МОРСКОЙ БАНК

УТВЕРЖДЕНО
Председателем Правления
МОРСКОГО БАНКА (АО)

Приказ № МБ-253
от «08» декабря 2023 г.

ЧАСТНАЯ ПОЛИТИКА
обработки персональных данных
в МОРСКОМ БАНКЕ (АО)

Версия 1.0

Москва - 2023

Содержание

1. Общие положения

1.1. Настоящая Частная Политика обработки персональных данных в МОРСКОМ БАНКЕ (АО) (далее – «Политика») разработана в соответствии с законодательством Российской Федерации, в том числе Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями) (далее - Федеральный закон от 27.07.2006 № 152-ФЗ), нормативно-правовыми актами Банка России, включая стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», федеральных органов исполнительной власти, политикой информационной безопасности Банка и иными внутренними нормативными документами Банка, и обязательна для исполнения всеми работниками и должностными лицами МОРСКОГО БАНКА (АО) (далее – «Банк»), осуществляющими обработку или имеющими доступ к персональным данным, и по отношению ко всем персональным данным, обрабатываемым в Банке (далее – ПДн).

1.2. Действие настоящей Политики распространяется на все процессы Банка, связанные с обработкой персональных данных. ПДн являются конфиденциальной, строго охраняемой информацией (составляющей охраняемую законом тайну Банка), и на них распространяются все требования, установленные внутренними нормативными документами Банка к защите конфиденциальной информации. Обезличенные и общедоступные ПДн не являются конфиденциальной информацией.

1.3. Обработка и обеспечение безопасности информации, отнесенной к ПДн, осуществляется в Банке с учетом мер, направленных на соответствие требованиям комплекса документов Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», и позволяет обеспечить защиту ПДн, обрабатываемых как в информационных системах персональных данных (далее - ИСПДн), т.е. в системах, целью создания которых является обработка ПДн и к защите которых требования и рекомендации по обеспечению безопасности ПДн предъявляют Федеральная служба безопасности (ФСБ России) и Федеральная служба по техническому и экспортному контролю (ФСТЭК России), так и в иных информационных системах, в которых ПДн обрабатываются совместно с информацией, защищаемой в соответствии с требованиями, установленными для этой информации (режим защиты сведений, составляющих банковскую тайну, коммерческую тайну и др.), в частности защиту от несанкционированного доступа и неправомерного распространения ПДн, обрабатываемых в Банке.

1.4. Важнейшими условиями достижения целей деятельности Банка являются обеспечение законности обработки персональных данных в технологических процессах Банка, а также обеспечение необходимого уровня безопасности информационных активов, к которым, в том числе, относятся персональные данные.

1.5. Целью настоящей Политики является установление основных принципов и подходов к обработке и обеспечению безопасности персональных данных в Банке, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.6. Настоящая Политика является общедоступным документом, раскрывает основные категории ПДн, обрабатываемых Банком, цели, способы, принципы обработки Банком ПДн, права и обязанности Банка при обработке ПДн, права и обязанности субъектов ПДн, а также перечень мер, применяемых Банком в целях обеспечения безопасности ПДн при их обработке. и подлежит размещению на информационном стенде Банка в местах обслуживания клиентов, а также публикации на официальном информационном сайте Банка в сети Интернет.

1.7. На основании приказа Федеральной службы по надзору в сфере связи,

информационных технологий и массовых коммуникаций Банк включен в реестр операторов, осуществляющих обработку персональных данных.

1.8. Во всех случаях, не охваченных положениями настоящей Политики, Работники Банка руководствуются требованиями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, и другими внутренними нормативными документами Банка, регулирующими отношения, связанные с обработкой персональных данных, в том числе с использованием средств автоматизации и без использования таких средств.

2. Нормативное регулирование

2.1. Настоящая Политика разработана на основе законодательства Российской Федерации, регламентирующего защиту персональных данных, а также нормативных документов Банка России в области информационной безопасности с учетом Рекомендаций Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2.2. В случае изменения законодательства Российской Федерации, внесения изменений в нормативные акты Банка России, федеральных органов исполнительной власти, а также во внутренние нормативные документы Банка настоящая Политика, до ее приведения в соответствие с такими изменениями, действует в части, не противоречащей законодательным и иным нормативно-правовым актам, а также соответствующим внутренним нормативным документам Банка.

3. Термины и определения

- **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
- **Администратор ИБ ИСПДн** – администратор информационной безопасности информационной системы ПДн (Работник Банка, назначаемый приказом Председателя Правления Банка);
- **Биометрические персональные данные** - данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;
- **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- **Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;
- **Информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- **Клиенты** - физические и юридические лица (резиденты и нерезиденты), индивидуальные предприниматели, физические лица, занимающиеся частной практикой, имеющие в банке банковский счет и (или) счет, открытый на основании договора расчетно-кассового обслуживания, и (или) заключившие с Банком договор на совершение какой-либо банковской операции или иной сделки.

- **Конфиденциальность персональных данных –** обязанность оператора, а также иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

- **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;

- **Оператор** — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- **Ответственный за организацию обработки персональных данных** - должностное лицо, которое назначается Приказом Председателя Правления, организующее принятие правовых, организационных и технических мер в целях обеспечения надлежащего выполнения функций по организации обработки персональных данных в Банке в соответствии с положениями законодательства Российской Федерации в области персональных данных;

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

- **Персональные данные, разрешенные для распространения (ПДРР)** — это персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

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

- **Представитель** - лицо, действующее от имени представляемого лица (Работника Банка, Клиента, корреспондента, контрагента, партнера) на основании закона, договора или доверенности;

- **Работник Банка** - физическое лицо, состоящее с Банком в трудовых отношениях (на основании трудового договора, контракта, договора подряда, договора возмездного оказания услуг или иного документа, определяющего прочие имущественные взаимоотношения и другие вопросы взаимодействия) и исполняющее служебные/договорные обязанности, принятое по основному месту работы, по совместительству или оказывающее Банку услуги по договору гражданско-правового характера;

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

- **Роскомнадзор** - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), является уполномоченным

федеральным органом исполнительной власти по защите прав субъектов персональных данных;

- **Субъект персональных данных (Субъект)** - физическое лицо, прямо или косвенно определенное или определяемое на основании относящихся к нему персональных данных;

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

- **Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

- **Уровень защищенности персональных данных** – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах 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.

4. Список используемых обозначений и сокращений

Банк – МОРСКОЙ БАНК (АО), являющийся в рамках Федерального закона «О персональных данных» оператором по обработке персональных данных;

ИБ – информационная безопасность;

ИСПДн – информационная система персональных данных;

ПДн – персональные данные;

РФ – Российская Федерация;

Субъект – субъект персональных данных;

ФСБ – Федеральная служба безопасности;

ФСТЭК – Федеральная служба по техническому и экспортному контролю.

5. Цели обработки персональных данных

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

5.2. Цели обработки персональных данных в Банке происходят, в том числе, из анализа правовых актов, регламентирующих деятельность Банка, целей фактически осуществляемой Банком деятельности, а также деятельности, которая предусмотрена учредительными документами Банка, и конкретных бизнес-процессов Банка в конкретных информационных системах персональных данных (по структурным подразделениям Банка и их процедурам в отношении определенных категорий субъектов персональных данных).

5.3. Не допускается обработка ПДн, не совместимая с целями сбора ПДн.

5.4. Банк осуществляет обработку персональных данных в следующих целях:

- обеспечения соблюдения актов законодательства и иных нормативно-правовых актов и осуществления и исполнения функций, полномочий и обязанностей, возложенных на Банк законодательством Российской Федерации, нормативно-правовыми и иными актами Банка России, федеральных органов исполнительной власти, уставом, лицензиями и внутренними нормативными документами Банка;

- осуществления банковской деятельности в соответствии с Уставом и Лицензиями Банка;

- рассмотрение резюме соискателей на должность и принятие решения о возможности заключения трудового договора с ними;

- заключение и исполнение трудовых договоров;

- обеспечение соблюдения законов и иных нормативных правовых актов, в том числе исполнение требований трудового, пенсионного, страхового и социального законодательства РФ;

- противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

- предоставления информации, в том числе отчетности, надзорным и контрольным органам в соответствии с требованиями законодательства РФ;

- - передачи Банком ПДн или поручения их обработки третьим лицам в соответствии с законодательством РФ;

- формирования данных о кредитной истории;

- осуществление мероприятий по возврату просроченной задолженности;

- ведение кадрового делопроизводства и организация учета Работников Банка;

- содействие Работникам в трудоустройстве, получении образования и продвижении по службе;

- контроль количества и качества выполняемой работы;

- обеспечение личной безопасности Работников Банка;

- обеспечение сохранности имущества Банка;

- принятие решения о заключении договора с потенциальным клиентом/контрагентом Банка;

- заключение, исполнение и прекращение гражданско-правовых договоров с физическими лицами: гражданами и индивидуальными предпринимателями, юридическими лицами;

- продвижение услуг Банка на рынке;

- защита законных прав и интересов Банка, в том числе в судах судебной системы РФ;

- ведение Банком административно-хозяйственной деятельности;

- ведение архива Банка;

- осуществление иных функций, возложенных на Банк законодательством Российской Федерации, нормативными актами Банка России.

6. Правовые основания обработки персональных данных

6.1. Правовыми основаниями обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Банк осуществляет обработку персональных данных.

6.2. В зависимости от цели обработки персональных данных, правовыми основаниями для такой обработки в Банке являются:

- Устав Банка;
- Лицензии Банка;
- договор, заключенный между Банком и Субъектом;
- согласие Субъекта на обработку персональных данных;

- общедоступность персональных данных Субъекта;
- Конституция РФ (в том числе статьи 23, 24);
- трудовое законодательство РФ;
- налоговое законодательство РФ;
- пенсионное законодательство РФ;
- страховое законодательство РФ;
- социальное законодательство РФ;
- Федеральный закон «О бухгалтерском учете» от 06.12.2011 № 402-ФЗ;
- Федеральный закон «О защите прав потребителей» от 07.02.1992 № 2300-1;
- Федеральный закон от 02.12.1990 №395-1 «О банках и банковской деятельности»;
- Федеральный закон от 23.12.2003 №177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации»;
- Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федеральный закон от 30.12.2004 № 218-ФЗ «О кредитных историях»;
- Федеральный закон от 26.12.1995 №208-ФЗ «Об акционерных обществах»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон 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»;
- Федеральный закон от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле»;
- Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг»;
- Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ;
- Федеральный закон «О потребительском кредите (займе)» от 21.12.2013 № 353-ФЗ;
- Федеральный закон «Об ипотеке (залоге недвижимости)» от 16.07.1998 № 102-ФЗ;
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015);
- Положение Банка России от 20.07.2007 № 307-П «О порядке ведения учета и представления информации об аффилированных лицах кредитных организаций»;
- Положение Банка России от 02.03.2012 № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации

(отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

- Положение Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств»;
- Положение Банка России от 28.06.2017 № 590-П «О порядке формирования кредитными организациями резервов на возможные потери по ссудам, ссудной и приравненной к ней задолженности»;
- Положение Банка России от 23.10.2017 № 611-П «О порядке формирования кредитными организациями резервов на возможные потери»;
- Положение Банка России от 29.01.2018 № 630-П «О порядке ведения кассовых операций и правилах хранения, перевозки и инкассации банкнот и монеты Банка России в кредитных организациях на территории Российской Федерации»;
- Указание Банка России от 15.07.2021 № 5861-У «О порядке представления кредитными организациями в уполномоченный орган сведений и информации в соответствии со статьями 7, 7.5 Федерального закона "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма";
- Указание Банка России от 16.08.2017 № 4498-У «О порядке передачи уполномоченными банками, государственной корпорацией «Банк развития и внешнеэкономической деятельности (ВНЕШЭКОНОМБАНК)» органам валютного контроля информации о нарушениях лицами, осуществляющими валютные операции, актов валютного законодательства Российской Федерации и актов органов валютного регулирования»;
- Инструкция Банка России от 30.06.2021 № 204-И «Об открытии, ведении и закрытии банковских счетов и счетов по вкладам (депозитам)»;
- 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» (с изменениями и дополнениями);
- Указание Банка России от 02.02.2021 № 5720-У «О порядке уведомления лиц, включенных в список инсайдеров, об их включении в такой список и исключении из него»;
- Приказ Федеральной службы безопасности Российской Федерации (ФСБ России) от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- иные Приказы и руководящие документы регулирующих органов – Роскомнадзор, ФСТЭК и ФСБ России;
- иные федеральные законы и нормативные правовые акты Российской Федерации и регуляторов, в целях исполнения которых Банк обязан осуществлять обработку персональных данных.

7. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

7.1. Объем и содержание (категории) обрабатываемых персональных данных в Банке соответствуют заявленным целям их обработки и не являются избыточными по отношению к заявленным целям их обработки.

7.2. Банк обрабатывает персональные данные следующих категорий субъектов персональных данных:

- кандидаты на вакантные должности Банка;
- Работники Банка;
- ближайшие родственники Работников Банка;
- бывшие Работники Банка;
- физические лица - участники Банка, члены органов управления и контроля за деятельностью Банка;
- аффилированные лица или представители юридического лица, являющегося аффилированным по отношению к Банку;
- физические лица - Клиенты Банка;
- представители, учредители, акционеры юридических лиц – клиентов Банка;
- физические лица – контрагенты Банка;
- представители, учредители, акционеры юридических лиц – контрагентов Банка;
- лица, попадающие в зону действия системы видеонаблюдения Банка в общественных местах;
- лица, посещающие помещения ограниченного доступа Банка;
- супруг/супруга Клиента Банка, поручитель, залогодатель клиента Банка;
- физические лица - получатели перевода денежных средств от клиентов Банка;
- потенциальные клиенты, контрагенты, партнеры, а также руководитель, участник (акционер) или работник юридического лица, являющегося потенциальным клиентом, партнером, контрагентом (информация, необходимая Банку в целях рассмотрения вопроса о заключении договорных отношений (проведении операций и сделок с потенциальным клиентом, контрагентом, партнером) и для выполнения требований законодательства РФ);
- иные физические лица, обработка персональных данных которых необходима Банку для осуществления и выполнения возложенных на него законодательством РФ функций, полномочий и обязанностей.

7.3. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Банком для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона от 27.07.2006 г. № 152-ФЗ (с изменениями и дополнениями).

7.4. Обработка биометрических персональных данных может осуществляться в Банке без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

7.5. Предоставление биометрических ПДн не может быть обязательным, за исключением случаев, предусмотренных пунктом 7.4. Банк не вправе отказывать в обслуживании в случае отказа Субъекта ПДн предоставить биометрические ПДн и (или)

дать согласие на обработку ПДн, если в соответствии с федеральным законом получение Банком согласия на обработку ПДн является обязательным.

7.6. В Банке не допускается обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и интимной жизни, за исключением случаев, предусмотренных частью 2 и 2.1 статьи 10 Федерального закона от 27.07.2006 г. № 152-ФЗ (с изменениями и дополнениями).

7.7. Обработка специальных категорий персональных данных, указанных в пункте 7.6. настоящей Политики, допускается в случаях, предусмотренных частью 2 и 2.1 статьи 10 Федерального закона от 27.07.2006 г. № 152-ФЗ (с изменениями и дополнениями), например, допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
2) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона от 27.07.2006 г. № 152-ФЗ.

7.8. Обработка специальных категорий ПДн, осуществлявшаяся в случаях, предусмотренных пунктом 7.7. должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено Федеральным законом от 27.07.2006 г. № 152-ФЗ.

8. Порядок, принципы и условия обработки персональных данных

8.1. Обработка персональных данных осуществляется Банком с соблюдением следующих принципов:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных целей обработки, не допускается нецелевая обработка персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- осуществляются сбор и дальнейшая обработка только тех персональных данных, которые отвечают заявленным целям обработки;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки, не допускается обработка избыточных персональных данных по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивается их точность и достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям обработки;
- обрабатываемые персональные данные подлежат уничтожению или обезличиванию по достижении целей обработки или, в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

8.2. Обработка персональных данных допускается при выполнении хотя бы одного из следующих условий:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- 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;

- обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;
- обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);
- обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
- 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. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы Субъекта ПДн, устанавливающие случаи обработки ПДн несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие Субъекта ПДн;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- 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;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона №152-ФЗ, при условии обязательного обезличивания персональных данных;
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

8.3. Персональные данные не раскрываются третьим лицам, не распространяются иным образом без согласия Субъекта, за исключением случаев, предусмотренных законодательством Российской Федерации.

8.4. С согласия Субъекта ПДн Банк вправе поручить обработку ПДн другому лицу, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее - поручение Банка). Лицо, осуществляющее обработку ПДн по поручению Банка, обязано соблюдать принципы и правила обработки ПДн,

предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ, соблюдать конфиденциальность ПДн, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ. В поручении Банка должны быть определены перечень ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федерального закона от 27.07.2006 № 152-ФЗ, обязанность по запросу Банка в течение срока действия поручения Банка, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Банка требований, установленных в соответствии с настоящей статьей, обязанность обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ, в том числе требование об уведомлении Банка о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ.

8.5. Лицо, осуществляющее обработку ПДн по поручению Банка, не обязано получать согласие Субъекта ПДн на обработку его ПДн.

8.6. В случае, если Банк поручает обработку ПДн другому лицу, ответственность перед Субъектом ПДн за действия указанного лица несет Банк. Лицо, осуществляющее обработку ПДн по поручению Банка, несет ответственность перед Банком.

8.7. В случае, если оператор поручает обработку ПДн иностранному физическому лицу или иностранному юридическому лицу, ответственность перед Субъектом ПДн за действия указанных лиц несет Банк и лицо, осуществляющее обработку ПДн по поручению Банка.

8.8. Банк вправе передавать персональные данные третьим лицам без получения согласия Субъекта в случаях, предусмотренных законодательством Российской Федерации (в федеральную налоговую службу, государственный пенсионный фонд и другим государственным органам, органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным законодательством Российской Федерации).

8.9. Работники Банка, допущенные к обработке персональных данных, обязаны:

- знать и неукоснительно выполнять положения:
- законодательства Российской Федерации в области персональных данных;
- настоящей Политики;
- иных локальных актов Банка по вопросам обработки и обеспечения безопасности персональных данных;
- обрабатывать персональные данные только в рамках выполнения своих должностных обязанностей;
- не разглашать персональные данные, обрабатываемые в Банке;
- сообщать о действиях других лиц, которые могут привести к нарушению положений настоящей Политики;
- сообщать об известных фактах нарушения требований настоящей Политики Ответственному за организацию обработки персональных данных в Банке.

8.10. Безопасность персональных данных в Банке обеспечивается выполнением согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности персональных данных, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и работы информационных систем персональных данных в случае реализации угроз.

8.11. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

9. Организация обработки персональных данных

9.1. Банк осуществил уведомление уполномоченного органа по защите прав Субъектов (Роскомнадзор) об осуществлении обработки персональных данных. Банк периодически осуществляет актуализацию сведений, указанных в уведомлении.

9.2. Обработка персональных данных в Банке осуществляется следующими способами:

- с использованием средств автоматизации;
- без использования средств автоматизации;
- смешанным способом (включающим как автоматизированную, так и неавтоматизированную обработку).

10. Права субъекта персональных данных

10.1. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку ПДн может быть дано Субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя Субъекта ПДн полномочия данного представителя на дачу согласия от имени Субъекта ПДн проверяются Банком.

10.2. Субъект, обработка персональных данных которого осуществляется Банком, имеет право на:

- получение сведений, касающихся обработки своих персональных данных;
- уточнение, блокирование или уничтожение персональных данных в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или используются для достижения целей, отличных от заявленной цели обработки;
- отзыв согласия на обработку персональных данных;
- иные права, установленные Федеральным законом №152-ФЗ «О персональных данных».

10.3. 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, указанных в Федеральном законе «О персональных данных».

10.4. Субъект персональных данных имеет право на получение следующей информации, касающейся обработки его персональных данных:

- подтверждение факта обработки персональных данных Банком, а также правовые основания и цель обработки;
- способы обработки персональных данных Банком;
- наименование и адрес местонахождения Банка;
- сведения о лицах (за исключением Работников Банка), которые имеют доступ к персональным данным, и лицах, которым может быть предоставлен такой доступ в порядке, предусмотренном законодательством Российской Федерации;
- перечень обрабатываемых персональных данных и 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 прав, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование и/или фамилию, имя, отчество и адрес местонахождения третьего лица, осуществляющего обработку персональных данных, если обработка персональных данных была поручена такому лицу.
- информацию о способах исполнения Банком обязанностей, установленных статьей 18.1 Федерального закона от 27.07.2006 № 152-ФЗ;
- иные сведения, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных» или другими федеральными законами.

10.5. Сведения, указанные в пункте 10.4, должны быть предоставлены Субъекту ПДн Банком в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим Субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

10.6. Право субъекта персональных данных на получение информации, касающейся обработки его персональных данных, может быть ограничено в случаях, установленных Федеральным законом №152-ФЗ «О персональных данных».

10.7. Запросы/обращения субъектов персональных данных по вопросам обработки персональных данных могут быть направлены в письменном виде по адресу местонахождения Банка. Информация об адресах местонахождения размещена на официальном сайте Банка в сети Интернет – **https://maritimebank.com.**

10.8. Сведения, указанные в пункте 10.4, предоставляются Субъекту ПДн или его представителю Банком **в течение десяти рабочих дней** с момента обращения либо получения оператором запроса Субъекта ПДн или его представителя. Указанный срок может быть продлен, **но не более чем на пять рабочих дней** в случае направления Банком в адрес Субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Банк предоставляет сведения, указанные в пункте 10.4, Субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

10.9. Запрос субъекта персональных данных должен содержать:

- серию и номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие наличие гражданско-правовых отношений между Банком и Субъектом (номер, дата заключения гражданско-правого договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Банком;
- подпись Субъекта или его представителя;
- дату направления запроса.

10.10. В случае, если сведения, указанные в пункте 10.4, а также обрабатываемые персональные данные были предоставлены для ознакомления Субъекту ПДн по его запросу, Субъект ПДн вправе обратиться повторно к Банку или направить ему повторный запрос в целях получения сведений, указанных в пункте 10.4, и ознакомления с такими ПДн не ранее чем через 30 дней после первоначального обращения или направления

первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект ПДн.

10.11. Субъект ПДн вправе обратиться повторно к Банку или направить ему повторный запрос в целях получения сведений, указанных в пункте 10.4, а также в целях ознакомления с обрабатываемыми ПДн до истечения 30 дней с даты первого запроса, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 10.8., должен содержать обоснование направления повторного запроса (причина его повторного (досрочного) направления).

10.12. Банк вправе отказать Субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 10.10 и 10.11. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Банке.

10.13. Право Субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе если:

- обработка ПДн, включая ПДн, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка ПДн осуществляется органами, осуществившими задержание Субъекта ПДн по подозрению в совершении преступления, либо предъявившими Субъекту ПДн обвинение по уголовному делу, либо применившими к Субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
- обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ Субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;
- обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

10.14. Субъект вправе обратиться с требованием об уточнении, блокировке или уничтожении персональных данных в случае, если персональные данные являются неполными, устаревшими, неточными, получены незаконно или не являются необходимыми для использования в заявленных целях.

10.15. В случае поступления запроса на уточнение/уничтожение персональных данных, обработка указанных персональных данных (за исключением хранения) приостанавливается на период проведения Банком проверки правомерности требования Субъекта.

10.16. Если в ходе проведения Банком проверки подтверждается, что обрабатываемые персональные данные являются неточными (неполными или устаревшими), то такие персональные данные уточняются.

10.17. Если в ходе проведения Банком проверки подтверждается, что обрабатываемые персональные данные получены незаконно или не являются необходимыми для использования в заявленных целях, и обеспечить правомерность их обработки не представляется возможным, такие персональные данные уничтожаются. При этом, Субъект в письменном виде уведомляется о совершенных с его персональными данными действиях.

10.18. В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональные данные Банком актуализируются, а обработка прекращается.[1]

10.19. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных;
- Банк не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом "О персональных данных" или иными федеральными законами;
- иное не предусмотрено иным соглашением между Банком и субъектом персональных данных.

10.20. При поступлении заявления об отзыве согласия на обработку персональных данных, Банк прекращает их обработку в течение 30 дней с даты поступления заявления об отзыве, если иное не предусмотрено гражданско-правовым договором, стороной которого является Субъект, или требованиями законодательства Российской Федерации.

10.21. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Банк обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Банк обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

10.22. В случае подтверждения факта неточности персональных данных Банк на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим

[1] Ст. 21 № 152-ФЗ «О персональных данных»

лицом, действующим по поручению оператора) **в течение 7 (семи) рабочих дней** со дня представления таких сведений и снять блокирование персональных данных.

10.23. В случае выявления неправомерной обработки персональных данных, осуществляемой Банком или лицом, действующим по поручению оператора, Банк в срок, не превышающий 3 (**трех) рабочих дней** с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, Банк в срок, **не превышающий 10 (десяти) рабочих дней** с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение.

Об устранении допущенных нарушений или об уничтожении персональных данных Банк обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

10.24. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок**, не превышающий 30 (тридцати) дней** с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

10.25. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного выше, Банк осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных **в срок не более чем 6 (шесть) месяцев**, если иной срок не установлен федеральными законами.

11. Обязанности Банка как Оператора

11.1. В случаях, установленных законодательством Российской Федерации в области персональных данных, Банк обязан предоставить Субъекту/или его законному представителю при обращении либо при получении запроса от Субъекта/или его законного представителя информацию, предусмотренную п. 10.4. настоящей Политики.

11.2. Обязанность предоставить доказательство получения согласия Субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ, возлагается на Банк.

11.3. При сборе персональных данных Банк обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на

территории Российской Федерации, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных».

11.4. Банк, как оператор персональных данных, определяет и принимает необходимые и достаточные меры для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, а также меры по обеспечению безопасности персональных данных при их обработке. Информация о принимаемых Банком мерах содержится в разделе 13 настоящей Политики.

11.5. Банк несет иные обязанности, установленные Федеральным законом «О персональных данных».

11.6. Банк обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, **включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.**

11.7. Указанная в пункте 11.6. информация (за исключением информации, составляющей государственную тайну) передается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, в Роскомнадзор.

11.8. Порядок передачи информации в соответствии с пунктом 11.7. устанавливается совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и Роскомнадзором.

11.9. Для учета информации об инцидентах, предусмотренных частью 3.1 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ, Роскомнадзор реестр учета инцидентов в области ПДн, определяет порядок и условия взаимодействия с Банком в рамках ведения указанного реестра[2].

11.10. Информация о компьютерных инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) ПДн, в порядке, установленном совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и Роскомнадзором, передается в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности[3].

12. Сроки обработки персональных данных

12.1. Сроки обработки и хранения персональных данных определяются целями их обработки, сроком действия договорных отношений с Субъектом (или юридическим лицом, представителем которого является Субъект), сроками, установленными в согласиях на обработку персональных данных, прекращением/изменением направления основной деятельности Банка, требованиями федеральных законов Российской Федерации, сроками исковой давности, а также правилами ведения архива Банка и в соответствии с Уведомлением об обработке персональных данных, направленным Банком в Роскомнадзор.

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

[2] дополнен с 1 марта 2023 г.
[3] дополнен с 1 марта 2023 г.

персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

12.3. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

13. Обеспечение безопасности персональных данных

13.1. При обработке персональных данных Банк принимает необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006г. № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами**.** Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006г. № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом от 27.07.2006г. № 152-ФЗ или другими федеральными законами.

13.2. Обеспечение безопасности персональных данных достигается в частности следующими мерами (включая, но не ограничиваясь):

- назначение Банком ответственного за организацию обработки персональных данных;
- издание Банком документов, определяющих политику Банка в отношении обработки персональных данных, локальных актов по вопросам обработки ПДн, определяющих для каждой цели обработки ПДн категории и перечень обрабатываемых ПДн, категории Субъектов, ПДн которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права Субъектов ПДн, а также возлагающие на Банк не предусмотренные законодательством Российской Федерации полномочия и обязанности;
- обязательство Работника Банка, закрепленное в трудовом договоре, заключенном между Банком и Работником, о неразглашении конфиденциальной информации;
- обязанность Работников Банка, закрепленная во внутренних нормативных документах банка, выполнять требования по соблюдению конфиденциальности и защиты ПДн Работников и Клиентов Банка, ставших известными Работнику в рамках исполнения им своих должностных обязанностей;
- обязательное включение в заключаемые Банком с взаимодействующими организациями и физическими лицами соглашения о передаче ПДн требований соблюдения конфиденциальности (включая обязательство неразглашения) и обеспечения безопасности ПДн при их обработке;
- документальное оформление требований к безопасности обрабатываемых данных.
- ознакомление работников Банка, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе, с требованиями к защите персональных данных, с документами, определяющими политику Банка в отношении обработки персональных данных, а также

иными внутренними локальными документами Банка по вопросам обработки персональных данных и (или) обучение указанных Работников Банка;

- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006г. № 152-ФЗ, достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением 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;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Контроль за принимаемыми мерами по обеспечению безопасности персональных данных:

1) уровнем защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требований к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону № 152-ФЗ «О персональных данных» (далее - Закон №152-ФЗ) и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Банка в отношении обработки персональных данных, локальным актам Банка;

5) оценка вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав Субъектов ПДн, который может быть причинен Субъектам ПДн в случае нарушения Закона №152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом №152-ФЗ ;

6) организационно-технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимые для выполнения требований к защите ПДн, исполнение которых обеспечивают установленные Правительством РФ уровни защищенности ПДн;

7) установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

8) обнаружение фактов несанкционированного доступа к ПДн и принятие мер по недопущению подобных инцидентов в дальнейшем;

9) применение программных средств защиты информации при обработке ПДн, в т.ч. в ИСПДн;

10) восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

11) иные технические меры, разрабатываемые и принимаемые Банком в соответствии с требованиями законодательства РФ, включая нормативные акты и требования уполномоченных органов.

13.3. В целях осуществления контроля соблюдения требований законодательства Российской Федерации и координации действий по обеспечению безопасности персональных данных назначено лицо, ответственное за организацию обработки персональных данных в Банке.

13.4. Особенности защиты биометрических персональных данных.

Банком обеспечивается защита биометрических ПДн в процессе сбора биометрических персональных данных физических лиц для целей передачи в ЕБС:

- на технологическом участке сбора биометрических персональных данных физических лиц;

- на технологическом участке передачи собранных биометрических персональных данных физических лиц между структурными подразделениями Банка;

- на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью передачи в ЕБС с использованием Единой системы межведомственного электронного взаимодействия (далее - СМЭВ);

- на технологическом участке передачи биометрических персональных данных физических лиц в ЕБС с использованием СМЭВ.

В процессе обработки запросов физических лиц и их персональных данных, а также информации о степени соответствия в целях проведения идентификации физического лица без его личного присутствия с использованием биометрических персональных данных (далее - удаленная идентификация):

- на технологическом участке удаленной идентификации клиента - физического лица;

- на технологическом участке проверки результатов удаленной идентификации клиента - физического лица в Единой системе идентификации и аутентификации (далее - ЕСИА) и ЕБС;

- на технологическом участке взаимодействия Банка с ЕСИА и ЕБС.

13.5. Банк обеспечивает защиту информации при использовании ЕБС с применением средств криптографической защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, разработанных и эксплуатируемых в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным Приказом ФСБ РФ от 09.02.2005 N 66, зарегистрированным Минюстом России 3 марта

2005 года, регистрационный N 6382, 25 мая 2010 года, регистрационный N 17350 (далее - Положение ПКЗ-2005), и технической документацией на СКЗИ.

13.6. С учетом важности и необходимости обеспечения безопасности ПДн Банк постоянно совершенствует системы защиты ПДн, обрабатываемых в рамках выполнения основной деятельности Банка, принимает дополнительные меры, направленные на защиту информации о клиентах, работниках, партнерах, контрагентах и других субъектах ПДн. В целях повышения эффективности указанных систем и мер Банк руководствуется рекомендациями надзорных и контрольных органов, а также лучшими российскими и международными практиками.

14. Заключительные положения

14.1. Настоящая Политика может быть пересмотрена в случае изменения требований законодательства Российской Федерации, нормативно-правовых актов регуляторов, процессов или способов обработки персональных данных, категорий Субъектов, а также целей и сроков обработки персональных данных.

14.2. Контроль исполнения требований настоящей Политики осуществляется лицом, ответственным за организацию обработки персональных данных в Банке, под руководством Председателя Правления Банка.

14.3. Ответственность должностных лиц Банка, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн, определяется в соответствии с законодательством РФ и внутренними нормативными документами Банка.

14.4. Регламенты (порядки) реагирования на запросы/обращения субъектов персональных данных и их представителей, уполномоченных органов по поводу неточности персональных данных, неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к своим данным, а также соответствующие формы уведомлений, журналов, актов, особенности обработки персональных данных, осуществляемой с использованием и без использования средств автоматизации и т.д., установлены в Банке иными внутренними нормативными документами Банка в области обработки персональных данных.