

**УТВЕРЖДАЮ**

**Представитель государственной корпорации  
«Агентство по страхованию вкладов»  
(Руководитель временной администрации  
АО Банк «Советский»)**

\_\_\_\_\_ **Ю.А. Тычинин**

**«26» февраля 2016 года**

**ПОЛИТИКА  
обработки и защиты персональных данных  
АО Банк «Советский»**

**Введена в действие Приказом от « 26 » февраля 2016 года № 126**

## 1. Общие положения

- 1.1. Настоящая «Политика обработки и защиты персональных данных АО Банк «Советский» (далее – Политика) разработана с целью установления основных принципов и подходов к обработке и обеспечению защиты персональных данных и определяет нормы АО Банк «Советский» (далее – Банк) в отношении обработки и обеспечения безопасности персональных данных сотрудников, клиентов и контрагентов Банка.
- 1.2. Настоящая Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и Стандарта ЦБР СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения» (принят и введен в действие распоряжением ЦБР от 17.05.2014 г. № Р-399) и иными нормативно-правовыми актами РФ.
- 1.3. В соответствии с Федеральным законом от 27.07.2006 г. №152 «О персональных данных» настоящая Политика должна размещаться на сайте Банка [www.sovbank.ru](http://www.sovbank.ru) в общем доступе, как документ, определяющий политику Банка в отношении обработки персональных данных субъектов персональных данных.

## 2. Термины, определения, сокращения

- 2.1. **Банк** – АО Банк «Советский».
- 2.2. **Информация** – сведения (сообщения, данные) независимо от формы их представления.
- 2.3. **Доступ к информации** – возможность получения информации и ее использования.
- 2.4. **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 настоящей политики оператором является Банк.
- 2.5. **Персональные данные (ПДн)** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).
- 2.6. **Субъект персональных данных (субъект ПДн)** – физическое лицо (клиент).
- 2.7. **Информационная система ПДн (ИСПДн)** – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.
- 2.8. **Обработка ПДн** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.
- 2.9. **Распространение ПДн** – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

- 2.10. **Предоставление ПДн** - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.
- 2.11. **Блокирование ПДн** – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).
- 2.12. **Уничтожение ПДн** – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.
- 2.13. **Обезличивание ПДн** – действия, в результате которых становится невозможно без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.
- 2.14. **РФ** – Российская Федерация.
- 2.15. **Федеральный закон 152-ФЗ** - Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

### **3. Категории субъектов персональных данных и цели обработки персональных данных**

- 3.1. Банк, как оператор ПДн, осуществляет обработку ПДн субъектов ПДн, полученных в установленном законодательством РФ порядке.
- 3.2. Банк осуществляет обработку ПДн следующих категорий субъектов ПДн:
  - 1) сотрудников Банка (в том числе кандидатов на вакантные должности);
  - 2) клиентов–физических лиц и их представителей;
  - 3) должностных лиц (представителей) клиентов–юридических лиц;
  - 4) должностных лиц (представителей) контрагентов Банка (партнеры, субподрядчики и пр.).
- 3.3. Обработка ПДн в ИСПДн осуществляется сотрудниками Банка в целях:
  - 1) осуществления банковских операций и иной деятельности, предусмотренной Уставом Банка, действующим законодательством РФ, нормативными актами Банка России;
  - 2) заключения, исполнения и прекращения договоров с физическими и юридическими лицами;
  - 3) организации кадрового учета сотрудников Банка и ведения кадрового делопроизводства.

### **4. Принципы обработки персональных данных**

- 4.1. Перечень ПДн, обрабатываемых в Банке, определен и утвержден локальными нормативными документами.
- 4.2. При обработке ПДн в Банке должны соблюдаться следующие принципы:
  - 1) законность целей и способов обработки ПДн;
  - 2) соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Банка;
  - 3) соответствие объема, характера, способов обработки ПДн целям обработки ПДн;

- 4) достоверность и актуальность ПДн;
- 5) достаточность ПДн для целей обработки;
- 6) недопустимость обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- 7) недопустимость объединения созданных для несовместимых между собой целей баз данных ИСПДн.

## **5. Организация защиты персональных данных**

- 5.1. Банк предпринимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн в соответствии с требованиями законодательства РФ в части обработки ПДн.
- 5.2. Организационные меры по защите ПДн включают в себя следующие меры безопасности:
  - 1) физическую защиту помещений, где производится обработка ПДн (пожарно-охранная сигнализация, внутриобъектовый режим, определение границ контролируемой зоны и т.д.);
  - 2) рациональное размещение рабочих мест сотрудников Банка, при котором исключается угроза утечки видовой информации;
  - 3) учет материальных носителей ПДн;
  - 4) знание и соблюдение сотрудниками Банка требований Федерального закона 152-ФЗ, локальных нормативных документов по защите ПДн в Банке;
  - 5) организацию регулярных проверок соблюдения сотрудниками Банка требований законодательства РФ и локальных документов Банка по защите ПДн;
  - 6) утверждение перечня уполномоченных лиц или подразделений ответственных за обеспечение защиты ПДн в Банке;
  - 7) разработка локальных нормативных актов, определяющие политику Банка в отношении обработки ПДн, а также иных документов, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, а также устранение последствий таких нарушений;
  - 8) осуществление внутреннего контроля и аудита соответствия обработки ПДн требованиям законодательства РФ и принятым в соответствии с ним нормативными актами, требованиям к защите ПДн, политикой Банка в отношении обработки ПДн и другими локальными актами;
  - 9) проведение оценки вреда, который может быть причинен субъектам ПДн данных в случае нарушения Федерального закона 152-ФЗ, соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом 152-ФЗ.
- 5.3. Технические меры по защите ПДн должны приниматься в соответствии с разработанной в Банке частной моделью угроз и включают в себя следующие меры безопасности:
  - 1) определение, выполнение и регистрация процедур контроля целостности и обеспечения доверенной загрузки программного обеспечения, в том числе

- программного обеспечения технических защитных мер, на средствах вычислительной техники, входящих в ИСПДн;
- 2) определение, выполнение, регистрация и контроль процедур доступа к эксплуатационной документации и архивным файлам, содержащим параметры настройки ИСПДн, в том числе настройки применяемых технических защитных мер;
  - 3) определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления ПДн;
  - 4) определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления программного обеспечения, в том числе программного обеспечения технических защитных мер, входящего в состав ИСПДн;
  - 5) идентификация и аутентификация устройств, используемых для осуществления доступа;
  - 6) размещение технических средств, предназначенных для администрирования ИСПДн, автоматизированных мест пользователей и серверных компонент ИСПДн в отдельных выделенных сегментах локальной вычислительных сетей;
  - 7) мониторинг сетевого трафика, выявление вторжений и сетевых атак и реагирование на них;
  - 8) определение, выполнение, регистрация и контроль процедур обновление сигнатурных баз технических защитных мер;
  - 9) определение, выполнение, регистрация и контроль процедур использования коммуникационных портов, устройств ввода-вывода информации, съемных машинных носителей и внешних накопителей информации;
  - 10) определение, выполнение, регистрация и контроль процедур доступа к архивам ПДн;
  - 11) организация защиты периметров сегментов локальной вычислительной сети, в которых расположены ИСПДн, и контроля информационного взаимодействия между сегментами локальной вычислительных сетей.

## **6. Права и обязанности субъекта персональных данных**

- 6.1. Субъект обязан предоставлять Банку достоверные сведения о себе и своевременно информировать Банк об изменении своих ПДн.
- 6.2. Банк проверяет достоверность сведений, сверяя данные предоставленные субъектом с имеющимися у субъекта документами.
- 6.3. Предоставление субъектом ПДн подложных документов или ложных сведений является основанием для расторжения договора между Банком и субъектом.
- 6.4. Сведения о ПДн должны быть предоставлены субъектом в письменном виде, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн.
- 6.5. Передача информации, содержащей ПДн субъектов, по телефону, факсу, электронной почте без письменного согласия субъекта недопустима.
- 6.6. Субъект имеет право на получение информации, касающейся обработки его ПДн, в том числе:
  - 1) подтверждения факта обработки ПДн Банком;

- 2) правовых оснований и целей обработки ПДн;
  - 3) способов, применяемых Банком для обработки ПДн;
  - 4) наименование и место нахождения Банка, сведения о лицах (за исключением сотрудников Банка), которые имеют доступ к ПДн или которым может быть предоставлен такой доступ на основании договора или в соответствии с действующим законодательством РФ;
  - 5) перечень обрабатываемых ПДн, относящихся к соответствующему субъекту, и источник их получения, если иной порядок представления таких данных не предусмотрен законодательством РФ;
  - 6) сроков обработки ПДн, в том числе сроков их хранения;
  - 7) информации об осуществленной или о предполагаемой трансграничной передаче данных;
  - 8) наименование и адрес юридического лица, осуществляющего обработку ПДн по поручению Банка, если обработка поручена или будет поручена такому лицу.
- 6.7. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с действующим законодательством РФ, в том числе если доступ субъекта к его ПДн нарушает права и законные интересы третьих лиц.
- 6.8. Субъект вправе требовать от Банка уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или если не являются необходимыми для заявленных Банком целей обработки.
- 6.9. Субъект вправе требовать извещения Банком всех лиц, которым ранее были сообщены неверные или неполные ПДн субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.
- 6.10. Согласие на обработку ПДн может быть отозвано субъектом по его письменному запросу.
- 6.11. Субъект вправе обжаловать любые неправомерные действия или бездействие Банка при обработке и защите его ПДн в соответствии с законодательством РФ.

## **7. Права и обязанности Банка**

- 7.1. Банк и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством РФ.
- 7.2. Банк имеет право:
- 1) отстаивать свои интересы в суде;
  - 2) предоставлять ПДн субъектов третьим лицам, если это предусмотрено действующим законодательством РФ;
  - 3) поручить обработку ПДн другому лицу с согласия субъекта ПДн, на основании заключаемого с этим лицом договора;
  - 4) отказать в предоставлении ПДн в случаях предусмотренных законодательством РФ;
  - 5) продолжить обработку ПДн субъекта без его согласия, если обработка ПДн необходима для исполнения (заключения) договора, сторонами которого

являются субъект ПДн и Банк, а также иных случаях предусмотренных законодательством РФ.

- 7.3. Обработка ПДн субъекта должна осуществляться исключительно в целях обеспечения соблюдения законодательства РФ, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, исполнения условий договора с клиентами Банка.
- 7.4. В бизнес-процессах Банка не должно быть решений, принимаемых на основании исключительно автоматизированной обработки ПДн и порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных п.7.5. настоящей Политики.
- 7.5. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных законодательством РФ, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.
- 7.6. В случае изменения сведений, указанных в уведомлении уполномоченного органа по защите прав субъектов ПДн об обработке Банком ПДн, Банк обязан уведомить об этих изменениях уполномоченный орган по защите прав субъектов ПДн.
- 7.7. Банк вправе осуществлять обработку ПДн без уведомления уполномоченного органа по защите прав субъектов ПДн, если эта обработка ПДн связана с заключением договора, стороной которого является субъект ПДн, если ПДн не распространяются, а также не предоставляются третьим лицам без согласия субъекта и используются Банком исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн.

## **8. Ответственность**

- 8.1. Нарушение норм, регулирующих получение, обработку и защиту ПДн может повлечь гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством РФ.
- 8.2. Сотрудники Банка, нарушающие требования настоящей Политики несут персональную ответственность в соответствии с Трудовым Кодексом РФ.