ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
АО «БАНК ФИНСЕРВИС»

Москва

2018

Оглавление

1. Общие положения

1.1. Назначением настоящей Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Настоящая Политика разработана с учетом требований законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных (далее – ПДн). Действие Политики распространяется на все процессы АО «Банк Финсервис» (далее – Банка), связанные с обработкой ПДн.

1.3. В настоящей Политике используются следующие понятия:

- персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту ПДн);
- оператор ПДн – 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 персональными данными;
- обработка ПДн - любое действие (операция) или совокупность действий (операций) с ПДн, совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;
- 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 ПДн - 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 информационной системе ПДн 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 ПДн;

- информационная система ПДн - 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.

1.4. Положения настоящей Политики являются обязательными для исполнения всеми работниками Банка, имеющими доступ к персональным данным.

1.5. Ознакомление работников Банка с положениями настоящей Политики осуществляется посредством рассылки Политики по системе электронного документооборота, используемого в Банке.

2. Цели обработки ПДн

2.1. Обработке подлежат только ПДн, которые отвечают целям их обработки.

2.2. Банк осуществляет обработку ПДн в следующих целях:

- ведение банковской деятельности в соответствии с Уставом Банка и выданными Банку лицензиями на совершение банковских и иных операций;
- заключение договоров с субъектами ПДн;
- подбор кандидатов на замещение вакантных должностей;
- установка трудовых взаимоотношений с субъектами ПДн;
- формирование бухгалтерской отчетности, отчетности в налоговые органы, органы статистики;
- проведения Банком акций, опросов, исследований;
- предоставления субъекту ПДн информации об оказываемых Банком услугах, о разработке Банком новых продуктов и услуг;
- формирование программ лояльности;
- осуществления Банком административно-хозяйственной деятельности;
- выявления случаев мошенничества, хищения денежных средств со счета, иных противоправных действий, предотвращения таких противоправных действий в дальнейшем и локализации последствий таких действий.

3. Правовые основания обработки ПДн

3.1. Правовым основанием обработки ПДн является совокупность правовых актов, во исполнение которых и в соответствии с которыми Банк осуществляет обработку ПДн.

3.2. В качестве правового основания обработки ПДн Банк руководствуется следующими нормативно правовыми актами:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);
- Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 02.12.1990 N 395-1 «О банках и банковской деятельности»;
- Федеральный закон от 13.03.2006 N 38-ФЗ «О рекламе»;
- Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- 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»;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации. Утверждено постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 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 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- Конвенция о защите физических лиц в отношении автоматизированной обработки данных личного характера (ETS N 108, заключена в г. Страсбурге 28.01.1981);
- Регламент № 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» (принят в г. Брюсселе 27.04.2016);

- Иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

4. Объем и категории обрабатываемых ПДн, категории субъектов ПДн

4.1. Банк обрабатывает следующие категории ПДн:

4.1.1. Категория 1 – ПДн, отнесенные в соответствии с Федеральным законом «О персональных данных» к специальным категориям ПДн:

- расовая, национальная принадлежности;
- состояние здоровья.

4.1.2. Категория 2 - ПДн, отнесенные в соответствии с Федеральным законом «О персональных данных» к биометрическим персональным данным - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Банком для установления личности субъекта ПДн, а именно:

- изображение лица;
- запись голоса.

4.1.3. Категория 3 – ПДн, которые не могут быть отнесены к категории 1, категории 2 или категории 4;

4.1.4. Категория 4 – ПДн, отнесенные в соответствии с Федеральным законом «О персональных данных» к общедоступным или обезличенным персональным данным. В общедоступные источники ПДн с письменного согласия субъекта ПДн могут включаться:

- фамилия, имя, отчество;
- год и место рождения;
- адрес;
- абонентский номер;
- сведения о профессии;
- иные ПДн, сообщаемые субъектом ПДн.
- категории субъектов ПДн:
- работники Банка, бывшие работники, кандидаты на замещение вакантных должностей, а также родственники работников;
- клиенты и контрагенты Банка (физические лица);
- представители/работники клиентов и контрагентов Банка (юридических лиц)

4.2. Категории субъектов ПДн:

- работники Банка, бывшие работники, кандидаты на замещение вакантных должностей, а также родственники работников;
- клиенты и контрагенты Банка (в т.ч. физические лица, не участвующие в трудовых отношениях с Банком);

- представители/работники клиентов и контрагентов Банка (юридических лиц).

5. Основные права и обязанности Банка

5.1. При сборе ПДн Банк предоставляет субъекту ПДн по его просьбе информацию, касающейся обработки его ПДн любым удобным для субъекта ПДн способом.

5.2. Если предоставление ПДн является обязательным в соответствии с федеральным законом, Банк обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

5.3. Банк обязан не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

5.4. Если ПДн получены не от субъекта ПДн, Банк, за исключением случаев, предусмотренных пунктом 5.5 настоящей Политики, до начала обработки таких ПДн предоставляет субъекту ПДн следующую информацию любым удобным для субъекта ПДн способом:

- наименование и адрес Банка;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- права субъекта ПДн;
- источник получения ПДн.

5.5. Банк освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные пунктом 5.4 настоящей Политики, в случаях, если:

- субъект ПДн уведомлен об осуществлении обработки его ПДн Банком;
- ПДн получены Банком на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- Банк осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта ПДн;
- предоставление субъекту ПДн сведений, предусмотренных пунктом 5.4 настоящей Политики, нарушает права и законные интересы третьих лиц.

5.6. При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети "Интернет", Банк обеспечивает обработку ПДн граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона «О персональных данных».

5.7. Банк принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Банк определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом «О персональных данных» или другими федеральными законами.

5.8. Банк обязан представить документы и локальные акты, указанные в части 1 статьи 18.1 Федерального закона «О персональных данных», и (или) иным образом подтвердить принятие мер, указанных в части 1 статьи 18.1 Федерального закона «О персональных данных», по запросу уполномоченного органа по защите прав субъектов ПДн.

5.9. Банк при обработке ПДн принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

5.10. Банк обязан сообщить 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 либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.

5.11. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя Банк обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

5.12. Банк обязан предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Банк обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Банк обязан уничтожить такие ПДн. Банк обязан уведомить субъекта ПДн или его представителя о внесенных измене-

ниях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

5.13. Банк обязан сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

5.14. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн Банк обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Банк обязан осуществить блокирование ПДн, относящихся к этому субъекту ПДн, с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

5.15. В случае подтверждения факта неточности ПДн Банк на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязан уточнить ПДн в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

5.16. В случае выявления неправомерной обработки ПДн, осуществляемой Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Банка. В случае, если обеспечить правомерность обработки ПДн невозможно, Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Банк обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

5.17. В случае достижения цели обработки ПДн Банк обязан прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн либо если Банк не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами.

5.18. В случае отзыва субъектом ПДн согласия на обработку его ПДн Банк обязан прекратить их обработку и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн либо если Банк не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами.

5.19. В случае отсутствия возможности уничтожения ПДн в течение указанного срока, Банк осуществляет блокирование таких ПДн и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.20. Банк обязан уведомить уполномоченный орган по защите прав субъектов ПДн в течение десяти рабочих дней в случае изменения следующих сведений:

- наименование, адрес Банка;
- цель обработки ПДн;
- категории ПДн;
- категории субъектов, ПДн которых обрабатываются;
- правовое основание обработки ПДн;
- перечень действий с персональными данными, общее описание используемых Банком способов обработки ПДн;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- фамилия, имя, отчество физического лица, ответственного за организацию обработки ПДн, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
- дата начала обработки ПДн;
- срок или условие прекращения обработки ПДн;
- сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки;
- сведения о месте нахождения базы данных информации, содержащей ПДн граждан Российской Федерации;
- сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации,

а также в случае прекращения обработки ПДн с даты возникновения таких изменений или с даты прекращения обработки ПДн.

5.21. Лицо, ответственное за организацию обработки ПДн в Банке назначается приказом Председателя Правления.

5.22. Лицо, ответственное за организацию обработки ПДн, получает указания непосредственно от исполнительного органа Банка и подотчетно ему.

5.23. Банк обязан предоставлять лицу, ответственному за организацию обработки ПДн, сведения, указанные в пункте 5.20 настоящей Политики.

5.24. Лицо, ответственное за организацию обработки ПДн, в частности, обязано:

- осуществлять внутренний контроль за соблюдением Банком и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;
- доводить до сведения работников Банка положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

6. Основные права и обязанности субъекта(ов) ПДн

6.1. Субъект ПДн имеет право на получение сведений, указанных в пункте 6.7 настоящей Политики, за исключением случаев, предусмотренных пунктом 6.8 настоящей Политики. Субъект ПДн вправе требовать от Банка уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Сведения, указанные в пункте 6.7 настоящей Политики, должны быть предоставлены субъекту ПДн Банком в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

6.3. Сведения, указанные в пункте 6.7 настоящей Политики, предоставляются субъекту ПДн или его представителю Банком при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Банком (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Банком, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6.4. В случае, если сведения, указанные в пункте 6.7 настоящей Политики, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к Банку или направить ему повторный запрос в целях получения сведений, указанных в пункте 6.7 настоящей Политики, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

6.5. Субъект ПДн вправе обратиться повторно к Банку или направить ему повторный запрос в целях получения сведений, указанных в пункте 6.7 настоящей Политики, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в пункте 6.4 настоящей Политики, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 6.3 настоящей Политики, должен содержать обоснование направления повторного запроса.

6.6. Банк вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пункте 6.4 и 6.5 настоящей Политики. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Банке.

6.7. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Банком;
- правовые основания и цели обработки ПДн;
- цели и применяемые Банком способы обработки ПДн;
- 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;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

Порядок предоставления субъекту ПДн информации, касающейся обработки его ПДн и форма запроса на получение информации определяется нормативным документом Банка.

6.8. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, если:

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

6.9. Обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта ПДн. Указанная обработка ПДн признается осуществляемой без предварительного согласия субъекта ПДн, если Банк не докажет, что такое согласие было получено.

6.10. Субъект ПДн вправе требовать от Банка прекратить обработку его ПДн, указанную в пункте 6.9 настоящей Политики.

6.11. Запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта

ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных пунктом 6.9 настоящей Политики.

6.12. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.

6.13. Субъект ПДн вправе получить от Банка разъяснения порядка защиты Банком прав и законных интересов субъекта ПДн, порядка принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, а также заявить возражение против такого решения и получить результаты рассмотрения такого возражения в течение тридцати дней со дня его подачи.

6.14. Если субъект ПДн считает, что Банк осуществляет обработку его ПДн с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Банка в уполномоченном органе по защите прав субъектов ПДн или в судебном порядке.

6.15. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7. Общий порядок и условия обработки ПДн

7.1. Обработка ПДн в Банке осуществляется только с согласия субъекта ПДн (его законного представителя) в случае, если получение такого согласия необходимо в соответствии с требованиями Федерального закона «О персональных данных», кроме случаев, установленных законодательством Российской Федерации с соблюдением требований конфиденциальности ПДн, установленных ст. 7 Федерального закона «О персональных данных», а также принятием мер, направленных на обеспечение выполнения обязанностей по обработке и защите ПДн, установленных законодательством Российской Федерации.

7.2. Формы письменного согласия на обработку ПДн устанавливаются нормативными и (или) методическими документами Банка, регламентирующими технологические и бизнес-процессы Банка, в рамках которых производится обработка ПДн. Достоверность предоставляемых ПДн должна проверяться принимающим их работником путем их сверки с информацией, содержащейся в оригиналах документов или их надлежащим образом заверенных копиях, предъявляемых субъектом ПДн или его законным представителем.

7.3. Банк осуществляет обработку ПДн с использованием средств автоматизации и без использования средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн в сроки, необходимые для достижения целей обработки ПДн.

7.4. Условиями прекращения обработки ПДн могут являться:

- достижение целей обработки ПДн;
- истечение срока действия согласия субъекта ПДн на обработку его ПДн;
- отзыв согласия субъекта ПДн на обработку его ПДн;
- выявление неправомерной обработки ПДн.

7.5. Представители органов государственной власти (в том числе, контролирующих, надзорных, правоохранительных, дознания и следствия и иных уполномоченных органов по основаниям, предусмотренным законодательством Российской Федерации) получают доступ к ПДн, обрабатываемым в Банке, в объеме и порядке, установленном законодательством Российской Федерации.

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

7.7. Хранение ПДн при обработке без использования средств автоматизации осуществляется обособленно от иной информации, в частности путем фиксации на отдельных материальных носителях (при наличии технической возможности) в специальных разделах или на полях форм (бланков). При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн используется отдельный материальный носитель.

7.8. Банк осуществляет деятельность по своевременному выявлению и внесению изменений в обрабатываемые ПДн с целью обеспечения их точности, достоверности и актуальности, в том числе по отношению к целям обработки ПДн. Соответствующие процедуры и инструкции устанавливаются нормативными и(или) методическими документами Банка, регламентирующими технологические и бизнес-процессы Банка, в рамках которых производится обработка ПДн. Изменения в ПДн вносятся уполномоченным работником Банка только на основании предоставленных надлежащим образом оформленных оригиналов документов или их заверенных копий.

7.9. В случае подтверждения факта неточности ПДн Банк на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом

по защите прав субъектов ПДн, или иных необходимых документов осуществляет уточнение ПДн в течение семи рабочих дней со дня представления таких сведений.

7.10. Банк уведомляет любым удобным способом субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

7.11. Банк может осуществлять передачу ПДн для обработки третьему лицу, если иное не предусмотрено законодательством Российской Федерации. При этом:

- обработка третьим лицом ПДн, предоставленных Банку субъектом ПДн (его законным представителем), может осуществляться только с согласия субъекта ПДн (его законного представителя), если получение такого согласия необходимо в соответствии с требованиями Федерального закона «О персональных данных»;
- обработка ПДн третьим лицом может осуществляться только на основании договора, в котором определены перечень действий (операций), которые будут осуществляться с ПДн, а также положения по обеспечению конфиденциальности и безопасности ПДн, в том числе требования не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации;
- процедуры передачи ПДн и их носителей, а также их учета выполняются в соответствии с установленным в Банке порядком ведения делопроизводства и соответствующими нормативными документами Банка.

7.12. Обрабатываемые ПДн обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

7.13. В случае выявления неточных ПДн или неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Банк осуществляет блокирование ПДн, относящихся к этому субъекту ПДн с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

7.14. В случае если обеспечить правомерность обработки ПДн невозможно, Банк в установленный срок с даты выявления неправомерной обработки ПДн, обеспечивает уничтожение таких ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Банк сообщает субъекту ПДн или его представителю, а в случае если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

7.15. Обрабатываемые ПДн уничтожаются, в установленные законодательством Российской Федерации сроки, по достижении целей обработки, в случае утраты необхо-

димости в достижении этих целей, а также в случае отзыва субъектом ПДн согласия на их обработку:

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

7.16. Процедуры уничтожения и обезличивания ПДн устанавливаются методическими документами Банка, регламентирующими аналогичные процедуры в отношении сведений ограниченного распространения, к которым относятся ПДн, и их носителей.

7.17. В случае достижения цели обработки ПДн Банк прекращает обработку ПДн, проводит анализ факта достижения цели обработки ПДн и в случае положительного результата обеспечивает уничтожение соответствующих ПДн в установленный срок с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн либо если Банк не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

7.18. В случае представления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Банк уничтожает такие ПДн в срок не превышающий семи дней со дня предоставления таких сведений.

7.19. В случае отсутствия возможности уничтожения ПДн в течение указанного срока, Банк осуществляет блокирование таких ПДн и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

8. Обеспечение безопасности обработки ПДн

8.1. В целях обеспечения безопасности обработки ПДн Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, установленных законодательством Российской Федерации о персональных данных.

8.2. Основными мерами защиты Пдн, используемыми Банком, являются:

- назначение лица, ответственного за организацию обработки ПДн;
- ограничение и контроль состава лиц, имеющих доступ к ПДн;

- ознакомление работников Банка с требованиями законодательства Российской Федерации по обработке и защите ПДн, а также обучение безопасной работе со средствами вычислительной техники;
- организация режима обеспечения физической безопасности помещений, носителей информации и оборудования;
- управление и контроль доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- регистрация и учёт событий в информационных системах, обрабатывающих ПДн;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- обеспечение антивирусной защиты;
- защита информационных систем от атак;
- обеспечение возможности восстановления модифицированных или уничтоженных ПДн с резервных носителей;
- осуществление периодического контроля достаточности и полноты реализации защитных мер;
- осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике Банка в отношении обработки ПДн, а также локальным актам Банка;
- определение угроз безопасности ПДн при их обработке в информационных системах ПДн;
- применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;
- учет машинных носителей ПДн.

8.3. Меры по обеспечению безопасности ПДн при их обработке устанавливаются в соответствии с требованиями законодательства Российской Федерации о защите ПДн, разрабатываемыми Банком моделями угроз для информационных систем ПДн, а также локальными нормативными актами Банка, регламентирующими вопросы обеспечения безопасности ПДн.

9. Ответственность

9.1. Каждый работник Банка несет персональную ответственность, предусмотренную законодательством Российской Федерации, за разглашение или утрату ПДн, обрабатываемых в Банке.

9.2. Работники Банка, обрабатывающие ПДн, обязаны:

- знать и исполнять требования законодательства Российской Федерации, внутренние документы Банка, регламентирующие обработку ПДн;
- обрабатывать ПДн только в рамках выполнения своих служебных обязанностей;
- не разглашать ПДн, обрабатываемые в Банке;
- незамедлительно сообщать лицу, ответственному за организацию обработки ПДн в Банке, о действиях других лиц, которые могут привести к нарушению положений настоящей Политики;
- незамедлительно сообщать лицу, ответственному за организацию обработки ПДн в Банке, о фактах нарушения требований законодательства Российской Федерации, настоящей Политики и внутренних документов Банка о ПДн.

9.3. По факту разглашения или утраты ПДн в Банке проводится служебное расследование в установленном порядке.

9.4. Одновременно с проведением служебного расследования в Банке принимаются меры по минимизации нежелательных последствий произошедшего, а также по недопущению (предотвращению) в дальнейшем разглашения или утраты ПДн.

9.5. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, а также требований к защите ПДн, установленных Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.

9.6. Все отступления от настоящей Политики расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством, внутренними нормативными документами Банка или соглашением сторон.

10. Контроль реализации Политики, ответственность за реализацию и поддержку Политики, условия её пересмотра

10.1. Ответственность за контроль над соблюдением настоящей Политики возлагается на лицо, назначенное приказом Председателя Правления ответственным за организацию процесса обработки ПДн в Банке.

10.2. Настоящая Политика публикуется на сайте Банка в открытом доступе.

10.3. Ответственным за пересмотр и поддержание в актуальном состоянии настоящей Политики является работник, ответственный за обработку ПДн.

10.4. Основанием для пересмотра настоящей Политики могут являться изменения:

- в законодательстве Российской Федерации (в частности, требованиях Федерального закона «О персональных данных»);
- в нормативных актах Банка России;
- целей обработки ПДн Банка;
- контрактных обязательств Банка.