УТВЕРЖДЕНА
приказом заместителя
председателя Правления
ПАО «Банк «Санкт-Петербург»
от 23.10.2017 № 102302

ПОЛИТИКА

ПАО «Банк «Санкт-Петербург»
в отношении обработки персональных данных

Санкт-Петербург

2017

Содержание

1. Общие положения 3
2. Цели сбора персональных данных 6
3. Правовые основания обработки персональных данных 6
4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных 7
5. Порядок и условия обработки персональных данных 8
6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным. 9

1. Общие положения

1.1. Настоящая Политика ПАО «Банк «Санкт-Петербург» в отношении обработки персональных данных (далее – Политика) устанавливает общие подходы к обработке персональных данных (далее – ПДн) физических лиц в ПАО «Банк «Санкт-Петербург» (далее – Банк), определяет цели и правовое основание обработки ПДн, а также категории ПДн, обрабатываемых в Банке.

1.2. Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - № 152-ФЗ), а также учитывает требования:

- Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждено постановлением Правительства РФ от 15.09.2008 № 687;
- Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждены постановлением Правительства РФ от 01.11.2012 №1119;
- Приказ ФСТЭК 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 Роскомнадзора от 30.05.2017 N 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения".

1.3. Настоящая Политика регламентирует следующие вопросы:

- порядок обработки ПДн в различных бизнес-процессах Банка;
- организация приема и обработки обращений и запросов субъектов ПДн;
- перечень мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в сфере обработки ПДн, устранение последствий таких нарушений;
- порядок ознакомления работников Банка с законодательством и внутренними документами о ПДн;
- порядок формирования и направления уведомлений об обработке ПДн в уполномоченный орган по защите прав субъектов ПДн;
- перечень правовых, организационных и технических мер по обеспечению безопасности ПДн;
- порядок осуществления внутреннего контроля за соблюдением Банком и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.

1.4. В целях обеспечения выполнения Банком обязанностей, предусмотренных законодательством РФ о ПДн, в Банке назначается Ответственный по ПДн.

1.5. Термины, используемые в настоящей Политике:

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

оператор персональных данных (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки

ПДн состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн. Банк является оператором;

обработка ПДн – любое действие (операция) или совокупность действий (операций) с ПДн, совершаемых с использованием средств автоматизации или без их использования. Обработка ПДн включает в себя, в том числе: сбор; запись; систематизацию; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; передачу (распространение, предоставление, доступ); обезличивание; блокирование; удаление; уничтожение.

автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники;

распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц;

предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн;

обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДнх;

информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах, данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

трансграничная передача ПДн – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

субъект ПДн - физическое лицо, чьи персональные данные Банк обрабатывает, предполагает обрабатывать в будущем или ранее обрабатывал.

конфиденциальность ПДн – обязательное для соблюдения Банком или иным лицом, получившим доступ к ПДн требование, не раскрывать третьим лицам и не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

1.6. Права и обязанности Банка и субъекта ПДн

1.6.1. Банк вправе:

- предоставлять ПДн субъектов третьим лицам, если это предусмотрено требованиями действующего законодательства (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении ПДн субъекту ПДн в случаях, предусмотренных законодательством;
- производить обработку ПДн субъекта без его согласия в случаях, предусмотренных законодательством.
- защищать свои права и законные интересы в судебном порядке.

1.6.2. Банк обязан:

- производить обработку ПДн при наличии правовых оснований;
- принимать меры по обеспечению конфиденциальности и безопасности ПДн;
- обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн,

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

- предоставлять ответы на запросы субъектов ПДн;

- принимать меры по устранению нарушений законодательства, допущенных при обработке ПДн, по уточнению, блокированию и уничтожению ПДн в случае их выявления.

- выполнять иные предусмотренные законодательством Российской Федерации обязанности.

1.6.3. Субъект ПДн, обладает правами, предусмотренными законодательством, в том числе:

- Получать информацию, касающуюся обработки его ПДн, включая:

1) подтверждение факта обработки ПДн Банком;

2) правовые основания и цели обработки ПДн;

3) цели и применяемые Банком способы обработки ПДн;

4) наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Банком или на основании федерального закона;

5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки ПДн, в том числе сроки их хранения;

7) порядок осуществления субъектом ПДн прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные федеральными законами.

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

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

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

1.6.4. При обращении в Банк с запросом о предоставлении информации, касающейся обработки его персональных данных, Субъект ПДн обязан, указывать в запросе номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором. Запрос должен содержать подпись сывать запрос субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

2. Цели сбора ПДн

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

2.2. Объем, характер обрабатываемых ПДн, способы обработки ПДн в Банке соответствуют заявленным целям обработки ПДн.

2.3. Цели обработки ПДн в Банке определяются на основании, анализа правовых актов, регламентирующих деятельность Банка, целей фактически осуществляемой Банком деятельности, а также деятельности, которая предусмотрена учредительными документами Банка, и конкретных бизнес-процессов Банка в конкретных ИСПДн.

2.4. Обработка ПДн в Банке осуществляется в целях:

- осуществления банковской деятельности, в соответствие с требованиями Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»;
- оказания клиентам полного комплекса банковских услуг,
- обязательного раскрытия информации на рынке ценных бумаг,
- раскрытия информации для целей соблюдения антимонопольного законодательства,
- соблюдения требований законодательства при выпуске и обращении ценных бумаг,
- осуществления прав владельцев ценных бумаг, выпущенных (выданных) Банком и иными лицами,
- соблюдения требований законодательства о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма,
- соблюдения требований налогового законодательства,
- соблюдение требований трудового законодательства
- осуществления исполнительного производства,
- соблюдения банковской тайны,
- осуществления финансово-хозяйственной деятельности Банка,
- рекламы услуг Банка,
- соблюдения требований иных нормативных правовых актов Российской Федерации

3. Правовые основания обработки ПДн

3.1. ПДн в Банке обрабатываются на основании:

- Федеральных законов, в том числе Федерального закона: от 02 декабря 1990 г. № 395-1 «О банках и банковской деятельности»; Федерального закона от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Федерального закона от 30.12.2004 г. № 218-ФЗ «О кредитных историях»; Федерального закона от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг», от 23 декабря 2003 года № 177-ФЗ «О страховании вкладов физических лиц в банках РФ»; а также Трудового кодекса РФ; Гражданского кодекса РФ, Налогового кодекса РФ, и иных нормативных правовых актов государственных органов, Банка России, органов местного самоуправления, принятых на основании и во исполнение федеральных законов;
- настоящей Политики, иных внутренних документов Банка, разработанных в развитие и дополнение настоящей Политики.
- Устава Банка;
- Договоров, заключаемых между Банком и субъектами ПДн.
- Согласия на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям Банка).

4. Объем и категории, обрабатываемых ПДн, категории субъектов ПДн.

4.1. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

4.2. В Банке обрабатываются ПДн, принадлежащие следующим категориям субъектов ПДн:

- клиентам/контрагентам Банка (представителям клиентов/контрагентов Банка),
- работникам Банка,
- кандидатам на вакантные должности в Банке,
- владельцам ценных бумаг, выпущенных (выданных) Банком,
- членам и кандидатам в члены органов управления и контроля Банка,
- единоличному исполнительному органу Банка,
- аффилированным лицам Банка,
- лицам, являющимся владельцами и/или состоящим в органах управления юридических лиц - владельцев именных ценных бумаг Банка (в случаях, предусмотренных законодательством),
- лицам, у которых может быть заинтересованность в совершении Банком сделок, согласно ст. 81 ФЗ от 26.12.1995 №208-ФЗ «Об акционерных обществах»,
- руководителям, работникам, участникам (акционерам, товарищам, пайщикам) контрагентов (потенциальных контрагентов) Банка, юридических лиц - клиентов (потенциальных клиентов) Банка.
- выгодоприобретателям, распорядителям, бенефициарным владельцам, поручителям.

4.3. В Банке обрабатываются следующие категории ПДн: фамилия, имя, отчество; год рождения; дата и место рождения; адрес; семейное положение; имущественное положение; образование; профессия; доходы.

4.4. Другие категории ПДн: кредитная история физических лиц; ИНН, СНИЛС, гражданство, данные документов, удостоверяющих личность, данные миграционных карт, данные документов, подтверждающих право пребывания на территории РФ, номера телефонов, факсов, адреса электронной почты, должность, место работы, адрес места работы, сведения о наличии (отсутствии) судимости субъектов персональных данных для случаев, прямо предусмотренных федеральными законами, данные о воинской обязанности и иные категории в соответствии с требованиями действующего законодательства.

4.5. Производится обработка биометрических ПДн:

- фотографических изображений,
- информации об особенностях строения папиллярных узоров пальцев рук работников Банка.

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

4.7. Обработка данных о состоянии здоровья допускается только в отношении ПДн 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 действующего трудового законодательства.

5. Порядок и условия обработки ПДн.

5.1. Обработка ПДн в Банке осуществляется следующими способами: сбор; запись; систематизацию; накопление; хранение; уточнение (обновление, изменение); извлечение;

использование; передачу (предоставление, доступ); обезличивание; блокирование; удаление; уничтожение.

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

5.3. Трансграничная передача ПДн осуществляется в соответствии с условиями предоставления услуг и соблюдением требований законодательства.

5.4. Сроки обработки ПДн определяются в соответствии со сроком действия договора с субъектом ПДн, приказом Федерального архивного агентства (Росархив) от 20.12.2019 г. N 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», требованиями законодательства РФ и подзаконных актов, включая нормативные документ Банка России, сроком исковой давности.

5.5. ПДн являются конфиденциальной информацией, Банком строго соблюдаются требования конфиденциальности ПДн, установленные ст. 7 Федерального закона «О персональных данных», а также принимаются меры по обеспечению безопасности ПДн при их обработке, предусмотренные ч. 2 ст. 18.1, ч. 1 ст. 19 Федерального закона «О персональных данных», требованиями и рекомендациями по обеспечению безопасности ПДн, предъявляемых Федеральной службой безопасности РФ, Федеральной службой по техническому и экспортному контролю РФ.

5.6. Банк вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено Федеральным законом, на основании заключаемого с этим лицом договора, (далее - поручение оператора). Лицо, осуществляющее обработку ПДн по поручению Банка, обязано соблюдать принципы и правила обработки ПДн, предусмотренные законодательством. В поручении Банка должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со ст. 19 №152-ФЗ.

5.7. В Банке применяются следующие меры по обеспечению безопасности ПДн:

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;
- межсетевые экраны;
- система обнаружения вторжений;
- средства обнаружения уязвимостей;
- система контроля почтового и веб-трафика.

2) организационные меры:

- определение уровней защищенности ПДн при их обработке в ИСПДн;
- определение угроз безопасности ПДн при их обработке в ИСПДн;
- назначение ответственных за обеспечение безопасности ПДн и ответственного за организацию обработки ПДн;
- учет лиц, допущенных к обработке ПДн;
- получение согласия субъекта ПДн на обработку его ПДн, а также передачу ПДн третьим лицам;

- утверждение внутренних документов, регламентирующих порядок получения и обработки ПДн субъектов ПДн;
- возложение на контрагентов обязанности соблюдения конфиденциальности и безопасности при обработке передаваемых им ПДн;
- возложение на работников Банка, имеющих доступ к ПДн, ответственности за соблюдение требований законодательства РФ и внутренних документов Банка в части, касающейся неразглашения конфиденциальной информации третьим лицам;
- внутренний контроль и аудит соответствия обработки ПДн требованиям N-152-ФЗ и других нормативно-правовых актов;
- публикация политики в отношении обработки и защиты ПДн на сайте Банка.

5.8. Условием прекращения обработки ПДн является достижение целей обработки ПДн, истечение срока действия согласия или отзыв согласия субъекта ПДн на обработку его ПДн, а также выявление неправомерной обработки ПДн.

5.9. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, за исключением случаев, когда срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.

5.10. Обработка ПДн осуществляется Банком с использованием баз данных находящихся на территории Российской федерации, в соответствие с требованиями ч.5 ст.18 № 152-ФЗ.

5.11. При обработке документов на бумажном носителе, содержащих сведения о субъектах ПДн Банком соблюдаются требования, установленные Постановлением Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5.12. Банком соблюдаются условия хранения ПДн, в том числе, при обработке ПДн без использования средств автоматизации, а именно, определены места хранения, обеспечены условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

5.13. Работники Банка, осуществляющие обработку ПДн, несут ответственность за исполнение требований законодательства, настоящей Политики и иных внутренних документов Банка, разработанных в развитие и дополнение настоящей Политики, при осуществлении конкретных видов банковской деятельности, связанных с обработкой ПДн.

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

6.1. В случае подтверждения факта неточности ПДн или неправомерности их обработки, ПДн подлежат их актуализации Банком, а обработка должна быть прекращена.

6.2. При достижении целей обработки ПДн, а также в случае отзыва субъектом ПДн согласия на их обработку ПДн подлежат уничтожению, если:

– иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;

– Банк не вправе осуществлять обработку без согласия субъекта ПДн на основаниях, предусмотренных № 152-ФЗ или иными федеральными законами;

– иное не предусмотрено иным соглашением между Банком и субъектом ПДн.

6.3. Банк обязан предоставить субъекту ПДн или его представителю информацию об осуществляемой им обработке ПДн такого субъекта по запросу.

6.4. Порядок направления субъектом ПДн таких запросов определен требованиями № 152-ФЗ и производится в соответствии с процедурой, изложенной в Порядке обработки персональных данных в ПАО «Банк Санкт-Петербург» (в действующей редакции). Запрос субъекта ПДн должен содержать следующую информацию:

- серию, номер документа, удостоверяющего личность субъекта ПДн, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта ПДн в отношениях с Банком (номер договора, дата заключения договора, и/или иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Банком;
- подпись субъекта ПДн.

6.5. Обращения субъектов ПДн по вопросам, связанным с обработкой ПДн, оформленное в свободной форме может быть направлено через Интернет-банк, Почтой России на официальный адрес Банка или непосредственно в дополнительный офис/филиал Банка.