



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

УТВЕРЖДЕНА
решением Совета директоров ПАО БАНК «СИАБ»
«26» марта 2018г.
Протокол от «28» марта 2018г. № 10 /2018

**Политика
в отношении обработки персональных данных**

**Санкт-Петербург
2018**

Оглавление:

Номер раздела	Наименование раздела:	Стр.
1	Общие положения	3
2	Правовые основания обработки персональных данных	5
3	Цели обработки персональных данных	5
4	Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных	5
5	Порядок и условия обработки персональных данных	6
6	Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным	7
7	Перечень мер, направленных на выполнение обязанностей Банка как оператора обработки персональных данных	7
8	Ответственность за нарушение требований настоящей Политики	8
9	Раскрытие информации в отношении обработки персональных данных	8

1. Общие положения

1.1. Настоящая Политика является основным внутренним нормативным документом ПАО БАНК «СИАБ» (далее – Банк), определяющим общее управление, цели, задачи и принципы в отношении обработки и обеспечения информационной безопасности персональных данных, а так же категории обрабатываемых в Банке персональных данных.

Действие настоящей Политики распространяется на все внутренние процессы Банка.

Настоящая Политика вступает в действие с даты утверждения и является обязательной для соблюдения всеми сотрудниками Банка, имеющими доступ к персональным данным.

Со дня начала действия настоящей Политики утрачивает действие «Политика в отношении обработки персональных данных», утвержденная 30.12.2014.

При изменениях законодательства Российской Федерации и нормативных правовых актов (далее – законодательство РФ) настоящая Политика подлежит актуализации, а до момента внесения в нее изменений - применяется в части, не противоречащей законодательству РФ.

Изменения в настоящую Политику вносятся по инициативе Департамента контроля информации, а также лица, ответственного за обеспечение информационной безопасности персональных данных в Банке.

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

Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» (далее – Закон о банках № 395-1);

Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах» (далее – Федеральный закон № 208-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 30.12.2004 № 218-ФЗ «О кредитных историях» (далее – Федеральный закон № 218-ФЗ);

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

Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (далее – Трудовой кодекс);

Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ (далее – Налоговый кодекс);

Приказ ФСФР России от 30.07.2013 № 13-65/пз-н «О порядке открытия и ведения держателями реестров владельцев ценных бумаг лицевых и иных счетов и о внесении изменений в некоторые нормативные правовые акты Федеральной службы по финансовым рынкам» (далее - правовые акты Федеральной службы по финансовым рынкам).

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:

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

• Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

• Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

• Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

• Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

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

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

1.5. Банк вправе:

- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено требованиями законодательства РФ (налоговые, правоохранительные органы и др.);

- отказывать в предоставлении персональных данных субъекту в случаях, предусмотренных законодательством РФ;

- производить обработку персональных данных субъекта без его согласия в случаях, предусмотренных законодательством РФ;

- защищать свои права и законные интересы в судебном порядке.

1.6. Банк обязан:

- производить обработку персональных данных при наличии правовых оснований;

- принимать меры по обеспечению конфиденциальности и безопасности персональных данных;

- обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных;

- сообщать субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя;

- предоставлять ответы на запросы субъектов персональных данных;

- принимать меры по устранению нарушений законодательства РФ, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных в случае их выявления;

- выполнять иные предусмотренные законодательством РФ обязанности.

1.7. Субъект персональных данных, обладает правами, предусмотренными законодательством РФ, в том числе:

- получать информацию, касающуюся обработки его персональных данных (подтверждение факта обработки персональных данных; правовые основания и цели обработки персональных данных; способы обработки персональных данных; наименование и место нахождения Банка, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании действующего законодательства Российской Федерации; обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен действующим законодательством Российской Федерации; сроки обработки персональных данных, в том числе сроки их хранения; порядка осуществления субъектом персональных данных своих 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; иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами);

- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- обжаловать в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;

- защищать свои права и законные интересы, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

1.8. Банк 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 законодательством Российской Федерации.

1.9. В случаях, когда предоставление персональных является обязательным в соответствии с законодательством Российской Федерации, Банк разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

1.10. Банк не предоставляет третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

2. Правовые основания обработки персональных данных

2.1. Основанием для обработки Банком персональных данных являются:

- законодательные и нормативные акты, перечисленные в п.1.2 настоящей Политики;
- правовые акты Федеральной службы по финансовым рынкам;
- Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг»;
- Положение Банка России от 30.12.2014 № 454-П «О раскрытии информации эмитентами эмиссионных ценных бумаг»;
- Устав ПАО БАНК «СИАБ»;
- договоры, заключенные между Банком и субъектами персональных данных;
- Согласие на обработку персональных данных субъекта персональных данных.

3. Цели обработки персональных данных

3.1. Обработка персональных данных осуществляется в целях:

- осуществления банковской деятельности в соответствии с требованиями законодательства РФ;
- осуществления финансово-хозяйственной деятельности Банка;
- обязательного раскрытия информации в соответствии с законодательством РФ, в том числе законодательства, регламентирующего деятельность на рынке ценных бумаг, законодательства о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма;
- осуществления прав владельцев ценных бумаг, выпущенных (выданных) Банком и иными лицами;
- соблюдения требований налогового, гражданского, трудового законодательства РФ;
- рекламы услуг Банка.

3.2. Обработка персональных данных в Банке ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями их сбора. Объем, характер обрабатываемых персональных данных, способы их обработки в Банке соответствуют заявленным целям обработки персональных данных.

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

4.1. 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.

4.2. В Банке обрабатываются персональные данные, принадлежащие следующим категориям субъектов:

- работникам Банка, бывшим работникам, кандидатам на замещение вакантных должностей;
- клиентам и контрагентам Банка (физическим лицам);
- представителям/работникам клиентов и контрагентов Банка (юридических лиц);
- членам и кандидатам в члены органов управления и контроля Банка;
- аффилированным лицам Банка;
- лицам, у которых может быть заинтересованность в совершении Банком сделок согласно ст. 81 Федерального закона № 208-ФЗ;
- руководителям, работникам, участникам (акционерам, товарищам, пайщикам) контрагентов (потенциальных контрагентов) Банка, юридических лиц - клиентов (потенциальных клиентов) Банка;
- выгодоприобретателям, распорядителям, бенефициарным владельцам, поручителям клиентов Банка.

4.3. Перечень обрабатываемых персональных данных применительно к конкретным целям и по каждой из категорий субъектов установлен во внутренних нормативных документах Банка.

4.4. В Банке запрещена обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

4.5. Обработка данных о состоянии здоровья допускается только в отношении персональных данных работников и кандидатов на работу в подразделения Банка в целях исполнения двусторонних договоров, регулирующих трудовые отношения Банка и его работника, а также в целях исполнения трудового законодательства Российской Федерации.

5. Порядок и условия обработки персональных данных

5.1. Обработка персональных данных в Банке осуществляется следующими способами: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ, распространение в случаях, предусмотренных законодательством РФ), обезличивание, блокирование, удаление, уничтожение.

5.2. В случае необходимости взаимодействия с третьими лицами в рамках достижения целей обработки персональных данных определяются условия передачи персональных данных в адрес третьих лиц (например, наличие договора поручения на обработку персональных данных, содержащего цели осуществляемой передачи, объем передаваемых персональных данных, перечень действий по их обработке, способы и иные условия обработки, включая требования к защите обрабатываемых персональных данных).

5.3. Трансграничная передача персональных данных осуществляется в соответствии с условиями предоставления услуг и соблюдением требований законодательства Российской Федерации.

5.4. Сроки обработки персональных данных определяются в соответствии со сроком действия договора с субъектом персональных данных, сроком исковой давности, а также иными требованиями законодательства РФ и нормативными документами Банка России.

5.5. Персональные данные являются конфиденциальной информацией, Банком строго соблюдаются требования конфиденциальности персональных данных, установленные ст. 7 Федерального закона № 152-ФЗ, а также принимаются меры по обеспечению безопасности персональных данных при их обработке, предусмотренные законодательством РФ.

5.6. Банк вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ, на основании заключаемого с этим лицом договора.

5.7. В Банке применяются следующие меры по обеспечению безопасности персональных данных:

1) технические меры:

- средства защиты от несанкционированного доступа (как встроенные в прикладное и системное программное обеспечение, так и дополнительные средства);
- антивирусное программное обеспечение;
- средства разграничения доступа к информационным ресурсам;
- система контроля почтового и веб-трафика.

2) организационные меры:

- определение уровней защищенности персональных данных при их обработке в информационных системах персональных данных;
- назначение ответственных за обеспечение безопасности персональных данных и ответственного за организацию обработки персональных данных;
- учет лиц, допущенных к обработке персональных данных;
- получение согласия субъекта персональных данных на обработку его персональных данных, а также передачу персональных данных третьим лицам;
- утверждение внутренних документов, регламентирующих порядок получения и обработки персональных данных субъектов персональных данных;
- возложение на контрагентов обязанности соблюдения конфиденциальности и безопасности при обработке передаваемых им персональных данных;
- возложение на работников Банка, имеющих доступ к персональным данным, ответственности за соблюдение требований законодательства РФ и внутренних документов Банка в части, касающейся неразглашения конфиденциальной информации третьим лицам;
- внутренний контроль и аудит соответствия обработки персональных данных требованиям Федерального закона № 152-ФЗ и нормативных правовых актов;
- публикация политики в отношении обработки и защиты персональных данных на сайте Банка.

5.8. Условием прекращения обработки персональных данных является 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.

5.9. 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, выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.10. Обработка персональных данных осуществляется Банком с использованием баз данных, находящихся на территории Российской Федерации, в соответствии с требованиями ч.5 ст.18 Федерального закона № 152-ФЗ.

5.11. При обработке документов на бумажном носителе, содержащих сведения о субъектах персональных данных, Банком соблюдаются требования, установленные Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5.12. Банком установлены условия хранения персональных данных, в том числе, при обработке персональных данных без использования средств автоматизации, такие как: определены места хранения, обеспечены условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ.

6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

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

6.2. Банк вносит изменения в персональные данные субъекта в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными.

6.3. 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, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- Банк вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или иными федеральными законами;
- другое не предусмотрено иным соглашением между оператором и субъектом персональных данных.

6.4. Банк уничтожает персональные данные субъекта в срок, не превышающий срок установленный законодательством со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

6.5. Банк обязан сообщить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу последнего.

6.6. Порядок 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 запросов/обращений устанавливаются внутренними нормативными документами Банка.

7. Перечень мер, направленных на выполнение обязанностей Банка как оператора обработки персональных данных

7.1. Банк назначает лиц, ответственных за организацию обработки персональных данных и за обеспечение информационной безопасности персональных данных.

7.2. Банк разрабатывает и утверждает внутренние нормативные документы по вопросам обработки и обеспечения информационной безопасности персональных данных.

7.3. Банк осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных требованиям Федерального закона № 152-ФЗ и принятым в соответствии с

ним нормативным правовым актам, требованиям к защите персональных данных, внутренним нормативным документам Банка.

7.4. Банк осуществляет оценку вреда, который может быть причинен субъектам в случае нарушения требований Федерального закона № 152-ФЗ, а также соотношения указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения своих обязанностей.

7.5. Банк осуществляет ознакомление своих сотрудников, осуществляющих обработку персональных данных, с законодательными актами Российской Федерации, нормативными документами Банка России, внутренними нормативными документами по вопросам обработки и обеспечения информационной безопасности персональных данных.

7.6. Банк осуществляет учет информационных систем персональных данных, мест хранения и обработки персональных данных (в том числе машинных носителей информации), а также учет сотрудников, осуществляющих обработку персональных данных.

7.7. Банк определяет актуальные угрозы безопасности персональных данных при их обработке в информационных системах персональных данных. В соответствии с выявленными актуальными угрозами безопасности персональных данных Банк внедряет комплекс организационных и технических мер, позволяющий нейтрализовать указанные угрозы.

7.8. Банк проводит оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных.

7.9. Банк устанавливает правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.

7.10. Банк внедряет средства минимизации полномочий доступа, разграничения доступа, мониторинга и контроля событий, обнаружения фактов неправомерного доступа, а также средства защиты информации, в том числе средства криптографической защиты информации, прошедшие в установленном порядке процедуру оценки соответствия.

7.11. Банк разрабатывает и внедряет меры реагирования на инциденты информационной безопасности в отношении персональных данных, а также меры по восстановлению персональных данных, модифицированных или уничтоженных вследствие неправомерного доступа к ним.

8. Ответственность за нарушение требований настоящей Политики

8.1. Контроль исполнения требований настоящей Политики осуществляется лицом, назначенным согласно распорядительному документу ответственным за организацию обработки персональных данных.

8.2. Работники, виновные в нарушении требований настоящей Политики, несут предусмотренную законодательством Российской Федерации ответственность.

9. Раскрытие информации в отношении обработки персональных данных

9.1. Банком направлено уведомление об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных. Банк включен в реестр операторов, осуществляющих обработку персональных данных.

9.2. 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.

9.3. Настоящая Политика подлежит публикации на официальном сайте Банка по адресу <https://www.siab.ru/>. Доступ к настоящей Политике для ознакомления с ней предоставляется неограниченному кругу лиц.