«Согласовано»
Председатель Правления
ООО Банка «Саратов»

_____И.Ю. Мумлева
«11 » июля 2014г.

«Утверждено»
Протокол Совета директоров Банка
От « 11 » июля 2014г.
Председатель Совета директоров Банка
« 11» июля 2014г.
_____И.В. Жидкова

Политика в отношении обработки и защиты персональных данных в ООО Банк «Саратов»

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с Федеральным законом «О персональных данных» (далее – Федеральный закон) и устанавливает единый порядок (принципы, цели, условия и способы обработки) обработки персональных данных в ООО Банк «Саратов» (далее по тексту – Банк), а также требования к защите персональных данных.

1.2. Политика разработана с учетом требований Конституции Российской Федерации, законодательных и иных нормативно правовых актов Российской Федерации в области персональных данных.

1.3. Положения политики обязательны для выполнения всеми сотрудниками Банка и служат основой для разработки нормативных документов, регламентирующих в Банке вопросы обработки персональных данных работников и иных субъектов персональных данных.

1.4. Банк является оператором персональных данных.

1.5. В целях настоящей Политики используются следующие термины и определения:

- **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- **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;
- **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;
- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
- **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- **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;
- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
- **обработка персональных данных**, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной **без использования средств автоматизации** (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека

2. Законодательные и иные нормативные акты, использованные при разработке Политики и поддерживающие ее

2.1. Конституция Российской Федерации.

2.2. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

2.3. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ.

2.4. Постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

2.5. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

2.6. Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

2.7. Приказ Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных" (вместе с "Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ").

2.8. Иные нормативные акты Российской Федерации и уполномоченных органов государственной власти.

2.9. В целях реализации положений политики в Банке изданы следующие нормативные документы:

2.9.1. положение об обработке персональных данных в ООО Банк «Саратов»,

2.9.2. политика информационной безопасности ООО Банк «Саратов»,

2.9.3. регламент реагирования на обращения субъектов персональных данных и надзорных органов в сфере обработки персональных данных в ООО Банке «Саратов»,

2.9.4. оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом,

2.9.5. приказы, регламентирующие доступ сотрудников к персональным данным и определяющие места хранения материальных носителей персональных данных,

2.9.6. иные документы, регламентирующие в Банке вопросы обращения с персональными данными.

3. Состав обрабатываемых персональных данных

3.1. Банк обрабатывает персональные данные следующих категорий субъектов:

- сотрудников Банка;
- персональные данные клиентов физических лиц;
- персональные данные руководителей контрагентов Банка;
- персональные данные руководителей и участников аффинированных лиц;
- персональные данные клиентов юридических лиц и индивидуальных предпринимателей - руководителей, участников и учредителей;
- иные субъекты персональных данных, сведения о которых необходимы для выполнения действующего законодательства.

4. Перечень персональных данных

4.1. Перечень персональных данных обрабатываемых в Банке определяется требованиями законодательства Российской Федерации и нормативными актами Банка с учетом целей обработки персональных данных определенных в данном документе.

4.2. Обработка специальных категорий данных, определенных в Федеральном законе, в Банке не осуществляется.

5. Основные принципы и цели обработки персональных данных

5.1. Информация, относящаяся к персональным данным, ставшая известной Банку является защищаемой, конфиденциальной информацией и охраняется Федеральным законом.

5.2. Обработка персональных данных осуществляется на законных основаниях в соответствии с принципами справедливости и добросовестности.

5.3. Обработка персональных данных в Банке ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

5.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

5.5. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Банк обеспечивается точность, достаточность и актуальность ПДн по отношению к целям их обработки, а также не допускается избыточность обрабатываемых ПДн по отношению к заявленным целям их обработки.

5.6. Хранение персональных данных осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные уничтожаются либо

обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.7. Банк осуществляет с персональными данными следующие действия:

- обработка с использованием средств автоматизации,
- обработка без использования таких средств,
- смешанная обработка.

Обработка включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.8. Банк осуществляет обработку персональных данных в следующих целях:

- обеспечение соблюдения законодательных и иных правовых актов Российской Федерации;
- осуществление функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Банк;
- заключение, исполнение и прекращение договоров гражданско-правового характера с физическими, юридическими лицами и индивидуальными предпринимателями и иными лицами в случаях, предусмотренных действующим законодательством Российской Федерации и нормативными актами Банка;
- регулирование трудовых отношений с сотрудниками Банка;
- обеспечение контрольно пропускного режима на объектах Банка;
- формирование внутренних справочно-информационных материалов (телефонного справочника, списка пользователей автоматизированных систем и т.д.) обеспечивающих деятельность Банка;
- осуществление прав и законных интересов Банка в рамках осуществления своей деятельности;
- исполнение судебных актов или актов других органов и должностных лиц подлежащих исполнению в рамках действующего законодательства Российской Федерации;
- иные законные цели.

6. Условия обработки персональных данных

6.1. До начала обработки персональных данных Банк обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

6.2. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, составленного по форме утвержденной Банком или в случаях, когда согласие не требуется согласно Федеральному закону,
- после принятия необходимых мер по защите персональных данных.

6.3. Передача персональных данных третьим лицам возможна только с согласия субъекта персональных данных или согласно требованию, налагаемому на Банк действующим законодательством.

6.4. В случае если Банк поручает обработку или передает персональные данные субъекта третьему лицу на основании договора, заключаемого с этим лицом. Существенными пунктами этого договора будут являться:

- соблюдение третьим лицом принципов и правил обработки персональных данных закрепленных в Федеральном законе,
- определение перечня действий (операций) с персональными данными, которые будут совершаться третьим лицом,

- обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке,
- указание требований к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона.

6.5. Доступ к персональным данным субъектов предоставляется сотрудникам Банка в соответствии с их должностными обязанностями на основании приказа Председателя Правления.

6.6. Сотрудники Банка и иные лица, получившие доступ к обрабатываемым персональным данным, предупреждаются о возможной дисциплинарной, административной, гражданско–правовой или уголовной ответственности в случае нарушения норм и требований действующего законодательства, регулирующего правила обработки и защиты персональных данных.

7. Права субъектов персональных данных

7.1. Субъект персональных данных имеет право на:

- получение информации касающейся обработки его персональных данных предусмотренной Федеральным законом, в случае если иное не предусмотрено Федеральным законодательством;
- требование уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принятие предусмотренных законом мер по защите своих прав;
- отзыв согласия на обработку персональных данных, если такое согласие давалось;
- обжаловать действия или бездействие Банка в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных считает, что обработка его персональных данных осуществляется с нарушением требований настоящего Федерального закона или иным образом нарушаются его права и свободы;
- осуществление иных прав предусмотренных законодательством Российской Федерации.

8. Меры по обеспечению защиты персональных данных

8.1. Оператор предпринимает необходимые организационные и технические меры по защите персональных данных.

8.2. Принимаемые меры основаны на требованиях:

- ст. 18.1, ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»,
- постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
- постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных",
- приказа ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных",
- нормативных документах Банка России, в области защиты информации, в том числе персональных данных.

8.2.1. В частности:

а. Назначены лица, ответственные за организацию обработки и обеспечение безопасности персональных данных.
б. Разработаны, внедрены и соблюдаются Политика информационной безопасности ООО Банк «Саратов» и другие локальные нормативные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.
в. Лица, ведущие обработку персональных данных, инструктируются и знакомятся с нормативными правовыми актами, регламентирующими порядок работы и защиты персональных данных.
г. Сотрудникам запрещается передавать или иным способом разглашать персональные данные, к которым они имеют доступ, кроме случаев, регламентированных Федеральным законом.
д. Разграничены права доступа к обрабатываемым персональным данным.
е. Определены места хранения материальных носителей персональных данных и соблюдаются условия, исключающие несанкционированный доступ к персональным данным.
ж. Обеспечено раздельное хранение материальных носителей персональных данных, обработка которых ведется в различных целях.
з. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям проводятся периодические проверки условий обработки персональных данных.
и. Проводится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом.
к. В качестве модели угроз принята отраслевая модель угроз и нарушителей информационной безопасности организаций банковской системы Российской Федерации.
л. Применяются прошедшие в установленном порядке процедуру оценки соответствия средств защиты информации.
м. Проводится учет машинных носителей персональных данных.
н. Помимо вышеуказанных мер, осуществляются меры технического характера, направленные на:
- предотвращение несанкционированного доступа к системам, в которых хранятся персональные данные;
- резервирование и восстановление персональных данных работоспособности технических средств и программного обеспечения, средств защиты информации в информационных системах персональных данных модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- иные необходимые меры безопасности.

9. Внутренний контроль соответствия обработки персональных данных требованиям Федерального закона, принятым в соответствии с ним нормативным правовым актам и внутренним нормативным документам Банка.

9.1. Контроль за соблюдением в Банке требований законодательства Российской федерации и локальных нормативных документов в области персональных данных (в том числе защиты персональных данных) осуществляется с целью:
- проверки соответствия обработки персональных данных законодательству Российской Федерации и локальным нормативным документам Банка в области персональных данных,

- принятия мер, направленных на предотвращение и выявление нарушений законодательства в области персональных данных, выявление возможных каналов несанкционированного доступа к персональным данным и устранение последствий подобных нарушений.

9.2. Внутренний контроль соблюдения сотрудниками Банка требований законодательства Российской Федерации и локальных нормативных документов в области персональных данных, в том числе защиты персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных в Банке.

9.3. Внутренний контроль соответствия обработки персональных данных требованиям Федерального закона, принятых в соответствии с ним нормативно правовых актов и локальных нормативных документов в области персональных данных осуществляет Служба внутреннего контроля.

9.4. Персональная ответственность за соблюдение требований законодательства Российской Федерации и локальных нормативных документов в области персональных данных, в том числе защиты персональных данных, в структурном подразделении Банка возлагается на руководителя данного структурного подразделения или лицо его замещающее.

10. Сроки хранения персональных данных

10.1. Сроки хранения персональных данных определяются исходя из:

- Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 23.07.2013) "О персональных данных".
- Федерального закона от 07.08.2001 N 115-ФЗ (ред. от 05.05.2014) "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма".
- Приказа Минкультуры России от 25.08.2010 N 558 "Об утверждении "Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения".
- Договора, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.
- Иных нормативно правовых актов, регламентирующих сроки хранения информации.

10.2. Персональные данные с истекшим сроком хранения подлежат уничтожению либо обезличиванию (в соответствии с методиками разрабатываемыми уполномоченным органом по защите прав субъектов персональных данных).

10.3. В Банке назначается комиссия, ответственная за уничтожение архивных документов, в том числе содержащих персональные данные.

10.4. Персональные данные с истекшим сроком хранения уничтожаются или обезличиваются в срок, не превышающий тридцати дней с момента истечения срока хранения.

10.5. Если персональные данные с истекшим сроком хранения не возможно уничтожить или обезличить в срок тридцать дней, то данные блокируются и их уничтожение или обезличивание обеспечивается в срок шесть месяцев.

10.6. Материальные носители персональных данных, обрабатываемых без использования средств автоматизации и с истекшим сроком хранения, подлежат хранению в выделенном месте архива банка и уничтожению вместе с другими архивными документами в срок не превышающий шести месяцев.

11. Лицо, ответственное за организацию обработки персональных данных в Банке.

11.1. Лицом, ответственным за организацию обработки персональных данных в Банке, является администратор информационной безопасности.

11.2. Лицо, ответственное за организацию обработки персональных данных в Банке получает указания и подотчетно Председателю Правления Банка.

11.3. Лицо, ответственное за организацию обработки персональных данных в Банке наделяется всеми необходимыми правами для выполнения своих обязанностей, оговоренными в Федеральном законе.

11.4. Лицо, ответственное за организацию обработки персональных данных в Банке обязано:

- осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных путем проведения обучений;
- организовывать прием обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

12. Публикация документа, определяющего политику Банка в отношении обработки персональных данных.

Настоящая политика подлежит публикации на официальном сайте Банка в разделе «Раскрываемая информация» в течение семи рабочих дней после утверждения Советом директоров Банка.