным бумагам, остатки и суммы движения по счетам, тип банковских карт, лимиты и другие сведения);
- Сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
- Сведения об идентификационном номере налогоплательщика;

- Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования);
- Сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения).

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Необходимость обработки и состав обрабатываемых персональных данных определяется исходя из принципа целесообразности такой обработки, при этом должны учитываться:

- цели обработки ПДн;
- планируемые характер и способы обработки ПДн;
- значимость обработки персональных данных для достижения целей деятельности организации;
- возникающие риски, связанные с обработкой персональных данных;
- затраты на осуществление обработки персональных данных, в том числе затраты на обеспечение требуемого уровня безопасности ПДн;

3.2. В Банке соответствующим приказом назначается лицо, ответственное за организацию обработки ПДн (далее – Ответственное лицо), в обязанности которого входят:

- обеспечение прав и интересов субъектов, персональные данные которых обрабатываются в Банке;
- определение соответствия характера и способа обработки целям обработки ПДн;
- определение состава обрабатываемых ПДн, перечня лиц, допущенных к обработке ПДн, перечня лиц, допущенных в помещения, в которых осуществляется обработка ПДн;
- анализ угроз безопасности ПДн;
- определение требований к системе защиты персональных данных;
- утверждение перечня и состава необходимых мероприятий по обеспечению безопасности;
- отслеживание состояния системы защиты персональных данных;
- взаимодействие с уполномоченным органом по защите прав субъектов персональных данных.

3.3. Ответственное лицо имеет право сформировать рабочую группу, состоящую из работников Банка, на которых возлагается ответственность за реализацию решений Ответственного лица в области обеспечения безопасности персональных данных. В состав рабочей группы входят представители подразделений, в которых обрабатываются персональные данные, а также представители направлений информационной безопасности и информационных технологий.

3.4. Решения об инициации новых бизнес-процессов обработки ПДн или внесении изменений в существующие бизнес-процессы обработки ПДн согласовываются Ответственным лицом.

3.5. Требования Ответственного лица к мероприятиям по обеспечению безопасности персональных данных являются обязательными для всех работников, осуществляющих обработку персональных данных.

3.6. Состав персональных данных, обрабатываемых в Банке, определяется внутренним документом и утверждается Председателем Правления Банка.

3.7. Банк не имеет права получать и обрабатывать персональные данные клиентов Банка об их расовой и национальной принадлежности, политических, религиозных и философских убеждениях, состоянии здоровья, интимной жизни.

4. КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В целях настоящего документа в качестве субъектов ПДн, персональные данные которых могут обрабатываться в Банке с использованием средств автоматизации или без использования таковых, понимаются нижеперечисленные категории физических лиц, условно именуемые далее:

4.1.1. Клиентами, в состав которых включаются:

- физические лица (заемщики, вкладчики и т.п.) и их Представители (лица, действующие по доверенности физических лиц и др.), имеющие договорные отношения с Банком о предоставлении банковских услуг, их поручители, выгодоприобретатели и т.п., а также потенциальные клиенты на этапе преддоговорных отношений с ними (действий в целях заключения договора);
- руководители, представители и работники юридических лиц, имеющих договорные отношения с Банком о предоставлении банковских услуг (в т.ч. корреспондентов) Банка или находящихся на этапе преддоговорных отношений с Банком;
- руководители, представители и работники юридических лиц, имеющих договорные отношения с Банком, отличные от предоставления банковских услуг или находящихся на преддоговорном этапе установления отношений.

4.1.2. Посетителями, в состав которых включаются:

- представители (должностные лица) государственных органов законодательной, исполнительной и судебной власти и управления;
- представители общественных организаций, коммерческих и некоммерческих структур и иных объединений (в т.ч. иностранных).

4.1.3. Иные субъекты персональных данных, которые не вошли в вышеперечисленные категории и, обработка персональных данных которых не противоречит законодательству РФ.

5. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Субъект ПДн имеет право на:

- Полную информацию о его персональных данных и обработке этих данных;
- Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта ПДн, за исключением случаев, предусмотренных федеральным законом;
- Определение своих представителей для защиты своих персональных данных;
- Требование об исключении или исправлении неверных и/или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства Российской Федерации. При отказе Банка исключить или исправить персональные данные, субъект ПДн имеет право заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера субъект ПДн имеет право дополнить заявлением, выражающим его собственную точку зрения;
- Требование об извещении Банком всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- Обжалование в суде любых неправомерных действий или бездействия Банка при обработке и защите его персональных данных.

6. ПОЛУЧЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ БАНКА

6.1. Получение персональных данных преимущественно осуществляется путем предоставления их клиентом Банка, на основании его письменного согласия (Приложение 1), за исключением случаев, предусмотренных действующим законодательством РФ.

6.2. Письменное согласие клиента Банка на обработку персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Банк «СКС» (ООО), получающего данное согласие;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие клиента Банка (субъекта персональных данных);
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Банком способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

6.3. Для обработки персональных данных, содержащихся в письменной форме согласия клиента Банка на обработку его персональных данных, дополнительное согласие не требуется.

6.4. Если персональные данные клиента Банка возможно получить только у третьей стороны, то он должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

6.5. В случае необходимости проверки персональных данных клиента, Банк «СКС» (ООО) должен заблаговременно сообщить об этом, о целях, предполагаемых источниках и способах получения персональных данных и последствиях отказа клиента Банка дать письменное согласие на их получение.

7. ХРАНЕНИЕ И ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Персональные данные клиентов Банка хранятся в подразделениях Банка, осуществляющих обслуживание клиентов, на бумажных носителях, в формах учетной документации, в автоматизированной базе данных. Хранение персональных данных клиентов Банка осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

7.2. Все действия по обработке персональных данных осуществляются только сотрудниками Банка, допущенными к работе с персональными данными приказом Председателя Правления или в соответствии с должностным положением¹ и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

7.3. Передача персональных данных клиентов Банка третьим лицам осуществляется Банк «СКС» (ООО) только с их письменного согласия, за исключением случаев, если:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица,

¹ В Должностных инструкциях сотрудников Банка, допущенных к работе с персональными данными по служебному положению, отдельным разделом должны быть указаны их права и обязанности при обработке персональных данных.

подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- Передача необходима для защиты жизни, здоровья и иных жизненно важных интересов клиента Банка, и получение его согласия невозможно;
- По запросу органов дознания, следствия и суда в связи с проведением расследования или судебным разбирательством;
- В целях организации работ с военными комиссариатами для постановки на воинский учет лиц, подлежащих призыву в порядке, установленном законодательством;
- В иных случаях, прямо предусмотренных Федеральными законами.

7.4. Передача персональных данных клиента Банка третьим лицам осуществляется на основании запроса третьего лица с разрешающей визой Председателя Правления Банка при условии соблюдения требований, предусмотренных п. 7.3 настоящего Положения.

7.5. В случаях, установленных действующим законодательством, доступ к персональным данным могут иметь государственные и негосударственные структуры:

- налоговые органы;
- правоохранительные органы (МВД, прокуратура и суды);
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- другие организации, перечень которых установлен действующим законодательством РФ.

8. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Безопасность персональных данных, обрабатываемых Банком, обеспечивается реализацией системы информационной безопасности Банка, включающей организационные и технические меры защиты информации, необходимые и достаточные для обеспечения требований нормативных правовых актов в области защиты персональных данных.

8.2. Общую организацию защиты персональных данных лиц и контроль соблюдения работниками мероприятий по защите персональных данных осуществляет Ответственное лицо.

8.3. Защите подлежат все обрабатываемые в Банке персональные данные, за исключением общедоступных и обезличенных персональных данных. Необходимые для защиты персональных данных мероприятия определяются Ответственным лицом.

8.4. В случае отсутствия работника на его рабочем месте не должно быть документов, содержащих персональные данные субъектов (работник должен соблюдать «политику чистых столов»).

8.5. В случае обнаружения признаков несанкционированного доступа к персональным данным или нарушения порядка хранения персональных данных, работник, осуществляющий обработку ПДн, обязан уведомить об этом Ответственное лицо.

8.6. Банком применяются следующие организационные и технические меры по защите информации:

- Назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;

- Ограничение и регламентация состава работников, имеющих доступ к персональным данным;
- Ознакомление работников с требованиями Федерального законодательства и нормативных документов Банка России, а также внутренних нормативных документов Банка по обработке и защите персональных данных;
- Регистрация и учёт действий пользователей информационных систем персональных данных;
- Применение систем программной и аппаратной аутентификации пользователей в информационной системе персональных данных;
- Применение средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи;
- Осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;
- Применение средств межсетевое экранирования и обнаружения вторжений;
- Применение средств резервного копирования и восстановления информации;
- Проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;
- Применение технических средств охраны помещений, в которых расположены технические средства информационных систем персональных данных, и мест хранения материальных носителей персональных данных.

9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТА

9.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту ПДн, установленных действующим законодательством, несут дисциплинарную, административную, гражданскую, уголовную или иную ответственность в соответствии с действующим законодательством Российской Федерации.

9.2. Сотрудники подразделений, в которых происходит обработка ПДн, несут персональную ответственность за обеспечение защиты обрабатываемых и хранящихся в их подразделениях ПДн.

9.3. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании ПДн возлагается на руководителей структурных подразделений и конкретных должностных лиц Банка, обрабатывающих ПДн.

9.4. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе, работникам Банка, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, внутренними нормативными актами (приказами, распоряжениями) Банка, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарного взыскания: замечания, выговора или увольнения.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Все имеющие отношение к персональным данным вопросы, не урегулированные настоящим Положением, разрешаются в соответствии с действующим законодательством Российской Федерации.

10.2. Порядок обработки и защиты персональных данных в филиалах Банк «СКС» (ООО) производится в соответствии с настоящим Положением.

10.3. Настоящее Положение вступает в силу с момента его утверждения Приказом Председателя Правления Банка.

10.4. Решения о внесении изменений и дополнений в Положение, а также о признании части или всех его положений утратившими силу, утверждаются Приказом Председателя Правления Банка.

Согласие на обработку персональных данных

Я, _____ (далее – Клиент),
(фамилия, имя, отчество)

проживающий(-ая) по адресу

(адрес регистрации)

документ, удостоверяющий личность, _____ № _____,
(вид документа) (серия и номер документа)

выдан _____,
(кем и когда выдан)

даю своё согласие Банк «СКС» (ООО) (далее – Банк или Оператор), зарегистрированному по адресу 121069, г. Москва, ул. Поварская, д. 23, стр. 4, на обработку своих персональных данных на следующих условиях:

1. Персональные данные будут обрабатываться в целях исполнения Банком обязательств по договору(ам), заключенному(ым) между Клиентом и Банком, выполнения операций в соответствии с поручениями Клиента;

2. Персональные данные будут обрабатываться в составе:

фамилия, имя, отчество;

паспортные данные;

год, месяц, дата и место рождения;

адрес регистрации, контактный телефон, адрес электронной почты;

семейное, социальное, имущественное положение;

образование;

профессия;

доходы;

должность и место работы;

(ненужное вычеркнуть, отсутствующее вписать)

3. Оператор может осуществлять с персональными данными такие действия, как: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

4. Обработка персональных данных может осуществляться с использованием или без использования средств автоматизации с передачей по внутренней сети Оператора, а также по сети Интернет в защищенном виде.

5. Передача персональных данных третьим лицам, включая и трансграничную передачу персональных данных как в страны, присоединившиеся к «Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» (Страсбург, 28 января 1981 года), страны, включенные в «Перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных» (утвержден Приказом Роскомнадзора от 15.03.2013 № 274), так и в прочие страны, может осуществляться Банком в целях выполнения поручений Клиента в соответствии с п. 1 настоящего Согласия.

6. Согласие даётся на срок, необходимый до достижения целей, указанных в п. 1, и может быть досрочно отозвано письменным запросом, направленным в адрес Оператора.

(подпись)

(_____)
(Фамилия И.О.)

(дата)