

Приложение 1
УТВЕРЖДЕНО
Протоколом заседания Правления
АО «Севастопольский Морской банк»
от 11.12.2019 г., № 1588/1

**ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
АО «СЕВАСТОПОЛЬСКИЙ МОРСКОЙ БАНК»**

СОДЕРЖАНИЕ

| | |
|---|----|
| 1. ОБЩИЕ ПОЛОЖЕНИЯ..... | 3 |
| 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ..... | 3 |
| 3. ПРИНЦИПЫ, ЦЕЛИ И СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ..... | 4 |
| 4. ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ..... | 5 |
| 5. ПРАВА И ОБЯЗАННОСТИ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ..... | 7 |
| 6. ОСОБЕННОСТИ АВТОМАТИЗИРОВАННОЙ И НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ..... | 9 |
| 7. МЕРЫ, ПРИНИМАЕМЫЕ БАНКОМ, ПО ОБЕСПЕЧЕНИЮ ВЫПОЛНЕНИЯ ОБЯЗАННОСТИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ..... | 12 |
| 8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ..... | 13 |

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика в отношении обработки персональных данных АО «Севастопольский Морской банк» (в дальнейшем – **Политика**) разработана в соответствии с требованиями действующего законодательства Российской Федерации о персональных данных, в т.ч. Федерального закона «О персональных данных» от 27.07.2006 г. №152-ФЗ (далее – Федеральный закон 152-ФЗ).

1.2. Настоящая Политика разработана в целях реализации требований законодательства Российской Федерации в области обработки персональных данных субъектов персональных данных и раскрывает способы и принципы обработки АО «Севастопольский Морской банк» (в дальнейшем – **Банк**) персональных данных, права и обязанности Банка при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых Банком в целях обеспечения безопасности персональных данных при их обработке.

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

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Термины и определения, используемые в настоящей Политике, применяются в том значении, в котором они используются в действующем законодательстве Российской Федерации, если иное не предусмотрено настоящей Политикой.

2.2. В настоящей Политике термины используются в следующем значении:

2.2.1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

2.2.3. Внутреннее структурное подразделение – обособленное структурное подразделение в составе Банка (операционный офис, операционная касса вне кассового узла), не являющееся юридическим лицом, представляющее и защищающее его интересы в Республике Крым и г. Севастополе, действующее в пределах предоставленных Банком полномочий.

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

2.2.5. Личное дело - личная карточка сотрудника и документы по сотруднику.

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

2.2.7. 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.

2.2.8. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Сведения, относящиеся к персональным данным, устанавливаются Перечнем конфиденциальных сведений, составляющих банковскую и коммерческую тайну, а также

персональные данные, обрабатываемые в АО «Севастопольский Морской банк», утверждаемым Правлением Банка.

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

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

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

2.2.12. 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.

3. ПРИНЦИПЫ, ЦЕЛИ И СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Обработка персональных данных Банком осуществляется на основе принципов:

– законности целей и способов обработки персональных данных, законности и справедливости основы обработки персональных данных;

– соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Банка;

– соответствия содержания и объема обрабатываемых персональных данных, способов обработки персональных данных заявленным целям обработки персональных данных;

– обеспечения точности, достаточности и актуальности персональных данных по отношению к целям их обработки;

– недопустимости избыточности обрабатываемых персональных данных по отношению к заявленным целям их обработки;

– недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой;

– обеспечения уничтожения или обезличивания персональных данных по достижении целей обработки способом, исключая возможность их восстановления, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

3.2 Обработка персональных данных в Банке осуществляется в целях:

– осуществления банковских операций и банковских сделок, оказания банковских услуг и осуществления иной деятельности, предусмотренной действующим законодательством, в соответствии с выданными Банку лицензиями;

– предоставления информации, в том числе отчетности надзорным и контрольным органам, предоставляемой в соответствии с требованиями действующего законодательства Российской Федерации;

– передачи Банком персональных данных или поручения их обработки третьим лицам в соответствии с действующим законодательством Российской Федерации;

– формирования данных о кредитной истории;

– направления информации (в том числе в целях продвижения на рынке), предоставления сведений уведомительного или маркетингового характера (в том числе путем осуществления прямых контактов с клиентом/потенциальным клиентом с помощью средств связи, включая электронные средства связи, почтовые отправления, SMS-сообщения), включая сведения о новых банковских продуктах, услугах, совместных продуктах Банка и третьих лиц, продуктов (товаров, работ, услуг) третьих лиц, проводимых акциях, мероприятиях, по которым имеется предварительное согласие клиента на их

получение; рассмотрения 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;

- осуществления и исполнения функций, полномочий и обязанностей, возложенных на Банк действующим законодательством Российской Федерации, нормативными правовыми и иными актами Банка России, федеральных органов исполнительной власти, Уставом, лицензиями и внутренними документами Банка;

- обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.3 Сроки обработки персональных данных.

3.3.1 Сроки обработки и хранения персональных данных в Банке определяются в соответствии со сроком действия договора с субъектом персональных данных, сроками хранения документов, содержащих персональные данные (на бумажных и электронных носителях), установленными номенклатурой дел Банка, сроком исковой давности, в соответствии с иными требованиями, определяющими сроки обработки и хранения персональных данных, установленными актами законодательства и иными нормативно-правовыми актами, а также сроком действия согласия субъекта на обработку его персональных данных.

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

4 ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Банком осуществляется обработка персональных данных, полученных в установленном законом порядке, принадлежащих следующим субъектам персональных данных:

- кандидатам на работу в Банк;
- работникам Банка,
- клиентам – физическим лицам, индивидуальным предпринимателям (владелец счета (счета по вкладу (депозиту), открытого в Банке, заемщик, принципал, и иные лица, пользующиеся финансовыми услугами Банка),
- потенциальным клиентам – физическим лицам, индивидуальным предпринимателям;
- представителям клиентов – физических лиц, индивидуальных предпринимателей;
- поручителям – физическим лицам,
- залогодателям – физическим лицам;
- руководителям, главным бухгалтерам и иным уполномоченным представителям юридических лиц, являющихся клиентами Банка (владелец счета, открытого в Банке, заемщик, принципал и пр.), поручителями, залогодателями;
- связанным с Банком лицам (в т.ч. аффилированным лицам), близким родственникам связанных с Банком лиц;
- физическим лицам, заключившим с Банком гражданско-правовые договоры;

– уполномоченным представителям партнеров Банка, субподрядчиков, поставщиков и других контрагентов, имеющих договорные отношения с Банком.

4.2. Банком осуществляется обработка персональных данных исключительно в соответствии с целями, заранее определенными и заявленными при сборе персональных данных, а также полномочиями Банка, определенными действующим законодательством Российской Федерации и договорными отношениями с клиентами и контрагентами Банка.

4.3. Банк получает и обрабатывает персональные данные с письменного согласия субъекта персональных данных, если иное не установлено внутренними нормативными документами Банка. Получение письменных согласий осуществляется в порядке, установленном внутренними нормативными документами Банка.

4.4. Субъект персональных данных принимает решение о предоставлении его персональных данных Банку и дает согласие на их обработку свободно и по собственной воле.

4.5. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. Согласие, полученное в форме электронного документа, подписанное электронной подписью субъекта персональных данных признается равнозначным согласию в письменной форме на бумажном носителе, содержащему собственноручную подпись субъекта персональных данных.

4.6. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Банком.

4.7. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в установленном порядке. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Банк прекращает обработку указанных персональных данных в порядке, установленном законодательством.

4.8. Банк вправе обрабатывать персональные данные (продолжить обработку персональных данных) без согласия субъекта персональных данных при наличии оснований, предусмотренных законодательством¹.

4.9. Обработка биометрических персональных данных (сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность) в Банке не осуществляется.

4.10. Банком не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

4.11. Персональные данные субъекта могут быть получены банком от лица, не являющегося субъектом персональных данных, в случаях, предусмотренных законодательством² и внутренними нормативными документами Банка.

4.12. В Банке запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных Федеральным законом 152-ФЗ.

4.13. Банк вправе поручить обработку персональных данных третьей стороне, при условии получения на то согласия субъекта персональных данных, если иное не предусмотрено действующим законодательством Российской Федерации, на основании заключаемого с третьей стороной договора, условием которого является соблюдение

¹ Пункты 2 - 11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Федерального закона 152-ФЗ.

² В т.ч. на основании пунктов 2 - 11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Федерального закона №152-ФЗ.

конфиденциальности и неразглашения персональных данных. Третья сторона, осуществляющая обработку персональных данных по поручению Банка, обязана соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом 152-ФЗ, обеспечивая конфиденциальность и безопасность персональных данных при их обработке.

4.14. Хранение полученных Банком персональных данных осуществляется на бумажных и на электронных носителях (в том числе в автоматизированных информационных системах). Право доступа к персональным данным (на бумажных и электронных носителях) субъектов персональных данных имеют (получают) только те работники Банка, которым это необходимо для выполнения их должностных обязанностей. К обрабатываемым персональным данным имеют доступ только те работники Банка, которым такой доступ необходим для выполнения их должностных обязанностей и которые в законном порядке наделены соответствующими полномочиями и правами доступа к персональным данным и средствам их обработки. Доступ иных лиц к персональным данным, обрабатываемым Банком, может быть предоставлен исключительно в предусмотренных законодательством случаях и в установленном законом порядке. Банк предоставляет доступ к персональным данным, обрабатываемым Банком, представителям органов государственной власти (в том числе, контролирующим, надзорным, правоохранительным и иным органам), в объеме и порядке, установленном действующим законодательством Российской Федерации. Банк не раскрывает третьим лицам и не распространяет иным образом (без согласия субъекта персональных данных) персональные данные, если иное не предусмотрено действующим законодательством Российской Федерации и внутренними нормативными документами Банка.

4.15. Передача персональных данных третьим лицам осуществляется Банком в соответствии с требованиями действующего законодательства. Банк не вправе передавать персональные данные третьей стороне без согласия субъекта, за исключением случаев, предусмотренных законодательством Российской Федерации и внутренними нормативными документами Банка.

4.16. Обработка персональных данных Банком осуществляется как с использованием, так и без использования средств автоматизации. Автоматизированная обработка персональных данных осуществляется в АБС и иных информационных системах Банка. Защита персональных данных в АБС и иных информационных системах Банка производится согласно действующему законодательству.

5 ПРАВА И ОБЯЗАННОСТИ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Для реализации и защиты своих прав и законных интересов субъект персональных данных имеет право обратиться в Банк. Банк рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

5.2. Субъект персональных данных имеет право 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 (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом 152-ФЗ;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом 152-ФЗ или другими федеральными законами.

5.3. Сведения, указанные в п.5.2., предоставляются Банком субъекту персональных данных или его представителю при обращении в Банк либо при получении Банком запроса данных от субъекта персональных данных или его представителя в порядке, установленном внутренними нормативными документами Банка.

5.4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

5.5. Субъект персональных данных вправе требовать от Банка уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Субъект персональных данных вправе требовать извещения всех лиц, которым ранее были сообщены неверные или неполные/неточные/неактуальные персональные данные такого субъекта персональных данных, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.6. Субъект персональных данных вправе обжаловать в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Банка при обработке персональных данных такого субъекта. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке. Субъект персональных данных имеет также иные права, установленные Федеральным законом 152-ФЗ. Субъект персональных данных вправе определять своих представителей для защиты своих персональных данных.

5.7. Субъект персональных данных вправе отозвать согласие на обработку своих персональных данных, за исключением случаев, предусмотренных законодательством.

5.8. Субъект персональных данных вправе реализовывать иные права, предусмотренные законом или договором.

5.9. Субъект персональных данных (его представитель) обязан:

- своевременно предоставлять Банку сведения об изменении своих персональных данных, если такая обязанность предусмотрена договором между субъектом персональных данных и Банком, законодательством или внутренними документами Банка;
- при предоставлении Банку своих персональных данных обеспечивать на момент предоставления персональных данных их точность, достоверность и актуальность, за которые субъект несет ответственность в соответствии с действующим законодательством;
- выполнять иные обязанности, предусмотренные законом или договором.

5.10. Банк, как оператор персональных данных, имеет право:

- осуществлять проверку точности, достоверности и актуальности предоставляемых персональных данных в случаях, объеме и порядке, предусмотренных и установленных законодательством;
- отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;
- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговым, правоохранным органам и др.);
- использовать персональные данные субъекта без его согласия, в случаях предусмотренных законодательством;
- отказать субъекту персональных данных, в случае его отказа от предоставления (непредоставления) Банку своих персональных данных, обработка которых необходима для предоставления субъекту банковских продуктов и услуг, в предоставлении соответствующих банковских продуктов и услуг в законном порядке, за исключением случаев, предусмотренных законодательством;
- отстаивать свои интересы в суде;
- реализовывать иные права, предусмотренные законом или договором.

5.11. Банк, как оператор персональных данных, обязан:

- не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством;
- использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством;
- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговым, правоохранным органам и др.);
- по требованию субъекта персональных данных прекратить обработку его персональных данных, за исключением случаев, предусмотренных законодательством;
- принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом 152-ФЗ и иными законодательными и нормативными актами Российской Федерации и государственных органов;
- выполнять иные обязанности, предусмотренные законом или договором.

6 ОСОБЕННОСТИ АВТОМАТИЗИРОВАННОЙ И НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Правила автоматизированной обработка персональных данных.

6.1.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

6.1.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

6.1.3. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания посторонних лиц в помещениях, в которых размещены данные информационные системы.

6.1.4. Компьютеры и(или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены

индивидуальными паролями доступа³. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) учетными записями, запрещается.

6.1.5. Порядок обработки персональных данных в информационных системах с использованием средств автоматизации.

6.5.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями Приказа ФСТЭК 21.

6.5.2. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

– настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;

– охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

6.1.6. Общие требования по защите персональных данных в автоматизированных системах.

6.6.1. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

6.6.2. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

– использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

– недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– постоянное использование антивирусного обеспечения для обнаружения «зараженных» файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

6.1.7. При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– предоставление лицам, допущенным к работе с персональными данными в информационной системе, соответствующих прав доступа;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– описание системы защиты персональных данных.

6.1.8. Банком в рамках Политики информационной безопасности разрабатываются внутренние нормативные документы, обеспечивающие защиту информации, в т.ч. и персональных данных, в информационной системе Банка.

6.2 Правила неавтоматизированной обработки персональных данных.

³ Требования к количеству и составу символов пароля устанавливаются внутренними нормативными документами Банка.

6.2.1. Неавтоматизированная обработка персональных данных осуществляется в виде обработки документов на бумажных носителях. Персональные данные на бумажных носителях обрабатываются работниками в помещениях подразделений Банка, доступ в которые устанавливается в соответствии с Инструкцией о пропускном режиме АО «Севастопольский Морской банк». При работе с документами, содержащими персональные данные, работник руководствуется пп. 2.14.2 – 2.14.3, 2.15 Регламента конфиденциального делопроизводства АО «Севастопольский Морской банк».

6.2.2. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

6.2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также внутренними нормативными документами Банка.

6.2.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (в дальнейшем – **типовая форма**), должны соблюдаться следующие условия:

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных – при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.2.5. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в Банк, или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена внутренним нормативным документом Банка, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных в Банк, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных в Банк.

6.2.6. Уничтожение или обезличивание части персональных данных, если это допускается носителем, должно производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

6.2.7. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на носителе, а если это не допускается особенностями носителя, - путем фиксации на том же носителе сведений о вносимых в них изменениях, либо путем изготовления нового носителя с уточненными персональными данными.

6.2.8. Документы, содержащие персональные данные, должны храниться в служебных помещениях в запираемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

6.2.9. Оставлять бумажные носители персональных данных на рабочих местах без присмотра запрещается.

7 МЕРЫ, ПРИНИМАЕМЫЕ БАНКОМ, ПО ОБЕСПЕЧЕНИЮ ВЫПОЛНЕНИЯ ОБЯЗАННОСТИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1 Организация и проведение мероприятий по обеспечению безопасности и защиты персональных данных в Банке осуществляется в соответствии с настоящей Политикой и иными внутренними документами Банка.

7.2 В целях обеспечения безопасности и защиты персональных данных при их обработке Банк предпринимает необходимые и достаточные правовые, организационные и технические меры (или обеспечивает их принятие) для защиты персональных данных от неправомерного (несанкционированного) или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. Указанные меры осуществляются Банком в соответствии с требованиями законодательства⁴, нормативно-правовых и иных актов в области обработки и защиты персональных данных.

7.3 В состав и перечень необходимых и достаточных для обеспечения выполнения требований законодательства мер, принимаемых Банком и направленных на обеспечение безопасности и защиты персональных данных, входят в т.ч. следующие:

- назначается Ответственное лицо (ответственные лица) за организацию обработки персональных данных;
- издаются внутренние нормативные документы по вопросам обработки персональных данных, а также внутренние нормативные документы, устанавливающие процедуры, направленные на предотвращение и выявление нарушений действующего законодательства Российской Федерации, устранение последствий таких нарушений;
- определяются угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;
- к информации, содержащей персональные данные, применяется режим конфиденциальности, то есть обязательное соблюдение лицом, получившим доступ к персональным данным, требования не допускать их распространения без согласия субъекта персональных данных, кроме случаев обезличивания (когда невозможно определить принадлежность персональных к конкретному субъекту), общедоступности (когда доступ к персональным данным предоставлен с согласия субъекта персональным данным неограниченному кругу лиц) или наличия иного законного основания;
- запросы сотрудников Банка на выгрузку информации из баз данных Банка, содержащих персональные данные, в обязательном порядке согласовываются с ответственным лицом, назначаемым в соответствии с абзацем вторым п. 7.3 настоящей

⁴ В т.ч. в соответствии со статьей 19 Федерального закона 152-ФЗ.

политики (форма запроса и согласования приведены в **Приложении 1** к настоящей Политике);

- при обработке персональных данных, в том числе в информационных системах персональных данных, применяются организационные и/или технические меры по обеспечению их безопасности, необходимые для выполнения требований к защите персональных данных;

- применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;

- на регулярной основе проводится оценка эффективности принимаемых мер по обеспечению безопасности персональных данных, в том числе до ввода в эксплуатацию информационной системы персональных данных;

- осуществляется учет машинных носителей персональных данных;

- осуществляется принятие мер в целях исключения фактов несанкционированного доступа к персональным данным;

- устанавливаются правила доступа к персональным данным, в том числе обрабатываемым в информационной системе персональных данных, а также проводится регистрация и учет действий, совершаемых с персональными данными в информационной системе персональных данных;

- устанавливается система доступа в помещения и здания Банка, организуется их охрана в рабочее и нерабочее время;

- хранение материальных носителей персональных данных осуществляется в закрытых шкафах, ящиках, сейфах;

- внедряются и применяются средства минимизации полномочий доступа, средства разграничения доступа (идентификация и аутентификация субъектов доступа, ограничения количества неудачных попыток доступа) и другие меры защиты;

- обеспечивается возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- все работники Банка ознакомляются под подпись с настоящей Политикой и внутренними нормативными документами Банка по вопросам обработки персональных данных (**Приложение 2**). Расписки об ознакомлении помещаются на хранение в личные дела сотрудников;

- осуществляется внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону 115-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, внутренним нормативным документам Банка.

7.4 Каждый сотрудник Банка несет ответственность за выполнение и соблюдение требований настоящей Политики. Сотрудники, допустившие нарушения требований настоящего Регламента, привлекаются к ответственности в порядке, установленном действующим законодательством Российской Федерации.

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

8 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Политика вступает в силу с момента ее утверждения.

7.2. Внесение изменений и дополнений к настоящей Политике, утверждение настоящей Политики в новой редакции осуществляется по решению Правления Банка.

7.3. Политика пересматривается по мере необходимости. Причинами пересмотра Политики могут послужить изменения в информационной инфраструктуре Банка и/или внедрение новых информационных технологий, а также изменения в действующем законодательстве Российской Федерации.

7.4. Ответственность за пересмотр, дополнения и изменения настоящей Политики возлагается на Отдел информационной безопасности.

7.5. В случае внесения изменений и дополнений в законодательство Российской Федерации, в том числе нормативные акты Банка России, а также внутренние нормативные документы Банка, настоящая Политика до приведения её соответствие с указанными документами действует в части, им не противоречащей.

Приложение 1
к Политике в отношении обработки
персональных данных
АО «Севастопольский Морской банк»

Заявка на выгрузку персональных данных

Предмет запроса: _____

Цель запроса: _____

Подразделение: _____

Запрашивает данные: _____
(должность, ФИО сотрудника полностью)

Руководитель подразделения: _____ . ____ . 20 ____ г. _____ / _____
(подпись) (расшифровка подписи)

СОГЛАСОВАНО:

_____ . ____ . 20 ____ г. _____ / _____
(должность ответственного лица за организацию обработки ПД) (подпись) (расшифровка подписи)

ОТМЕТКИ ОБ ИСПОЛНЕНИИ ЗАЯВКИ:

Выгрузку персональных данных, согласно заявке, произвел:
_____ . ____ . 20 ____ г. _____ / _____
(должность) (подпись) (расшифровка подписи)

Приложение 2
к Политике в отношении обработки
персональных данных
АО «Севастопольский Морской банк»

РАСПИСКА ОБ ОЗНАКОМЛЕНИИ
с внутренними нормативными документами АО «Севастопольский Морской банк» в сфере
обработки персональных данных

Я, _____
(ФИО, должность)

_____ ,
ознакомлен (-а) со следующими внутренними нормативными документами банка в сфере
обработки персональных данных:

- Политикой в отношении обработки персональных данных АО «Севастопольский Морской банк»;
- Регламентом обработки и обеспечения безопасности персональных данных сотрудников АО «Севастопольский Морской банк»;
- Регламентом обработки и обеспечения безопасности персональных данных, обрабатываемых в АО «Севастопольский Морской банк»;
- Перечнем конфиденциальных сведений, составляющих банковскую и коммерческую тайну, а также персональные данные, обрабатываемые в АО «Севастопольский Морской банк».

(дата)

_____/_____
(подпись) (расшифровка подписи)