



**Публичное акционерное общество
«Санкт-Петербургский Индустриальный Акционерный Банк»
(ПАО БАНК «СИАБ»)**

УТВЕРЖДЕНА
решением Совета директоров ПАО БАНК «СИАБ»
30.06.2023
Протокол № 12/2023 от 03.07.2023

**Политика
в отношении обработки персональных данных
в ПАО БАНК «СИАБ»**

**Санкт-Петербург
2023 год**

Оглавление:

Номер раздела	Наименование раздела:	Стр.
1	Общие положения	3
2	Категории субъектов персональных данных, персональные данные которых обрабатываются Банком	5
3	Цели обработки персональных данных	5
4	Перечень персональных данных, обрабатываемых в Банке	6
5	Основные принципы и условия обработки персональных данных	6
6	Порядок обработки персональных данных	8
7	Права субъекта персональных данных	10
8	Обязанности Банка, как оператора	12
9	Меры Банка, направленные на обеспечение выполнения обязанностей по обработке персональных данных	12
10	Меры Банка, направленные на обеспечение выполнения обязанностей по защите персональных данных	13
11	Ответственность	13
12	Раскрытие информации в отношении обработки персональных данных	14

1. Общие положения

1.1. Настоящая Политика является основополагающим внутренним документом ПАО БАНК «СИАБ» (далее – Банк), определяющим цели, задачи и принципы политики в отношении обработки и обеспечения безопасности персональных данных.

Настоящая Политика вступает в действие с даты утверждения Советом директоров Банка и является обязательной для соблюдения всеми сотрудниками Банка. Со дня утверждения настоящей Политики утрачивает действие «Политика в отношении обработки персональных данных», утвержденная 26.03.2018.

Целью настоящей Политики является установление основных принципов и подходов к обработке и обеспечению безопасности персональных данных в Банке.

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

Политика обязательна для ознакомления и исполнения всеми сотрудниками, допущенными к обработке персональных данных в Банке.

На основании приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор) Банк включен в реестр операторов, осуществляющих обработку персональных данных.

При изменениях законодательства Российской Федерации и нормативных правовых актов (далее – законодательство РФ) настоящая Политика подлежит пересмотру, а до момента внесения в нее изменений - применяется в части, не противоречащей законодательству РФ. При изменении Организационной структуры Банка настоящая Политика не требует внесения изменений за исключением случаев, когда невозможно однозначно установить передачу полномочий и ответственности подразделений, обозначенных в настоящей Политике.

Пересмотр и обновление настоящей Политики осуществляется по результатам анализа актуальности, достаточности и эффективности используемых мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Банка, а также по результатам других контрольных мероприятий.

Изменения в настоящую Политику вносятся по инициативе Директора Департамента контроля информации, Вице-Президента по безопасности, Советника по информационной безопасности.

1.2. Политика разработана в соответствии с действующим законодательством РФ, в частности, использованы:

Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;

Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ);

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ);

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе»;

Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;

Федеральный закон от 28.06.2014 № 173-ФЗ «Об особенностях осуществления финансовых операций с иностранными гражданами и юридическими лицами, о внесении изменений в Кодекс Российской Федерации об административных правонарушениях и признании утратившими силу отдельных положений законодательных актов Российской Федерации»;

Федеральный закон от 03.07.2016 № 230-ФЗ «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» (далее - Федеральный закон № 230-ФЗ);

Федеральный закон от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»;

Постановление 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»;

Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без

использования средств автоматизации»;

Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление № 1119);

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»;

Приказ 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 Минцифры России от 10.09.2021 № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации».

Применяемые нормативные документы используются с учетом последующих изменений и дополнений.

1.3. На основе настоящей Политики утверждаются иные внутренние документы Банка по вопросам обработки и защиты персональных данных в Банке.

1.4. Используемые термины и определения:

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

биометрические персональные данные - сведения, 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 - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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

конфиденциальность персональных данных – обязательное для соблюдения Банком или иным лицом, получившим доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных или наличия иного законного основания, предусмотренного законодательством РФ;

обезличивание - 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, а также путем смешанной обработки, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

ответственный за организацию обработки персональных данных - должностное лицо, назначенное приказом Президента-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 законодательством РФ в области персональных данных;

персональные данные (далее также - ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

персональные данные, разрешенные субъектом персональных данных для распространения, - 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 Федеральным законом № 152-ФЗ;

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

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

специальная категория персональных данных - сведения касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

субъект персональных данных - 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;

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.

2. Категории субъектов персональных данных, персональные данные которых обрабатываются Банком

2.1. Банком осуществляется обработка полученных в установленном законом порядке персональных данных, принадлежащих:

– кандидатам на работу и сотрудникам Банка, в том числе уволенным, близким родственникам, членам семьи сотрудников Банка, практикантам;

– потенциальным клиентам (в т.ч. заемщикам), клиентам (в т.ч. заемщикам) - физическим лицам, индивидуальным предпринимателям (физическим лицам, зарегистрированным в установленном порядке и осуществляющим предпринимательскую деятельность без образования юридического лица), физическим лицам, занимающимся в установленном законодательством РФ порядке частной практикой, физическим лицам - выгодоприобретателям, бенефициарным владельцам, представителям, поручителям, залогодателям, бывшим клиентам, заявителям не ставшим клиентами;

– пользователям сайта Банка;

– контрагентам (физическим лицам) - лицам, осуществляющим выполнение работ (оказание услуг) и заключившим с Банком договоры гражданско-правового характера;

– представителям контрагентов - представителям лиц, заключивших с Банком договоры гражданско-правового характера;

– клиентам других юридических лиц, обработка персональных данных для которых осуществляется по поручению указанных юридических лиц в соответствии с законодательством РФ;

– акционерам и членам Совета директоров Банка;

– посетителям Банка;

– иным физическим лицам, вступившим или имеющим намерение вступить в договорные отношения с Банком;

– иным физическим лицам, обращающимся в Банк (при необходимости обработки их персональных данных для целей выполнения их запросов).

3. Цели обработки персональных данных

3.1. Обработка персональных данных в информационной системе персональных данных сотрудниками Банка осуществляется в целях осуществления Банком деятельности на финансовых рынках в соответствии с имеющимися лицензиями, в том числе:

– осуществления банковских операций и иной деятельности, предусмотренной Уставом ПАО БАНК «СИАБ», действующим законодательством РФ;

– заключения, исполнения и прекращения гражданско-правовых договоров с физическими

лицами и с юридическими лицами;

- организации кадрового учета сотрудников Банка, исполнения делопроизводства, при обучении сотрудников;

- предоставления информации о Банке, его продуктах и услугах, усовершенствования продуктов и (или) услуг Банка и для разработки новых продуктов и (или) услуг Банка, ведения статистики о пользователях сайта, мобильного приложения Банка, хранения персональных настроек пользователей, отслеживания состояния сессии доступа пользователей, предоставления дистанционного обслуживания, формирования списка интересов и т.п.;

- формирования и предоставления отчетности регулирующим органам в соответствии с требованиями законодательства РФ;

- улучшения клиентского опыта, качества обслуживания Банком, организации улучшения программного обеспечения Банка;

- продвижения продуктов и услуг третьих лиц, в том числе передачи информационных и рекламных сообщений об услугах третьих лиц путем осуществления прямых контактов с помощью средств связи, проведения стимулирующих мероприятий;

- создания информационных систем данных, анализа, моделирования, прогнозирования, построения математических моделей, профилирования, таргетирования, построения скоринг-моделей, их использования и передачи результатов обработки информации третьим лицам, обогащения и сегментации для формирования и адаптации возможных услуг и предложений Банка и третьих лиц, анализа агрегированных и анонимных данных, статистических и исследовательских целей;

- обеспечения охраны помещений и хранилищ, сохранности денег, ценностей и оборудования, контроля и управления доступом на территорию Банка, к специалистам по обслуживанию клиентов, к индивидуальным сейфовым ячейкам;

- установления личности субъекта персональных данных, в случаях, предусмотренных законодательством.

- осуществления обработки, включая сбор и хранение, биометрических персональных данных (данных изображения лица, полученных с помощью фото- и видеоустройств, данных голоса, полученных с помощью звукозаписывающих устройств) с целью их передачи в единую биометрическую систему;

- проверки биометрических персональных данных и передачи информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в государственных органах, банках и иных организациях, указанных в абз.1 ч.1 ст.14.1 Федерального закона № 149-ФЗ, в единой биометрической системе;

- размещения или обновления в электронной форме в единой системе идентификации и аутентификации (ЕСИА), а также в единой информационной системе персональных данных, обеспечивающей сбор, обработку, хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (ЕБС) сведений, необходимых для регистрации в ней клиента - физического лица, и сведений, предусмотренных абзацем вторым пп.1 п.1 ст.7 Федерального закона № 115-ФЗ.

4. Перечень персональных данных, обрабатываемых в Банке

4.1. Перечень персональных данных, в том числе биометрических персональных данных, специальных категорий персональных данных, обрабатываемых в Банке, определяется в соответствии с законодательством РФ и внутренними нормативными документами Банка с учетом целей обработки персональных данных и с направлением Банком Уведомления об обработке персональных данных в Роскомнадзор.

5. Основные принципы и условия обработки персональных данных

5.1. Основными принципами обработки персональных данных в Банке являются:

- обработка персональных данных должна осуществляться на законной и справедливой основе. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- обработка персональных данных должна ограничиваться достижением конкретных,

заранее определенных и законных целей;

- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- обработке подлежат только персональные данные, которые отвечают целям их обработки;

- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Банк принимает необходимые меры, либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

Хранение персональных данных должно осуществляться 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.

5.2. Условиями обработки персональных данных в Банке являются:

- 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 РФ на Банк функций, полномочий и обязанностей;

- обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве;

- 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;

- 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 № 230-ФЗ, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

- обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

5.3. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн) и которые используются Банком для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

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

Обработка сведений о состоянии здоровья допускается только в случаях если:

- субъект персональных данных дал согласие в письменной форме на обработку своих ПДн;

- персональные данные сделаны общедоступными субъектом персональных данных;

– обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством РФ;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

– обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

Обработка специальных категорий персональных данных незамедлительно прекращается, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено Федеральным законом № 152-ФЗ.

5.5. Банк до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

5.6. Банк не использует персональные данные для принятия решений, основанных на исключительно автоматизированной обработке.

5.7. Банк вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом № 152-ФЗ, на основании заключаемого с этим лицом договора (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ. В поручении оператора должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, требования, предусмотренные ч. 5 ст. 18 и ст. 18.1 Федерального закона № 152-ФЗ, обязанность по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии со ст.6 указанного Федерального закона, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст.19 Федерального закона 152-ФЗ, в том числе требование об уведомлении оператора о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона № 152-ФЗ.

5.8. Лицо, осуществляющее обработку персональных данных по поручению Банка, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5.9. В случае, если Банк поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Банк. Лицо, осуществляющее обработку персональных данных по поручению Банка, несет ответственность перед Банком.

6. Порядок обработки персональных данных

6.1. Банк осуществляет обработку персональных данных с использованием средств автоматизации и без использования средств автоматизации, а также смешанную обработку персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, анализ и использование, передачу (распространение, предоставление, доступ) и поручение обработки персональных данных третьим лицам, получение от третьих лиц, обезличивание, блокирование, удаление, уничтожение персональных данных в сроки, необходимые для достижения целей обработки персональных данных.

6.2. В Банке запрещается принятие решений на основании исключительно автоматизированной обработки персональных данных, которые порождают юридические последствия в отношении субъекта персональных данных, или иным образом затрагивают его

права и законные интересы, кроме случаев и условий, предусмотренных законодательством РФ в области персональных данных.

Персональные данные не раскрываются третьим лицам без согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ.

6.3. Представители органов государственной власти (в том числе, контролирующих, надзорных, правоохранительных, дознания и следствия и иных уполномоченных органов по основаниям, предусмотренным законодательством РФ) получают доступ к персональным данным, обрабатываемым в Банке, в объеме и порядке, установленном законодательством РФ.

6.4. В ходе своей деятельности Банк может осуществлять трансграничную передачу персональных данных в соответствии с требованиями Федерального закона № 152-ФЗ, с учетом целей обработки персональных данных, указанных в разделе 3 настоящей Политики, и в соответствии с Уведомлением об обработке персональных данных, направленным Банком в Роскомнадзор.

6.5. Обработка персональных данных в Банке осуществляется с согласия субъекта персональных данных кроме случаев, установленных законодательством РФ, с соблюдением требований конфиденциальности персональных данных, установленных ст.7 Федерального закона № 152-ФЗ, а также принятием мер, направленных на обеспечение выполнения обязанностей по обработке и защите персональных данных, установленных законодательством РФ. При этом:

- обработка специальных категорий персональных данных, биометрических данных, трансграничная передача персональных данных осуществляется только при наличии согласия в письменной форме субъекта персональных данных, оформленного в соответствии с п.4 ст.9 Федерального закона № 152-ФЗ;

- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется на основании согласия, которое оформляется отдельно от иных согласий субъекта персональных данных. В данном согласии субъект имеет право определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, а также установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц;

- обработка персональных данных субъектов, не достигших совершеннолетия, осуществляется при наличии согласия законного представителя такого субъекта.

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

6.7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных установлен Федеральным законом № 152-ФЗ, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.8. В случае подтверждения факта неточности персональных данных или неправомерности их обработки персональные данные подлежат актуализации Банком, а обработка должна быть прекращена, соответственно.

6.9. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, в установленные законодательством РФ сроки:

- если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- если Банк не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или иными федеральными законами;

- если иное не предусмотрено иным соглашением между Банком и субъектом персональных данных.

6.10. Банк предоставляет субъекту персональных данных или его представителю сведения,

касающиеся обработки его персональных данных, по соответствующему обращению или запросу субъекта персональных данных или его представителя в доступной форме и не содержащие персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.11. Запрос субъекта персональных данных на получение сведений, касающихся обработки его персональных данных Банком, должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, а также, в случае обращения представителя, реквизиты доверенности или иного документа, подтверждающего полномочия представителя субъекта персональных данных;

- сведения, подтверждающие участие субъекта персональных данных в отношениях с Банком (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Банком;

- подпись субъекта персональных данных или его представителя;

6.12. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством РФ.

6.13. Обращение субъекта персональных данных или его законного представителя в Банк в целях реализации его прав, установленных Федеральным законом № 152-ФЗ, осуществляется в письменном виде по установленной в Банке форме с предъявлением документа, удостоверяющего личность субъекта персональных данных (за исключением, когда обращение осуществляется в форме электронного документа подписанного электронной подписью в соответствии с законодательством РФ), а в случае обращения представителя (законного представителя) – с предъявлением паспорта представителя и доверенности или иного документа, подтверждающего полномочия представителя субъекта персональных данных. Субъект персональных данных вправе обратиться в Банк с претензией в любой офис Банка (информация о них размещена на сайте Банка <https://siab.ru/>).

6.14. Банк рассматривает обращение субъекта персональных данных/отзыв согласия на обработку персональных данных и предоставляет на него ответ в соответствии с законодательством РФ.

7. Права субъекта персональных данных

7.1. 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 сотрудников Банка), которые имеют доступ к персональным данным или которым могут быть переданы или раскрыты персональные данные на основании договора с Банком или на основании федерального закона;

- перечень и категории обрабатываемых персональных данных, относящихся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом № 152-ФЗ;

- 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 персональных данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка поручена или будет поручена такому лицу;

- наличие исключительно автоматизированного процесса принятия решений Банком на основании персональных данных;

- иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

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

7.3. Субъект персональных данных имеет право потребовать исправить свои персональные данные в случае обнаружения неточностей в составе персональных данных, которые обрабатываются Банком, а также внести дополнения в персональные данные, в том числе посредством предоставления дополнительного заявления.

7.4. Субъект персональных данных имеет право отозвать свое согласие на обработку персональных данных и потребовать удалить свои персональные данные из систем Банка, если персональные данные больше не требуются для целей, в которых они были получены, и у Банка отсутствуют имеющие законные основания для обработки его данных.

7.5. Субъект персональных данных имеет право потребовать ограничить обработку его персональных данных в целях рекламных предложений Банка.

7.6. Субъект персональных данных имеет право обратиться к Банку с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения.

7.7. В силу ч.4 ст.9 Федерального закона № 152-ФЗ согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой форме, позволяющей подтвердить факт его получения, но при этом оно должно содержать исчерпывающий перечень информации:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе; фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

- цель обработки персональных данных и перечень персональных данных, на обработку которых дается согласие;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

- подпись субъекта персональных данных.

7.8. Вышеуказанное согласие не предполагает разрешение такой функции обработки персональных данных как распространение. Федеральным законом № 152-ФЗ в ст.10.1 установлено, что согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

7.9. Банк (оператор) обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

7.10. Требования к содержанию такого согласия устанавливаются Банком во внутренних нормативных документах.

7.11. Согласие на распространение информации, содержащей ПДН, должно включать:

- фамилию, имя, отчество (при наличии) субъекта персональных данных;

- контактную информацию (номер телефона, адрес электронной почты или почтовый адрес субъекта персональных данных);

- сведения об операторе, которым будут распространяться персональные данные;

- сведения об информационных ресурсах Банка (оператора), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных;

- цель (цели) обработки персональных данных;
- категории и перечень персональных данных, на обработку которых дается согласие;
- категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов;
- условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (заполняется по желанию субъекта персональных данных);
- срок действия согласия.

7.12. Субъект персональных данных имеет также иные права, установленные законодательством РФ.

8. Обязанности Банка, как оператора

8.1. В случаях, установленных законодательством РФ в области персональных данных, Банк обязан предоставить субъекту персональных данных или его представителю при обращении либо при получении запроса от субъекта персональных данных или его представителя соответствующую информацию.

8.2. Банк при сборе персональных данных, в том числе посредством сети Интернет, обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

8.3. Банк несет иные обязанности, установленные законодательством РФ.

9. Меры Банка, направленные на обеспечение выполнения обязанностей по обработке персональных данных

9.1. Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом № 152-ФЗ или другими федеральными законами.

9.2. В Банке принимаются следующие меры по обеспечению выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ в области обработки персональных данных:

– назначается должное лицо, ответственное за организацию обработки персональных данных;

– издаются: настоящая Политика в отношении обработки персональных данных, внутренние нормативные документы по вопросам обработки персональных данных, а также внутренние нормативные документы, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

– применяется комплекс правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со ст.19 Федерального закона 152-ФЗ, направленных на нейтрализацию актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных Банка;

– проводится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых Банком (оператором) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ.

– осуществляется внутренний контроль и (или) аудит соответствия обработки персональных данных в Банке Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, внутренним нормативным документам в области обработки и обеспечения безопасности персональных данных;

– ведется анализ создаваемых в Банке продуктов и процессов на предмет надлежащей обработки персональных данных;

– осуществляется ознакомление сотрудников Банка, непосредственно осуществляющих обработку персональных данных, с законодательством РФ о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политикой, внутренними нормативными документами Банка по вопросам обработки персональных данных.

10. Меры Банка, направленные на обеспечение выполнения обязанностей по защите персональных данных

10.1. Организованная Банком система защиты информационных систем персональных данных включает в себя комплекс правовых, организационных и технических мер, направленных на нейтрализацию актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных Банка, и учитывает особенности информационной инфраструктуры Банка и архитектуры информационных систем персональных данных Банка, используемых информационных технологий в информационных системах Банка.

10.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Банка определяются и применяются с учетом установленных уровней защищенности персональных данных при их обработке в информационных системах персональных данных в соответствии с Постановлением № 1119.

10.3. Выбор и внедрение средств защиты в рамках системы защиты персональных данных при их обработке в информационных системах персональных данных Банка осуществляется в соответствии с требованиями законодательства РФ в области персональных данных.

10.4. Защита персональных данных при их обработке в информационных системах персональных данных Банка от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, обеспечивается применением взаимосвязанной совокупности мер и средств защиты, в частности:

– определяются угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

– применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, направленные на нейтрализацию актуальных угроз безопасности персональных данных в соответствии с законодательством РФ;

– применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации, предназначенные для нейтрализации актуальных угроз безопасности;

– осуществляется оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– осуществляется учет машинных носителей персональных данных;

– проводятся мероприятия по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих 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;

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

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

– осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

11. Ответственность

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

11.2. Каждый сотрудник Банка, получающий для работы документ, содержащий персональные данные, несет ответственность за сохранность и конфиденциальность

информации.

11.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

11.4. За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы с информацией ограниченного доступа Банк вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

12. Раскрытие информации в отношении обработки персональных данных

12.1. Обеспечение реализации прав субъектов персональных данных осуществляется посредством исполнения запросов, направляемых субъектами Банку на:

- почтовый адрес: Российская Федерация, 196084, Санкт-Петербург, ул. Черниговская, д. 8, лит. А, пом. 1-Н;

- электронный адрес: privacy@siab.ru.

12.2. Настоящая Политика подлежит публикации на официальном сайте Банка по адресу <https://siab.ru/>.

Доступ к настоящей Политике для ознакомления с ней предоставляется неограниченному кругу лиц.