АО «АБ «РОССИЯ»

УТВЕРЖДЕНО

решением Правления
АО «АБ «РОССИЯ»
протокол от «9» января 2017г. № 792,
с изменениями, утвержденными
решением Правления АО «АБ РОССИЯ»
от «7» августа 2018 г. № 01-08/18

ПОЛИТИКА
обработки персональных данных
в АО «АБ «РОССИЯ»

Санкт-Петербург
Версия 1.1

2018

Содержание

1. Общие положения

1.1. Настоящая «Политика обработки персональных данных в АО «АБ «РОССИЯ» (далее – Политика) определяет основные принципы обработки и обеспечения защиты персональных данных физических лиц в АО «АБ «РОССИЯ» (далее – Банк) и является обязательной для выполнения всеми работниками Банка.

1.2. Целью разработки настоящей Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в Банке.

1.3. Действие Политики распространяется на все процессы Банка, связанные с обработкой персональных данных.

1.4. Политика разработана в соответствии законодательством Российской Федерации о персональных данных, в том числе в соответствии с требованиями следующих федеральных законов Российской Федерации и иных нормативно-правовых актов, регламентирующих обработку персональных данных:

- Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.5. В Политике используются следующие термины и определения:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

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;

Общедоступные персональные данные – персональные данные, доступ к которым предоставлен субъектом персональных данных неограниченному кругу лиц и на которые не распространяются требования о конфиденциальности;

Ответственный за организацию обработки персональных данных – работник Банка, назначенный распорядительным актом Председателя Правления Банка ответственным за осуществление внутреннего контроля за соблюдением требований законодательства Российской Федерации о персональных данных, организацию приема и обработки обращений и запросов субъектов персональных данных, доведение до сведений работников Банка законодательства Российской Федерации и внутренних документов Банка о персональных данных;

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

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.

1.6. Персональные данные являются конфиденциальной информацией, охраняемой в соответствии с действующим законодательством Российской Федерации и внутренними документами Банка, регламентирующими его действия по защите конфиденциальной информации.

2. Категории субъектов персональных данных и состав обрабатываемых персональных данных

2.1. При осуществлении деятельности Банк обрабатывает персональные данные следующих категорий субъектов персональных данных:

- работников Банка (персональные данные, необходимые Банку в связи с трудовыми отношениями и касающиеся конкретного работника);
- кандидатов на работу в Банке (персональные данные, необходимые Банку для принятия решения о соответствии кандидата, установленным законодательством Российской Федерации и Банком требованиям);
- работников Банка, с которыми прекращены трудовые отношения (персональные данные, обработку которых Банк обязан осуществлять в случаях, установленных законодательством Российской Федерации, после прекращения трудового договора с работником);
- аффилированных лиц, инсайдеров или руководителей, участников (акционеров) или работников юридического лица, являющихся аффилированными лицами по отношению к Банку (персональные данные, необходимые Банку для осуществления банковской деятельности, в том числе для отражения в отчетных документах о деятельности Банка в соответствии с требованиями действующего законодательства Российской Федерации);
- клиентов Банка, а также руководителей, участников (акционеров) или работников юридических лиц, являющихся клиентами Банка (персональные данные, необходимые Банку для выполнения своих обязательств в рамках договорных отношений с клиентом и требований законодательства Российской Федерации);

- потенциальных клиентов, контрагентов, заемщиков (персональные данные, необходимые Банку в целях рассмотрения вопросов о заключении договоров, проведения операций и сделок с потенциальным клиентом, контрагентом, заемщиком и исполнения требований законодательства Российской Федерации);
- представителей клиентов, выгодоприобретателей, бенефициарных владельцев (персональные данные, необходимые Банку для выполнения своих обязательств в рамках договорных отношений с клиентом и требований законодательства Российской Федерации);
- залогодателей, поручителей (персональные данные, необходимые Банку для выполнения обязательств в рамках договорных отношений и требований законодательства Российской Федерации);
- иных лиц, давших согласие Банку на обработку своих персональных данных либо сделавших свои персональные данные общедоступными, а также лиц, персональные данные которых Банк обрабатывает без согласия субъектов персональных данных в случаях, предусмотренных законодательством Российской Федерации.

3. Цели обработки персональных данных

3.1. Целями обработки персональных данных в Банке являются:

- осуществление банковских операций и иной деятельности, предусмотренной Уставом и лицензиями Банка, действующим законодательством Российской Федерации, в том числе:
  - Федеральным законом от 02.12.1990 № 395-1 «О банках и банковской деятельности»,
  - Федеральным законом от 30.12.2004 № 218-ФЗ «О кредитных историях»,
  - Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»,
  - Федеральным законом от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле»,
  - Федеральным законом от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг»,
  - Федеральным законом от 23.12.2003 № 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации»,
  - Федеральным законом от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;
- заключение, исполнение, изменение и прекращение гражданско-правовых договоров с физическими, юридическими лицами, индивидуальными предпринимателями, физическими лицами, занимающимися в установленном законодательством Российской Федерации порядке частной практикой, и иными лицами, в случаях, предусмотренных действующим законодательством Российской Федерации и Уставом Банка;
- организация кадрового учета и кадрового делопроизводства в Банке, обеспечение соблюдения трудового законодательства Российской Федерации;
- исполнение требований налогового законодательства Российской Федерации в связи с исчислением и уплатой налога на доходы физических лиц.

4. Основные принципы обработки персональных данных

4.1. Основные принципы обработки персональных данных:

- законность и справедливость целей и способов обработки персональных данных;
- безопасность обработки персональных данных, минимизация риска нанесения ущерба субъекту персональных данных;
- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Банка;
- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- недопустимость объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;
- хранение персональных данных в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели их обработки, если срок хранения персональных данных не установлен федеральным законом либо договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- уничтожение либо обезличивание по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении, если иное не предусмотрено федеральным законом.

4.2. Работники Банка, обрабатывающие персональные данные, обязаны:

- знать и исполнять требования законодательства Российской Федерации, внутренние документы Банка, регламентирующие обработку персональных данных;
- обрабатывать персональные данные только в рамках выполнения своих служебных обязанностей;
- не разглашать персональные данные, обрабатываемые в Банке;
- сообщать о действиях других лиц, которые могут привести к нарушению положений настоящей Политики;
- сообщать Ответственному за организацию обработки персональных данных о фактах нарушения требований законодательства Российской Федерации, настоящей Политики и внутренних документов Банка о персональных данных.

5. Обработка персональных данных

5.1. Обработка персональных данных осуществляется в Банке только с согласия субъекта персональных данных (законного представителя субъекта персональных данных) за исключением установленных Федеральным законом «О персональных данных» случаев, в том числе указанных в п. 5.2 настоящей Политики.

5.2. Согласие субъекта персональных данных на обработку персональных данных не требуется в следующих случаях:

5.2.1. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей;

5.2.2. 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;

5.2.3. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

5.2.4. Осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе

(далее – персональные данные, сделанные общедоступными субъектом персональных данных);

5.2.5. Обработка персональных данных необходима для осуществления прав и законных интересов Банка или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

5.2.6. Обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.

5.3. Формы письменного согласия об обработке персональных данных соответствуют требованиям Федерального закона «О персональных данных», и утверждаются Банком.

5.4. Достоверность и актуальность сведений представленных субъектом персональных данных (законным представителем субъекта персональных данных) проверяется работником Банка путем сверки с информацией, содержащейся в оригиналах документов или их копиях, заверенных в установленном законодательством Российской Федерации порядке.

5.5. Обработка персональных данных в Банке осуществляется с использованием средств автоматизации и без использования средств автоматизации.

5.6. Банк вправе передать обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, на основании договора, заключаемого с этим лицом, обязательным условием которого является соблюдение этим лицом требований Федерального закона «О персональных данных».

5.7. Персональные данные не раскрываются третьим лицам и не распространяются иным образом без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

5.8. Предоставление доступа к персональным данным представителям органов государственной власти осуществляется в порядке и объеме, установленном законодательством Российской Федерации.

5.9. Банк может осуществлять трансграничную передачу персональных данных в соответствии с Федеральным законом «О персональных данных» и иными федеральными законами.

5.10. Хранение Банком персональных данных осуществляется не дольше, чем того требует достижение цели обработки, если срок хранения персональных данных не установлен федеральным законом или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.11. Обрабатываемые персональные данные подлежат уничтожению или обезличиванию по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6. Права субъекта персональных данных

6.1. Субъект персональных данных имеет право:

6.1.1. Получать информацию, касающуюся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Банком,
- правовые основания и цели обработки персональных данных,

- цели и применяемые Банком способы обработки персональных данных,
- наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона,
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом,
- сроки обработки персональных данных, в том числе сроки их хранения,
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»,
- информацию об осуществленной или о предполагаемой трансграничной передаче данных,
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка поручена или будет поручена такому лицу,
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами;

6.1.2. Требовать от Банка уточнения его 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;

6.1.3. Отозвать согласие на обработку персональных данных (при этом Банк вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Федеральном законе «О персональных данных»).

6.2. Право на доступ субъекта персональных данных к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

– обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
– доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

7. Обязанности Банка

7.1. При обработке персональных данных Банк обязан:

7.1.1. Предоставить субъекту персональных данных по его просьбе информацию, указанную в пп. 6.1.1 настоящей Политики;

7.1.2. Разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные в случае, если предоставление персональных данных является обязательным в соответствии с федеральным законом;

7.1.3. Предоставить субъекту персональных данных, если персональные данные получены не от субъекта персональных данных, за исключением случаев, указанных в п. 7.2 настоящей Политики, до начала обработки таких персональных данных, информацию, указанную в п. 3 ст. 18 Федерального закона «О персональных данных»;

7.1.4. Обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, при сборе персональных данных, в том числе в сети Интернет, за исключением случая, указанного в пп. 5.2.1 настоящей Политики.

7.2. Банк освобождается от обязанности предоставить субъекту персональных данных сведения, указанные в пп. 7.1.3 настоящей Политики, в случаях, если:
- субъект персональных данных уведомлен об осуществлении обработки его персональных данных Банком;
- персональные данные получены Банком на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- предоставление субъекту персональных данных сведений, предусмотренных пп. 7.1.3 настоящей Политики, нарушает права и законные интересы третьих лиц.

8. Обеспечение безопасности обработки персональных данных

8.1. В целях обеспечения безопасности обработки персональных данных Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, установленных законодательством Российской Федерации о персональных данных.

8.2. Основными мерами защиты персональных данных, используемыми Банком, являются:
- назначение Ответственного за организацию обработки персональных данных;
- ограничение и контроль состава лиц, имеющих доступ к персональным данным;
- ознакомление работников Банка с требованиями законодательства Российской Федерации по обработке и защите персональных данных, а также обучение безопасной работе со средствами вычислительной техники;
- организация режима обеспечения физической безопасности помещений, носителей информации и оборудования;
- управление и контроль доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- регистрация и учёт событий в информационных системах, обрабатывающих персональные данные;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- обеспечение антивирусной защиты;
- защита информационных систем от атак;
- обеспечение возможности восстановления модифицированных или уничтоженных персональных данных с резервных носителей;
- осуществление периодического контроля достаточности и полноты реализации защитных мер;
- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Банка в отношении обработки персональных данных, а также локальным актам Банка;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных.

8.3. Меры по обеспечению безопасности персональных данных при их обработке устанавливаются в соответствии с требованиями законодательства Российской Федерации о защите персональных данных, разрабатываемыми Банком моделями угроз для информационных систем персональных данных, а также локальными нормативными актами Банка, регламентирующими вопросы обеспечения безопасности персональных данных.

9. Заключительные положения

9.1. Контроль исполнения требований настоящей Политики осуществляется Ответственным за организацию обработки персональных данных.

9.2. Банк и его работники несут установленную законодательством Российской Федерации ответственность за нарушение Федерального закона «О персональных данных».

9.3. Настоящая Политика размещается на официальном сайте Банка в сети Интернет.

9.4. Внесение необходимых изменений, дополнений в настоящую Политику осуществляется в случаях изменения законодательства Российской Федерации о персональных данных, но не реже чем один раз в три года.

9.5. По вопросам обработки и защиты информации необходимо обращаться:

9.5.1. Адрес: 191124, Россия, Санкт-Петербург пл. Растрелли. д. 2, лит. А;

9.5.2. Телефон: (812) 335-85-00, 8-800-100-11-11;

9.5.3. Официальный адрес электронной почты: bank@abr.ru.