УТВЕРЖДЕНА
решением Совета директоров
АКБ «ПРОМИНВЕСТБАНК» (ПАО)
19.04.2018
Протокол № 4

Председатель Совета директоров

П.Е. Брянских

ПОЛИТИКА
в отношении обработки персональных данных
в АКБ «ПРОМИНВЕСТБАНК» (ПАО)

г. Москва, 2018 год

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика в отношении обработки персональных данных (далее - Политика) определяет правила, требования и принципы обеспечения безопасности персональных данных в АКБ «ПРОМИНВЕСТБАНК» (ПАО) (далее - Банк).

Настоящая Политика разработана в соответствии с действующим законодательством Российской Федерации и нормативными актами банка России, в том числе:

- Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» (с изменениями и дополнениями).
- Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Стандартом Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы российской федерации. Общие положения».

Важнейшим условием реализации целей деятельности Банка, является обеспечение необходимого и достаточного уровня безопасности конфиденциальной информации, в том числе персональных данных и банковских технологических процессов, в рамках которых они обрабатываются.

Обеспечение безопасности персональных данных является одной из приоритетных задач Банка.

Банк при обработке персональных данных принимает 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 обеспечении безопасности персональных данных, обрабатываемых как в информационных системах персональных данных, так и в иных автоматизированных банковских системах, в которых персональные данные обрабатываются совместно с другими сведениями ограниченного доступа, Банк ориентируется на законодательство Российской Федерации в сфере обработки и защиты персональных данных и комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

Обработка и обеспечение безопасности информации, отнесенной к персональным данным в Банке позволяет обеспечить защиту персональных данных, обрабатываемых как в информационных системах персональных данных, т.е. в системах, целью создания которых является обработка персональных данных и к защите которых требования и рекомендации по обеспечению безопасности персональных данных предъявляют Федеральная служба безопасности Российской Федерации (ФСБ России), Федеральная служба по техническому и экспортному контролю (ФСТЭК России), так и в иных информационных системах, в которых персональные данные обрабатываются совместно с информацией, защищаемой в соответствии с требованиями, установленными для этой информации (режим защиты сведений, составляющих банковскую тайну, коммерческую тайну и др.).

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная банковская система (АБС) - автоматизированная система, реализующая банковский технологический процесс.

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (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.

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

3. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Сведениями, составляющими персональные данные, в Банке является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

3.2. Состав персональных данных, подлежащих защите в Банке, формируется в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и другими нормативными документами.

3.3. В Банке осуществляется обработка следующих категорий субъектов персональных данных:

- персональные данные Клиента (потенциального Клиента, партнера, контрагента), а также персональные данные руководителя, представителя, бенефициарного владельца Клиента, участника (акционера) или сотрудника юридического лица, являющегося Клиентом (потенциальным Клиентом, партнером, контрагентом) Банка — информация, необходимая Банку для выполнения своих обязательств в рамках договорных отношений с Клиентом и для выполнения требований законодательства Российской Федерации;
- персональные данные Заемщика (залогодателя, поручителя, принципала)/потенциального Заемщика (залогодателя, поручителя, принципала), а также персональные данные руководителя, представителя, бенефициарного владельца, участника (акционера) или сотрудника юридического лица, являющегося Заемщиком (залогодателем, поручителем, принципалом)/потенциальным Заемщиком (залогодателем, поручителем, принципалом) — информация, необходимая Банку для выполнения своих договорных обязательств и осуществления прав в рамках соответствующего договора, заключенного с Заемщиком (залогодателем, поручителем, принципалом), для минимизации рисков Банка, связанных с нарушением обязательств по кредитному договору (договору залога, договору поручительства, договору о предоставлении банковской гарантии и др.) и для выполнения требований законодательства Российской Федерации;
- персональные данные работника Банка — информация, необходимая Банку в связи с трудовыми отношениями и касающаяся конкретного работника.

4. ЦЕЛИ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Банк осуществляет обработку персональных данных в следующих целях:

- рассмотрение возможности совершения банковских операций и/или сделок (получение кредита, размещение депозита и т.д.) в соответствии с лицензией Банка России, выданной Банку;
- предоставление отчетности государственным надзорным органам в соответствии с требованиями действующего законодательства Российской Федерации;
- заключение и исполнение договоров с клиентами/контрагентами Банка и/или реализация совместных проектов;
- проведение мероприятий по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- формирование данных о кредитной истории;
- проведение мероприятий по урегулированию заявлений, претензий, сообщений клиентов по вопросам качества обслуживания, предоставления продуктов;
- обеспечение пропускного режима на объектах Банка;

- рассмотрение возможности заключения трудового соглашения/договора с субъектом персональных данных;
- регулирование трудовых (гражданско-правовых) отношений субъекта персональных данных с Банком (обеспечение соблюдения законов и иных нормативных правовых актов, содействие работникам в трудоустройстве, обучении и продвижении по службе, обеспечение личной безопасности работников);
- рассмотрение возможности установления договорных отношений с субъектом персональных данных по его инициативе с целью дальнейшего предоставления финансовых и иных услуг путем заключения договора, одной из сторон которого, либо выгодоприобретателем по которому является субъект персональных данных;
- осуществление функций, полномочий и обязанностей, возложенных на Банк действующим законодательством Российской Федерации.

4.2. Обработка персональных данных в Банке осуществляется с согласия субъектов персональных данных в случаях, требующих наличие такого согласия.

4.3. Банк без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

4.4. Доступ к обрабатываемым в Банке персональным данным разрешается только тем работникам Банка, которым персональные данные необходимы в связи с исполнением ими своих служебных обязанностей и только в необходимом объеме.

4.5. Передача ПДн между пользователями ресурса ПДн, предусматривающего передачу ПДн только между работниками Банка, имеющими доступ к ПДн, осуществляется в рабочем порядке с учетом технологии работы с соответствующим ресурсом ПДн.

4.6. Субъект персональных данных имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей его персональные данные (за исключением случаев, предусмотренных ч.8 ст.14 Федерального закона №152-ФЗ «О персональных данных»). Субъект имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

4.7. Представители органов государственной власти (в том числе контролирующих, надзорных, правоохранительных и иных органов) получают доступ к персональным данным, обрабатываемым в Банке, в объеме и порядке, установленном законодательством Российской Федерации.

4.8. Обработка запроса от уполномоченного органа по защите персональных данных осуществляется совместно подразделением, обрабатывающим соответствующие персональные данные, и сотрудником Банка, ответственным за организацию обработки ПДн.

4.9. Об обработке персональных данных в Банке сотрудником, ответственным за организацию обработки ПДн в Банке, направляется уведомление в уполномоченный орган по защите прав субъектов ПДн по форме уполномоченного органа в порядке и в сроки, установленные Федеральным законом "О персональных данных" (за исключением случаев, предусмотренных ч.2 ст.22 Федерального закона №152-ФЗ «О персональных данных»).

4.10. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только при условии предварительного согласия субъекта персональных данных.

4.11. Для обработки персональных данных применяются типовые формы документов, которые определяются Банком, Правительством РФ, Банком России, а также уполномоченными министерствами и ведомствами РФ. Под типовой формой документа понимается шаблон, бланк документа или другая унифицированная форма документа, используемая Банком с целью сбора ПДн.

4.12. Трансграничная передача персональных данных осуществляется в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

5. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обработка персональных данных Банком осуществляется на основе принципов:

- законности и справедливости целей и способов обработки персональных данных;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
- иных принципов и условий, определенных законодательством Российской Федерации в сфере обработки и защиты персональных данных.

6. ПРАВА БАНКА

6.1. Банк как оператор персональных данных, вправе:

- отстаивать свои интересы в суде;
- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении персональных данных в случаях предусмотренных законодательством;
- использовать персональные данные субъекта без его согласия, в случаях предусмотренных законодательством.

7. ПРАВА СУБЪЕКТА ПДн

7.1. Субъект персональных данных либо его представитель, полномочия которого надлежащим образом оформлены, имеет право:

- требовать 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;
- на получение информации, содержащей перечень своих персональных данных, обрабатываемых Банком и источник их получения;
- на получение информации о сроках обработки своих персональных данных, в том числе о сроках их хранения;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Банка при обработке его персональных данных;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;
- отозвать свое согласие на обработку персональных данных в соответствии с требованиями законодательства Российской Федерации;
- иные права, определенные законодательством Российской Федерации.

8. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Сроки обработки персональных данных определяются в соответствии:

- со сроком действия договора с субъектом персональных данных;
- Приказом Минкультуры РФ от 25.08.2010 № 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»;
- Постановлением ФКЦБ РФ от 16.07.2003 № 03-33/пс «Об утверждении Положения

о порядке и сроках хранения документов акционерных обществ»;

- сроком исковой давности;
- а также иными требованиями законодательства РФ и нормативными документами Банка России.

8.2. В Банке создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию в Банке данных типовых форм документов установлены Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

9. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Банк предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных.

9.2. В целях выполнения требований законодательства Российской Федерации в сфере обработки и защиты персональных данных в Банке назначается ответственный за организацию обработки персональных данных.

9.3. При работе с материальными носителями персональных данных в Банке осуществляются процедуры по ограничению физического доступа к этим носителям путем установления пропускного режима в помещения Банка, а также по работе с носителями в условиях и их хранению в местах, не позволяющих посторонним лицам получить к ним доступ.

10. УПРАВЛЕНИЕ РИСКАМИ

10.1. Реализация Политики в отношении обработки персональных данных направлена в первую очередь на минимизацию информационных и операционных рисков, связанных с возможным нарушением доступности, целостности, достоверности и конфиденциальности персональных данных, как информационного актива, по причине возможных информационно-технологических сбоев и, как следствие, с дальнейшим возникновением убытков и (или) оттоком средств с расчетных счетов, счетов депозитов вследствие потери Банком деловой репутации.

10.2. Основываясь на требованиях Банка России, а также международно-признанных принципах и стандартах управления рисками банковской деятельности и рекомендациях Базельского комитета по банковскому надзору, Банк осуществляет управление информационными и операционными рисками в соответствии со следующими основными принципами:

10.2.1. *Принцип системности и комплексности* предполагает использование системного подхода в управлении информационными и операционными рисками, включающего:

- идентификацию рисков;
- анализ и оценку рисков;
- принятие и/или ограничение рисков;
- мониторинг и контроль за рисками.

В целях управления информационными и операционными рисками Банк осуществляет:

- регулярное выявление, оценку и документирование моделей угроз нарушения доступности, целостности, достоверности и конфиденциальности персональных данных;
- сбор и анализ внутренних данных по случаям нарушения доступности, целостности, достоверности и конфиденциальности персональных данных (в т.ч. отчетов (заключений, актов) СВА, СВК, данных, предоставленных другими подразделениями Банка, и др.);
- сбор и анализ данных об операционных убытках вследствие нарушения доступности, целостности, достоверности и конфиденциальности персональных данных;
- классификацию процессов обработки персональных данных (анализ и оценка основных этапов, организационных функций, ключевых моментов обработки персональных данных, способствующих выявлению сопряженных рисков, взаимозависимостей между рисками,

недостатков контроля или управления рисками, а также определению очередности последующих управленческих мер);

- анализ ключевых индикаторов уровня риска, представляющих собой статистические данные, позволяющие понять состояние операционных процессов и выявить недостатки, способствующие нарушению доступности, целостности, достоверности и конфиденциальности персональных данных, и возникновению потенциальным убытков;

Поскольку реализация информационных и операционных рисков способствует реализации прочих финансовых и нефинансовых рисков, принимаемых Банком в процессе осуществления своей деятельности, оценка рисков, связанных с нарушением доступности, целостности, достоверности и конфиденциальности персональных данных, носит комплексный характер (по всем возникающим видам рисков и их совокупности).

10.2.2. ***Принцип методологического единства*** предполагает применение в Банке единообразной и адекватной характеру и масштабам деятельности Банка методологии для идентификации и оценки информационного, операционного риска, а также сопряженных с ними рисков, связанных с нарушением доступности, целостности, достоверности и конфиденциальности персональных данных. Использование принципа предполагает издание Банком внутренних методологических документов, касающихся анализа принимаемых рисков и других вопросов управления рисками, а также осуществление контроля за исполнением структурными подразделениями Банка заложенных в нормативно-методологических документах требований и рекомендаций.

Основу методологии оценки информационного риска составляет система качественно-количественной оценки:

- степени возможности нарушения доступности, целостности, достоверности и конфиденциальности персональных данных в результате воздействия выявленных и (или) предполагаемых угроз;

- степени тяжести последствий от нарушения доступности, целостности, достоверности и конфиденциальности персональных данных.

Основу методологии оценки операционного риска составляет:

- базовый индикативный подход (Положение Банка России от 03.11.2009 № 346-П «О порядке расчета размера операционного риска») к оценке требований к собственным средствам (капиталу) в отношении операционного риска;

- метод количественного анализа распределения фактических убытков, позволяющий сделать прогноз потенциальных операционных убытков, исходя из размеров операционных убытков, имеющих место в Банке в прошлом;

- анализа системы ключевых индикаторов риска деятельности Банка, анализа фактов понесенных убытков от реализации операционного риска.

10.2.3. ***Принцип контроля за распределением и делегированием полномочий*** предполагает взвешенное сочетание централизованного и децентрализованного принятия решений для обеспечения безопасности персональных данных при их обработке в Банке.

Данный принцип реализуется Банком через выполнение следующих условий:

- наличие четкого разделения полномочий и указание пределов полномочий коллегиальных органов управления Банка и должностных лиц, внутренних структурных подразделений Банка при обработке персональных данных;

- коллегиальность принятия решений по вышеуказанным операциям, наличие внутренних нормативных актов (инструкций, положений, правил) Банка, регламентирующих порядок и последовательность действий, а также процедуры взаимодействия подразделений Банка в процессе обработки персональных данных;

- разделение функций инициирования и исполнения обработки персональных данных, ее сопровождения и контроля;

- иные условия и требования, установленные нормативными документами Банка России.

10.3. В целях минимизации информационного и операционного риска, связанных с нарушением доступности, целостности, достоверности и конфиденциальности персональных данных, в Банке применяются следующие меры:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое, избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- контроль за соблюдением сотрудниками требований нормативно-методических документов по защите информации и сохранении тайны;
- определение и регламентация состава сотрудников, имеющих право доступа в помещение, в котором размещается серверное оборудование;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований доступа работниками Банка;
- ограничение физического доступа к носителям персональных данных путем установления пропускного режима в помещения Банка, а также работа с носителями персональных данных в условиях и их хранение в местах, не позволяющих посторонним лицам получить к ним доступ;
- разработка защиты от несанкционированного входа в информационную систему,
- адекватные процедуры безопасности и контроля информации (использование систем кодировок для защиты информации во время сеансов приема/передачи или хранения информации; программного обеспечения, обеспечивающего различный уровень доступа к базам данных, файлам, программам и т.п.);
- использование резервных серверов и дублирующих мощностей в телекоммуникациях и вычислительных сетях;
- регистрация и мониторинг действий пользователей автоматизированных систем;
- отслеживание и протоколирование производимых в информационной сети операций;
- осуществление поддержки в течение времени использования автоматизированных информационных систем, включая определение правил приобретения, разработки и обслуживания (сопровождения) программного обеспечения;
- организация пропускного режима и контроля деятельности посторонних лиц;
- использование технических средств охраны и сигнализации;
- организация порядка охраны территории, здания, помещений, транспортных средств;
- выработка требований к защите информации при интервьюировании и собеседовании.

10.4. Управление сопряженными рисками, возникающими в связи с нарушением доступности, целостности, достоверности и конфиденциальности персональных данных, осуществляется в соответствии:

- со Стратегией по управлению рисками и капиталом Банка;
- внутренними документами, регламентирующими управление соответствующими видами рисков;
- решениями исполнительных и/или коллегиальных органов управления Банка.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Настоящая Политика является внутренним документом Банка, общедоступной и подлежит размещению на официальном сайте Банка.

11.2. Настоящая Политика подлежит изменению, дополнению в случае изменения в законодательства Российской Федерации в сфере обработки и защиты персональных данных.

11.3. Контроль исполнения требований настоящей Политики осуществляется лицом, ответственным за организацию обработки персональных данных в Банке.

11.4. Ответственность должностных лиц Банка, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных

данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Банка.

Лист согласования

Исполнитель:

Начальник Управления контроля и информации

_____ М.Б. Горбачев

«__» апреля 2018 года

СОГЛАСОВАНО:

Главный бухгалтер

_____ М.А. Некрасов
«__» апреля 2018 года

Ведущий специалист
договорно-правового отдела ЮУ

_____ Е.А. Андреева
«__» апреля 2018 года

Начальник Административного управления

_____В.В. Мотылева
«__» апреля 2018 года

Начальник Управления электронной обработки данных

_____А.И. Шароватов
«__» апреля 2018 года

Руководитель Службы внутреннего контроля

_____ Н.И. Атрошенко
«__» апреля 2018 года