Публичное акционерное общество «МТС-Банк»
ПАО «МТС-Банк»

УТВЕРЖДЕНА

Решением Правления
Публичного акционерного общества
«МТС-Банк»

Протокол № 48
от «07» ноября 2017 г.

ПОЛИТИКА

В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАО «МТС-Банк»

Рег. № 04-00039/17-(0) от «07» ноября 2017 г.

Введена в действие Решением Правления ПАО «МТС-Банк»:
Протокол заседания Правления № 48 от «07» ноября 2017 г.

г. Москва 2017

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) определяет средства, цели и принципы обработки персональных данных в Банке.

1.2. Обеспечение безопасности персональных данных и обеспечение соответствия требованиям законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных является одной из приоритетных задач Банка.

1.3. Персональные данные, обрабатываемые в Банке, относятся к информации ограниченного доступа и на них распространяются все требования по защите информации, установленные во внутренних документах Банка.

1.4. Банк является оператором персональных данных и внесен в реестр операторов персональных данных (рег. № 09-0060617).

1.5. Банк организует и обеспечивает обработку и безопасность персональных данных в соответствии с Комплексом БР ИББС, нормативно-методическими документами регуляторов в области обработки и обеспечения безопасности персональных данных.

1.6. Необходимые правовые, организационные и технические меры для защиты персональных данных регламентируются внутренними документами Банка в области защиты информации.

1.7. Настоящая Политика размещена на официальном сайте Банка http://www.mtsbank.ru для обеспечения неограниченного доступа к ней.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В рамках настоящего документа используются следующие термины и определения:

Наименование термина	Определение термина
Персональные данные	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Оператор персональных данных (оператор)	ПАО «МТС-Банк».
Обработка персональных данных	любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.
Автоматизированная обработка персональных данных	обработка персональных данных с помощью средств вычислительной техники.
Распространение персональных данных	действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Наименование термина	Определение термина
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.
Банк	ПАО «МТС-Банк»

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Банк обрабатывает персональные данные в целях:

3.1. выполнения возложенных на Банк законодательством Российской Федерации и нормативными актами Банка России функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О рынке ценных бумаг», «О страховании вкладов физических лиц в банках Российской Федерации»;

3.2. принятия решения о возможности заключения трудового договора с соискателями должностей;

3.3. централизованного ведения учетных записей и формирования единого телефонного справочника;

3.4. организации внутриобъектового режима Банка;

3.5. организации учета работников Банка для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия работнику в трудоустройстве, обучении, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «Об обязательном медицинском страховании в РФ», а также Уставом и нормативными актами Банка.

4. ПРАВОВЫЕ ОСНОВАНИЯ ДЛЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Банк осуществляет обработку персональных данных: ст. ст. 85-90 Трудового кодекса Российской Федерации; ст. ст. 6-10 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; ст. 5,6,33 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»; ст. 4, 5 Федерального закона от 30.12.2004 № 218-ФЗ «О кредитных историях»; ст. 30 Федерального закона от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг»; ст. 44, 53, 81. 82, 92 Федерального закона 26.12.1995 № 208-ФЗ «Об акционерных обществах»; ст. 4, 7, 9 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»; ст. 9 Федерального закона от 10.12.2003 N 173-ФЗ «О валютном регулировании и валютном контроле»; ст. 6 Федерального закона от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»; Стандартом Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

5. ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В БАНКЕ

5.1. Перечень персональных данных, обрабатываемых в Банке, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Банка, с учетом целей обработки персональных данных, указанных в разделе 3 настоящей Политики.

5.2. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, в Банке не осуществляется.

6. ПЕРЕЧЕНЬ ДЕЙСТВИЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ И СПОСОБЫ ИХ ОБРАБОТКИ

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

6.2. Обработка персональных данных в Банке осуществляется следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по защищенным каналам связи ;
- смешанная обработка персональных данных.

7. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сроки обработки персональных данных определяются сроком действия договора с субъектом персональных данных, трудовым кодексом Российской Федерации, приказом Минкультуры России 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», сроком исковой давности, а также иными требованиями законодательства Российской Федерации.

8. КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

К категориям субъектов персональных данных, чьи персональные данные обрабатываются Банком, относятся:

- работники Банка, бывшие работники, кандидаты на замещение вакантных должностей, а также родственники работников;
- клиенты Банка (физические лица);
- представители/работники клиентов и контрагентов Банка (юридических лиц).

9. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Обработка персональных данных Банком осуществляется на основе следующих принципов:

- законность и справедливость обработки персональных данных;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и конкретных целей обработки;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимость объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;
- 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;
- уничтожение персональных данных либо обезличивание по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- соблюдение конфиденциальности персональных данных.

12.1. Обработка персональных данных осуществляется на основании согласия на обработку персональных данных, а также условий, определенных законодательством Российской Федерации.

12.2. Банк вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

12.3. При поручении обработки третьему лицу Банк поручает такую обработку с согласия субъекта персональных данных и на основании заключаемого с этим лицом договора, с включением в такой договор обязательных положений по соблюдению принципов и правил обработки персональных данных, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных». В таком поручении определяются:

- перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;

- цели обработки персональных данных;
- обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;
- требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ «О персональных данных» или указание на уровень защищенности информационной системы персональных данных, которая будет использоваться для обработки персональных данных.

12.4. Перечень третьих лиц, которым в рамках осуществления договорных отношений поручается обработка персональных данных, указывается на официальном сайте Банка.

12.5. При осуществлении хранения персональных данных Банк использует базы данных, находящиеся на территории Российской Федерации, в соответствии с ч. 5 ст. 18 Федерального закона «О персональных данных».

10. МЕРЫ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.6. В соответствии с частью 2 статьи 19 Федерального закона «О персональных данных» для обеспечения безопасности персональных данных при их обработке в Головном офисе, региональных филиалах, дополнительных и операционных офисах Банка применяются организационные и технические меры защиты, необходимые для обеспечения соответствия установленным уровням защищенности персональных данных, в том числе:

- назначен работник, ответственный за организацию обработки персональных данных;
- персональные данные обрабатываются в соответствии с требованиями организационно-распорядительных документов Банка, регламентирующих порядок обработки и защиты персональных данных;
- информация обрабатывается в контролируемых помещениях, расположенных в пределах границ охраняемой зоны;
- определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;
- предоставление доступа к персональным данным работникам Банка, только для выполнения их должностных/функциональных обязанностей;
- осуществляется круглосуточная охрана помещений, в которых размещаются технические средства и другие элементы информационных систем персональных данных;
- хранение бумажных и съемных носителей информации осуществляется в сейфах и закрытых шкафах;
- разграничен доступ пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации, входящих в состав информационных систем персональных данных;
- осуществляется учет: съемных носителей информации, средств криптографической защиты информации, ключевых носителей информации;
- применяются специальные программно - технические средства для контроля и ограничения доступа к информации;
- осуществляется резервирование технических средств, резервное копирование и дублирование информационных массивов и носителей информации в соответствии с политикой принятой в Банке;

– обеспечивается парольная зашита при доступе к ресурсам информационных систем персональных данных, а также к сетевому оборудованию, входящего в их состав;

– для защиты информационных ресурсов информационных систем персональных данных от вредоносного программного обеспечения на серверах и автоматизированных рабочих местах Банка применяется эшелонированная система антивирусной защиты;

– обеспечивается мониторинг состояния информационной безопасности в круглосуточном режиме и защита от утечек конфиденциальной информации, в том числе и персональных данных;

– при передаче информации, составляющей персональные данные, по каналам связи используются российские сертифицированные средства криптографической защиты информации.

12.7. Функции обеспечения контроля за выполнением организационных и технических мер по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных Банка, возложены на ответственное структурное подразделение и работников, ответственных за организацию обработки и обеспечение безопасности персональных данных.

11. ПРАВА И ОБЯЗАННОСТИ

12.8. Руководство Банка обязуется:

- обеспечить конфиденциальность информации, содержащей персональные данные субъектов персональных данных;
- обеспечить выполнение требований, предъявляемых к обработке персональных данных законодательством и внутренними документами Банка;
- в случае реорганизации или ликвидации Банка осуществлять учет, сохранность и передачу персональных данных субъектов персональных данных на государственное хранение в соответствии с законодательством Российской Федерации.

12.9. Субъект персональных данных, предоставляющий Банку право на обработку своих персональных данных, в соответствии с положениями Федерального закона «О персональных данных» имеет право:

- на доступ к своим персональным данным;
- на прекращение обработки персональных данных (по требованию, при отсутствии оснований для отказа, предусмотренных Федеральным законом «О персональных данных»);
- на получение информации, касающейся 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, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона;
  - перечень обрабатываемых персональных данных и источник их получения;
  - сроки обработки персональных данных, в том числе сроки их хранения;
  - порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

- информацию об осуществлении или предполагаемой трансграничной передаче данных;
- наименование и адрес лица, осуществляющего обработку персональных данных по поручению Банка, как оператора персональных данных, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

- на обжалование действий или бездействий Банка в Роскомнадзор или в судебном порядке в случае нарушений требований Федерального закона «О персональных данных».

12.10. Заявление оформляется в произвольной форме с соблюдением требований Федерального закона «О персональных данных».

12.11. Процедура обработки запросов уполномоченного органа по защите прав субъектов персональных данных и иных надзорных органов, осуществляющих контроль и надзор в области персональных данных, а также другие процедуры по обработке обращений субъектов персональных данных или их законных представителей определяется «Регламентом реагирования на обращения субъектов персональных данных и надзорных органов».

13. ОТВЕТСТВЕННОСТЬ

13.1. Руководство Банка несет ответственность за нарушение положений данной Политики и норм, регулирующих обработку и обеспечение безопасности персональных данных и вправе привлекать работников Банка, к дисциплинарной, административной, гражданско-правовой или уголовной ответственности в соответствии с действующим законодательством Российской Федерации за допущенные нарушения.

14. ПОРЯДОК ВВОДА В ДЕЙСТВИЕ И ПЕРЕСМОТРА ПОЛИТИКИ

14.1. Ввод в действие и утверждение настоящего документа осуществляется в соответствии с действующей редакцией «Порядка разработки, утверждения, введения в действие, внесения изменений и прекращения действия нормативных документов».

14.2. Пересмотр Политики должен осуществляться на периодической и внеплановой основе.

14.2.1 Внеплановое внесение изменений может производиться:

- в случае изменения действующей нормативно-правовой базы в области защиты информации;
- по результатам анализа инцидентов ИБ, оценки операционных рисков и рисков ИБ;
- по результатам проведения самооценок и аудитов ИБ;
- в случае изменения организационной структуры Банка;
- в случае изменения технологических и бизнес процессов Банка.

14.2.2. На периодической основе, настоящая Политика должна пересматриваться не реже одного раза в два года.