

УТВЕРЖДЕНО
Правлением ОАО АКБ «ИТ Банк»
Председателем Правления
ОАО АКБ «ИТ Банк»

_____ **О.А. Сильнягин**

« ____ » _____ **2015 г.**

**Политика ОАО АКБ «ИТ Банк» в отношении обработки
персональных данных**

Общие положения

Политика ОАО АКБ «ИТ Банк» (далее - Банк) в отношении обработки персональных данных (далее - Политика) определяет порядок, условия обработки персональных данных и реализацию требований по их защите в ОАО АКБ «ИТ Банк».

Законодательной основой настоящей Политики является Конституция Российской Федерации, Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», федеральные законы, Указы Президента Российской Федерации, постановления Правительства Российской Федерации, другие нормативные правовые акты в области обработки и обеспечения безопасности персональных данных, а также руководящие документы ФСТЭК России и ФСБ России.

В настоящей Политике используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Персональные данные являются конфиденциальной информацией.

Обеспечение необходимого и достаточного уровня безопасности персональных данных и другой конфиденциальной информации является важнейшим условием деятельности Банка.

Принципы обработки персональных данных

Обработка персональных данных осуществляется Банком на законной и справедливой основе.

При обработке персональных данных Банком соблюдаются следующие принципы:

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей; не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки; не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность

по отношению к целям обработки персональных данных; принимаются необходимые меры по удалению или уточнению неполных или неточных данных;

- хранение персональных данных осуществляется 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.

Персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не предусмотрено федеральным законом.

Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Сроки обработки персональных данных определяются в соответствии требованиями законодательства РФ и нормативными документами Банка России.

Сроки хранения документов, в том числе электронных документов, содержащих персональные данные, определяются в соответствии требованиями законодательства РФ и нормативными документами Банка России.

Порядок уничтожения документов, содержащих персональные данные определены Инструкцией по делопроизводству.

Порядок обработки персональных данных

Обработка персональных данных осуществляется на основании условий, определенных законодательством Российской Федерации.

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, по собственной воле и в своих интересах. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Банком.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Банк вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, предусмотренных законодательством РФ.

Персональные данные относятся к охраняемой информации, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, кроме случаев:

- обезличивания, когда невозможно определить принадлежность персональных данных к конкретному субъекту;
- общедоступности, когда доступ к данным неограниченного круга лиц предоставлен с согласия субъекта.

Полученные Банком персональные данные хранятся на следующих видах носителей:

- бумажные носители;
- электронные носители (в том числе автоматизированные информационные системы).

Доступ к бумажным и электронным носителям персональных данных субъектов получают только те работники Банка, которым это необходимо для выполнения их должностных обязанностей.

Банк за свой счет обеспечивает необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

При передаче персональных данных Банк должен соблюдать следующие требования:

- не передавать персональные данные третьей стороне без согласия субъекта, за исключением случаев, предусмотренных законодательством РФ;
- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, осуществляется только в случаях наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных; исполнения договора, стороной которого является субъект персональных данных, а также в иных предусмотренных законодательством случаях.

Автоматизированная обработка персональных данных осуществляется в информационных системах персональных данных. Защита персональных данных в информационных системах банка производится согласно действующему законодательству в соответствии с классификацией ИСПДн.

Обеспечение безопасности персональных данных

Для защиты персональных данных в Банке применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований по защите персональных данных:

- используются шифровальные (криптографические) средства защиты информации, средства от несанкционированного доступа, выполняются процедуры определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- обеспечивается защита информации с применением прошедших процедуру оценки соответствия средств защиты информации;
- проводится оценка эффективности принимаемых мер по обеспечению безопасности персональных данных; обеспечивается выявление фактов несанкционированного доступа к персональным данным и принятие соответствующих мер, а также восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- реализован механизм разграничения прав доступа к персональным данным, обрабатываемым в информационной системе, а также регистрация и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- обеспечивается контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровню защищенности информационных систем.

В качестве мер по организационной и технической защите информации внедрены и применяются средства минимизации полномочий доступа, средства разграничения доступа (идентификация и аутентификация субъектов доступа, ограничения количества неудачных попыток доступа), протоколирование фактов доступа к персональным данным и другие меры защиты.

Заключительные положения

Настоящая Политика является внутренним документом Банка, доступным для ознакомления субъектам персональных данных.

Ответственность должностных лиц Банка, имеющих доступ к персональным данным за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с действующим законодательством РФ.

Сведения об ОАО АКБ «ИТ Банк», как об операторе, осуществляющем обработку персональных данных, внесены в Реестр операторов, осуществляющих обработку персональных данных, под регистрационным номером 11-0210941, дата внесения записи - 18 июля 2011 года.