

УТВЕРЖДЕНО  
решением Совета директоров АО «ГОРБАНК»  
(Протокол № 19 от «29» января 2024 г.)



**«ПЕТЕРБУРГСКИЙ ГОРОДСКОЙ БАНК»**  
**АКЦИОНЕРНОЕ ОБЩЕСТВО**  
**(АО «ГОРБАНК»)**

**ПОЛИТИКА**  
**ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**(действует с 01.02.2024 г.)**

## СОДЕРЖАНИЕ:

|  |           |
|--|-----------|
| <b>ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ</b>  | <b>3</b>  |
| <b>ГЛАВА 2. ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕЙ ПОЛИТИКЕ</b>  | <b>5</b>  |
| <b>ГЛАВА 3. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ</b>   | <b>6</b>  |
| <b>ГЛАВА 4. КАТЕГОРИИ И ПОРЯДОК ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ</b>   | <b>7</b>  |
| <b>ГЛАВА 5. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ</b>   | <b>9</b>  |
| <b>ГЛАВА 6. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ</b>  | <b>10</b> |
| <b>ГЛАВА 7. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ</b>   | <b>11</b> |
| <b>ГЛАВА 8. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДН), РЕСУРСЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ХАРАКТЕРИСТИКИ</b> | <b>13</b> |
| <b>ГЛАВА 9. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ</b>  | <b>14</b> |
| <b>ГЛАВА 10. ПРАВА И ОБЯЗАННОСТИ БАНКА В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ</b>  | <b>16</b> |
| <b>ГЛАВА 11. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ</b>   | <b>19</b> |
| <b>ГЛАВА 12. ОБРАБОТКА ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИХ ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ И УПОЛНОМОЧЕННЫХ ОРГАНОВ</b>                              | <b>21</b> |
| <b>ГЛАВА 13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ</b>  | <b>21</b> |
| <b>ПРИЛОЖЕНИЯ</b>  | <b>22</b> |

## ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

**1.1.** Важнейшим условием реализации целей деятельности Акционерного общества «ПЕТЕРБУРГСКИЙ ГОРОДСКОЙ БАНК» (АО «ГОРБАНК») (далее по тексту – «Банк»), является обеспечение необходимого и достаточного уровня информационной безопасности активов, к которым в том числе относятся персональные данные и банковские технологические процессы, в рамках которых они обрабатываются.

**1.2.** Персональные данные являются конфиденциальной, строго охраняемой информацией, на которую распространяются все требования, установленные внутренними документами Банка к защите конфиденциальной информации. Обеспечение безопасности персональных данных является одной из приоритетных задач Банка.

**1.3.** Обработка и обеспечение безопасности информации, отнесенной к персональным данным, осуществляется Банком в соответствии с законодательством Российской Федерации (далее по тексту – «РФ») и, нормативными документами Банка России, внутренними документами Банка, что позволяет обеспечить защиту персональных данных, обрабатываемых, как в информационных системах персональных данных, так и в иных информационных системах, в которых персональные данные обрабатываются совместно с информацией, защищаемой в соответствии с требованиями, установленными для этой информации (режим защиты сведений, составляющих банковскую тайну, коммерческую тайну и др.).

**1.4.** Настоящая «Политика обработки персональных данных» (далее по тексту – «Политика») определяет порядок сбора, обработки и защиты персональных данных клиентов Банка, их представителей, выгодоприобретателей, бенефициарных владельцев и иных лиц, чьи персональные данные обрабатываются Банком, с целью обеспечения 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, устанавливает права и обязанности Банка и субъекта персональных данных в области обработки и защиты персональных данных, а также ответственность должностных лиц Банка, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Настоящая Политика размещается Банком на своем официальном сайте в сети Интернет по адресу [www.gorbank.spb.ru](http://www.gorbank.spb.ru).

**1.5.** Настоящая Политика разработана Банком в соответствии с требованиями действующего законодательства РФ и нормативными документами Банка, в том числе:

- Уставом Банка;
- Конституцией Российской Федерации от 12.12.1993 г. (ст. 2, 17-24, 41) (с изменениями и дополнениями);
- Главой 14 (ст. 56-90) Трудового кодекса Российской Федерации от 30.12.2001 г. № 197-ФЗ (с изменениями и дополнениями);
- частями 1, 2, 4 Гражданского кодекса Российской Федерации (с изменениями и дополнениями);
- Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями) (далее по тексту – «Закон о персональных данных»);
- Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 г. № 18 «Об утверждении

требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»;

- Постановлением Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Федеральным законом от 14.07.2022 г. № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»;
- Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;
- Приказом Роскомнадзора от 27.10.2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;
- Приказом Федерального архивного агентства от 31.07.2023 г. № 77 «Об утверждении Правил организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в государственных органах, органах местного самоуправления и организациях».

**1.6.** В соответствии со ст. 22.1 Закона о персональных данных приказом по Банку назначено **лицо, ответственное за организацию обработки персональных данных** (далее по тексту – «Должностное лицо Банка»), в обязанности которого входит:

- осуществлять внутренний контроль за соблюдением Банка и его сотрудниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения сотрудников Банка положения законодательства РФ о персональных данных, внутренних документов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

**1.7.** Банк вносит изменения и/или дополнения в настоящую Политику, как по собственной инициативе, так и в связи с изменением законодательства РФ, в т.ч. с появлением новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, нормативных актов Банка России, путем утверждения ее новой редакции, но не реже 1 раза в 3 года.

**1.8.** Если в результате изменения законодательных и нормативных правовых актов РФ, Банка России отдельные пункты настоящей Политики вступают с ними в противоречие, эти пункты утрачивают силу. До момента внесения изменений в настоящую Политику Банк руководствуется законодательными и нормативно-правовыми актами РФ и Банка России.

**1.9.** Вопросы, не урегулированные в настоящей Политике, регулируются законодательными и нормативными правовыми актами РФ и Банка России, а также внутренними документами Банка.

**1.10.** Настоящая Политика распространяется на все субъекты персональных данных, а также сотрудников Банка, имеющих доступ к персональным данным субъектов персональных данных и осуществляющих весь перечень действий с персональными данными.

При приеме Банком на работу нового работника его ознакомление с действующей редакцией настоящей Политики осуществляется до подписания с ним трудового договора. Подтверждением ознакомления вновь принятого работника с действующей редакцией настоящей Политики является подпись работника, проставленная на трудовом договоре и в отдельном Листе ознакомления.

При внесении изменений в настоящую Политику работники Банка знакомятся с текстом новой редакции под подпись в отдельном Листе ознакомления, который прилагается к измененной редакции настоящей Политики в распечатанном виде. Подготовка Листа ознакомления, ознакомление работников Банка с действующей редакцией настоящей Политики под подпись в Листе ознакомления и его хранение осуществляется Должностным лицом Банка, указанным в п. 1.6. настоящей Политики.

**1.11.** Особенности обработки персональных данных соискателей на замещение вакантных должностей и сотрудников Банка устанавливаются в Положении «О персональных данных сотрудников».

## **ГЛАВА 2. ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕЙ ПОЛИТИКЕ**

**2.1.** Для целей настоящей Политики применяются следующие термины и определения:

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

**Субъекты персональных данных** – физические лица, вступившие в договорные, трудовые и иные гражданско-правовые отношения с Банком, пользующиеся услугами Банка, иные физические лица, являющиеся потенциальными субъектами персональных данных Банка, а также представители субъекта персональных данных, выгодоприобретатели (т.е. лица, к выгоде которых действует субъект персональных данных), бенефициарные владельцы.

**Оператор** – АО «ГОРБАНК».

**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.

**Документы, содержащие персональные данные** – документы, предоставляемые субъектами персональных данных, их представителями, выгодоприобретателями, бенефициарными владельцами, необходимые для заключения договоров, проведения операций и/или сделок, а также документы, предоставляемые субъектами персональных данных для заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений с Банком, в которых содержится любая информация, относящаяся к субъекту персональных данных.

**Передача персональных данных** – действия, направленные на передачу персональных данных определенному/неопределенному кругу лиц. Передача персональных данных возможна в форме предоставления, доступа или распространения.

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц при условии получения согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

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

**Блокирование персональных данных** – временное прекращение обработки 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 (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Ресурс персональных данных** – совокупность персональных данных, обрабатываемых с использованием или без использования средств автоматизации и автоматизированной банковской системы (далее по тексту – «АБС»), в том числе ИСПДн, объединенных общими целями обработки.

**Несанкционированный доступ (несанкционированные действия) к ИСПДн** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

## **ГЛАВА 3. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**3.1.** Персональные данные в Банке обрабатываются на основании совокупности правовых актов, во исполнение которых оператор осуществляет обработку персональных данных:

- Федеральных законов, в том числе Федерального закона от 02 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (с изменениями и дополнениями), Федерального закона от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изменениями и дополнениями), Федерального закона от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях» (с изменениями и дополнениями), Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг» (с изменениями и дополнениями), Федерального закона от 23 декабря 2003 г. № 177-ФЗ «О страховании вкладов в банках Российской Федерации» (с изменениями и дополнениями), Трудового кодекса Российской Федерации, Гражданского кодекса Российской Федерации, Налогового кодекса Российской Федерации, иных нормативных правовых актов, 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 персональных данных;

- Согласия на обработку персональных данных.

## **ГЛАВА 4. КАТЕГОРИИ И ПОРЯДОК ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**4.1.** Перечень (объем) персональных данных, подлежащих обработке, хранению и защите в Банке, установлен в Приложении 1 к настоящей Политике. Содержание и объем персональных данных соответствует целям обработки. Обрабатываемые данные не должны быть избыточны по отношению к заявленным целям их обработки.

Банк не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни физического лица, за исключением случаев, предусмотренных Законом о персональных данных.

**4.2.** Категории субъектов персональных данных, персональные данные которых обрабатываются Банком это:

- физические лица – граждане РФ;
- физические лица – иностранные граждане и лица без гражданства;

в случае если физические лица являются:

- клиентами или потенциальными клиентами Банка;
- представителями клиентов Банка;
- выгодоприобретателями по операциям клиентов Банка;
- бенефициарными владельцами клиентов Банка;
- поручителями или залогодателями по сделкам и/или операциям клиентов Банка;
- супругами клиентов (при получении согласия на сделку и иной информации, содержащей персональные данные);
- сотрудниками Банка, кандидатами на вакантные должности;
- стороной по гражданско-правовым договорам;
- контрагентами Банка по сделкам;
- иными лицами, имеющими договорные отношения с Банком, и с которыми взаимодействуют сотрудники Банка в процессе своей деятельности.

**4.3.** Основными документами, содержащими персональные данные субъектов персональных данных Банка, являются:

- ❖ документы, необходимые для заключения и исполнения договора банковского счета, а также для банковского обслуживания;
- ❖ договоры на банковское обслуживание с использованием системы «Интернет-Банк»;
- ❖ анкеты субъекта персональных данных Банка, его представителя, выгодоприобретателя, бенефициарного владельца;
- ❖ договоры банковского вклада/депозита, договоры аренды банковского сейфа и иные договоры оказания Банком услуг;
- ❖ кредитный договор, договор залога, договор поручительства, соглашение о выдаче банковской гарантии;
- ❖ заявка субъекта персональных данных Банка на выдачу кредита и документы, предоставляемые для выдачи кредита и дальнейшего обслуживания;
- ❖ письма, заявления, обращения, претензии, жалобы субъектов персональных данных и иные предоставленные ими документы, анкеты соискателей вакансий;
- ❖ расчетные документы, первичные документы по бухгалтерским операциям, реестры по различным операциям;
- ❖ договоры, заключаемые с контрагентами, а также документы, предоставляемые для заключения таких договоров;
- ❖ другие документы, возникающие в процессе деятельности Банка.

**4.4.** Получение персональных данных преимущественно осуществляется путем предоставления их субъектом персональных данных вместе с его письменным согласием, за исключением случаев, предусмотренных действующим законодательством РФ, когда согласие на обработку персональных данных не требуется.

В обязанности сотрудников Банка, осуществляющих сбор персональных данных субъекта персональных данных, входит получение согласия субъекта персональных данных на обработку его персональных данных под личную подпись. Если по какой-либо уважительной причине персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие;

В письменном согласии на обработку персональных данных содержится следующая информация:

- фамилия, имя, отчество (при наличии) субъекта персональных данных;
- согласие на обработку персональных данных
- контактная информация (номер телефона, адрес электронной почты или почтовый адрес субъекта персональных данных);
- сведения о Банке, как об операторе - наименование, адрес, указанный в Едином государственном реестре юридических лиц, идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту персональных данных);
- цель (цели) обработки персональных данных;



- категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных:
- персональные данные (фамилия, имя, отчество (при наличии), год, месяц, дата рождения, место рождения, адрес, семейное положение, образование, профессия, социальное положение, доходы, другая информация, относящаяся к субъекту персональных данных);
- категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов (заполняется по желанию субъекта персональных данных);
- 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.

Помимо вышеперечисленного, письменное согласие на обработку персональных данных разрешенных субъектом персональных данных для распространения, также должно содержать:

- разрешение субъекта персональных данных для распространения его персональных данных Банком как оператором;
- сведения об информационных ресурсах Банка, как оператора, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных (адрес сайта Банка в информационно-телекоммуникационной сети Интернет);
- запрет/отсутствие запрета (в форме ответа «да» / «нет») запрета на передачу (кроме предоставления доступа) персональных данных неограниченному кругу лиц, на обработку или условия обработки (кроме получения доступа) персональных данных неограниченным кругом лиц;
- возможность указать субъектом персональных данных конкретные запрет на передачу (кроме предоставления доступа) персональных данных неограниченному кругу лиц, запрет на обработку или условия обработки (кроме получения доступа) персональных данных неограниченным кругом лиц.

Форма согласия на обработку персональных данных установлена в Приложении 2 к настоящей Политике.

Форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения установлена в Приложении 3 к настоящей Политике.

## **ГЛАВА 5. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

### **5.1. Банк осуществляет обработку персональных данных в целях:**

- осуществления банковских операций, сделок и иной деятельности, предусмотренной действующим законодательством РФ, нормативными актами Банка России, Уставом Банка, полученными лицензиями и нормативными актами Банка;
- заключения, исполнения, изменения и прекращения гражданско-правовых договоров с физическими/юридическим лицами, индивидуальными предпринимателями, физическими лицами, занимающимися в установленном законодательством РФ порядке частной практикой, и иными лицами, в случаях, предусмотренных действующим законодательством РФ и Уставом Банка;
- организации кадрового учета и ведения кадрового делопроизводства в Банке, обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- обеспечения соблюдения законодательства Российской Федерации.

Обработка персональных данных несовместима с целями сбора персональных данных не допустима.

## **ГЛАВА 6. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**6.1.** Сроки обработки персональных данных определяются в соответствии со сроком действия договора, заключенного с субъектом персональных данных и согласия субъекта персональных данных на обработку персональных данных, Приказом Федерального архивного агентства от 20.12.2019 г. № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», Постановлением Федеральной комиссии по рынку ценных бумаг от 16.07.2003 г. № 03-33/пс «Об утверждении Положения о порядке и сроках хранения документов акционерных обществ», сроком исковой давности, а также требованиями действующего законодательства РФ, нормативными документами Банка России и внутренними документами Банка.

**6.2.** Персональные данные субъектов персональных данных, их представителей, выгодоприобретателей, бенефициарных владельцев могут создаваться и храниться как на бумажных носителях, так и в электронном виде как с использованием средств автоматизации, так и без использования средств автоматизации, при непосредственном участии сотрудника Банка.

Руководители структурных подразделений обеспечивают невозможность доступа к персональным данным субъектов персональных данных лицам, не уполномоченным законом либо Банком для получения соответствующих сведений.

В течение года, следующего за отчетным, документы, содержащие персональные данные, могут храниться в структурных подразделениях Банка. Дальнейшее хранение документов, содержащих персональные данные, осуществляется в архиве Банка в соответствии с номенклатурой дел Банка.

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 Законом о персональных данных, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

**6.3.** В случае достижения цели обработки персональных данных прекращается их обработка Банком, а персональные данные подлежат уничтожению в срок, предусмотренный законодательством Российской Федерации. В случае отзыва субъектом персональных данных своего согласия на обработку Банк обязан прекратить обработку персональных данных, и, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, предусмотренный законодательством Российской Федерации.

Уничтожению подлежат данные, цели обработки которых достигнуты, а также данные, сроки хранения которых истекли или утрачена необходимость достижения целей их обработки.

Экспертиза документов и данных, содержащих персональные данные как на бумажном носителе, так и в электронном виде, на предмет уничтожения осуществляется Экспертной комиссией Банка, назначенной приказом по Банку.

Уничтожение содержащих персональные данные документов и данных, выделенных Экспертной комиссией Банка, производится в порядке, установленном внутрибанковским «Порядком работы Архива».

**6.4. Блокирование персональных данных осуществляется с учетом следующей специфики:**

- в АБС Банка - посредством закрытия доступа к конкретному разделу меню или подсистеме для определенных групп сотрудников;
- персональных данных на бумажных носителях - посредством закрытия доступа к соответствующим персональным данным.

Блокированию подлежат персональные данные в случае выявления неправомерной обработки персональных данных, выявления неточных персональных данных при обращении или запросу субъекта персональных данных или его представителя, а также по запросу органа по защите прав субъектов персональных данных на период проверки с момента обращения или получения запроса, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц в случае выявления неточных персональных данных.

В случае подтверждения факта неточности персональных данных Банк обязан уточнить персональные данные в течение 7 (семи) рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

В случае выявления неправомерной обработки персональных данных в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, Банк обязан прекратить неправомерную обработку персональных данных. Об устранении допущенных нарушений Банк обязан уведомить адреса, по обращению/запросу которого было выявлена неправомерная обработка персональных данных.

## **ГЛАВА 7. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**7.1.** Обработка персональных данных осуществляется с соблюдением требований, определенных в «Положении об особенностях обработки персональных данных,

осуществляемой без использования средств автоматизации» (утв. Постановлением Правительства от 15.09.2008 г. № 687) и «Требованиях к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119).

**7.2.** Обработка персональных данных Банком осуществляется на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- справедливости;
- ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- недопустимости обработки персональных данных, не совместимой с целями сбора персональных данных;
- недопустимости объединения баз данных информационных систем, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- соответствия персональных данных целям их обработки;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям их обработки;
- недопустимости обработки персональных данных, избыточных по отношению к заявленным целям их обработки;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Банка;
- обеспечения точности обрабатываемых персональных данных, их достаточности, достоверности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных;
- принятия Банком необходимых мер либо обеспечения их принятия по удалению или уточнению неполных, или неточных данных;
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, если срок хранения персональных данных не установлен Законом о персональных данных, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных;
- уничтожения либо обезличивания обрабатываемых персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Законом о персональных данных.

### **7.3. Условия обработки персональных данных.**

Обработка персональных данных осуществляется Банком с соблюдением принципов и правил, предусмотренных Законом о персональных данных и настоящей Политикой.

Обработка персональных данных допускается в случаях, если она:

- ✓ осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- ✓ необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения функций, полномочий и обязанностей, возложенных законодательством РФ на Банк;
- ✓ осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;
- ✓ необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном

производстве;

✓ необходима для исполнения договора, стороной (выгодоприобретателем, поручителем) которого 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). Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных;

✓ необходима для осуществления прав и законных интересов Банка или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

✓ необходима для опубликования или обязательного раскрытия персональных данных в соответствии с Федеральным законом.

**7.4.** Обработка персональных данных в Банке осуществляется как неавтоматизированным способом обработки персональных данных, так и автоматизированным способом обработки персональных данных в информационных системах и автоматизированной банковской системе.

## **ГЛАВА 8. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДн), РЕСУРСЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ХАРАКТЕРИСТИКИ**

**8.1.** Обработка персональных данных в информационных системах персональных данных осуществляется при непосредственном участии сотрудника Банка с учетом следующего:

- персональные данные обособливаются от иных информационных ресурсов;
- персональные данные (материальные носители), обработка которых осуществляется в различных целях, хранятся отдельно;
- лица, осуществляющие обработку персональных данных, действуют строго в рамках своих должностных полномочий;
- при хранении персональных данных соблюдаются условия, обеспечивающие их сохранность и исключающие несанкционированный доступ к ним.

**8.2.** Ресурсами персональных данных являются информационные системы Банка, в которых обрабатываются персональные данные. Перечень информационных систем устанавливается отдельным внутренним документом Банка.

Доступ сотрудникам Банка к информационным системам предоставляется только в объеме, необходимом для выполнения своих должностных обязанностей.

**8.3.** ИСПДн в Банке вводится в эксплуатацию приказом.

**8.4.** Автоматизированные банковские системы (далее – АБС), информационные системы могут быть отнесены к ИСПДн с учетом следующего:

- вопрос об отнесении АБС, информационной системы к ИСПДн рассматривается комиссией, назначаемой приказом по Банку. В состав комиссии в обязательном порядке должны быть включены сотрудники Отдела информационной

безопасности, Управления автоматизации и программного обеспечения, а также Службы безопасности Банка;

- к ИСПДн должны быть отнесены как минимум АБС, целью создания и использования которых является обработка персональных данных;
- решение об отнесении АБС и информационной системы к ИСПДн принимается комиссией с учетом целей создания и использования АБС и информационной системы, вида реализуемого технологического процесса и обрабатываемых персональных данных;
- решение об отнесении АБС и информационной системы к ИСПДн отражается в акте классификации ИСПДн.

#### **8.5. Критерии определения уровня защищенности персональных данных в ИСПДн:**

- определение уровня защищенности персональных данных в ИСПДн Банка производится в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства РФ от 01.11.2012 г. № 1119;
- определение уровня защищенности персональных данных в ИСПДн производится на основе типа информационной системы, объема обрабатываемых персональных данных, актуальных угроз для ИСПДн и целей создания АБС, информационной системы.

Уровень защищенности персональных данных в ИСПДн подлежит определению членами комиссии и фиксируется актом, утверждаемым Председателем Правления Банка (или лицом его замещающим).

## **ГЛАВА 9. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**9.1.** В целях обеспечения выполнения обязанностей, предусмотренных настоящей Политикой, при обработке персональных данных Банк предпринимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения, а также от иных неправомерных действий в отношении персональных данных.

К вышеуказанным мерам обеспечения безопасности персональных данных относятся:

- утверждение Советом директоров Банка настоящей Политики;
- назначение в Банке лица, ответственного за организацию обработки персональных данных;
- назначение приказом Председателя Правления Банка сотрудников, ответственных за обработку и хранение персональных данных;
- подписание сотрудниками Банка при приеме на работу договорного обязательства о неразглашении конфиденциальной информации, к которой относятся персональные данные;
- установление приказом по Банку мест/помещений для хранения персональных данных и порядка доступа к таким местам/помещениям, в том числе хранение ключей для доступа к указанным местам/помещениям;
- охрана всех помещений Банка в нерабочее время;

- хранение всех персональных данных в запираемых шкафах и/или помещениях, права доступа в которые посторонние лица не имеют или имеют только в сопровождении сотрудника Банка, на несъемных или съемных носителях информации;
- определение правил доступа сотрудников к персональным данным, обрабатываемым в информационной системе персональных данных;
- обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- осуществление проверок обеспечения безопасности персональных данных в Банке Комиссией по информационной безопасности, Службой внутреннего аудита с целью соблюдения требований:
  - нормативных актов РФ,
  - настоящей Политики,
  - внутренних нормативных документов Банка,
  - установленных мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- определение оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения положений законодательства Российской Федерации о персональных данных, в соответствии с требованиями, установленными Регламентом оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона «О персональных данных», утвержденным Правлением Банка.

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

**9.2.** Система защиты персональных данных включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и актуальных информационных технологий, используемых в информационных системах.

**9.3. Для обеспечения безопасности персональных данных при неавтоматизированной обработке предпринимаются следующие меры:**

– определяются места хранения содержащих персональные данные носителей, которые оснащаются следующими средствами защиты:

- в помещениях Банка размещаются специально оборудованные шкафы, запираемые на ключ. По окончании рабочего дня шкафы запираются механическими ключами, помещение сдается под охрану;
- здание Банка находится под круглосуточной охраной;
- в здании Банка осуществляется круглосуточное видеонаблюдение;
- все действия по обработке персональных данных субъекта персональных данных осуществляются только сотрудниками Банка, допущенными к работе с персональными данными субъектов персональных данных приказом Председателя Правления, и только в объеме, необходимом для выполнения ими своих должностных обязанностей;

– при обработке персональных данных на съемных носителях не допускается фиксация на одном носителе персональных данных, обработка которых осуществляется в целях, несовместимых между собой. При несовместимости целей обработки персональных данных,

зафиксированных на одном съемном носителе, если не имеется возможности осуществлять их отдельно, должны быть приняты следующие меры:

- при необходимости использования определенных персональных данных отдельно от находящихся на том же съемном носителе других персональных данных, осуществляется копирование подлежащих использованию персональных данных способом, исключающим одновременное копирование персональных данных, не подлежащих использованию, и используется только копия;
- при необходимости уничтожения части персональных данных уничтожается или форматируется съемный носитель с предварительным копированием сведений, не подлежащих уничтожению, на другой съемный носитель способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

Эти правила применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном съемном носителе персональных данных и информации, не являющейся персональными данными. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на съемном носителе, а если это не допускается техническими особенностями съемного носителя - путем изготовления нового съемного носителя с уточненными персональными данными, при этом предыдущий съемный носитель, подлежит уничтожению. Уничтожение или обезличивание части персональных данных, если это допускается съемным носителем, должно производиться способом, исключающим дальнейшую их обработку с сохранением возможности обработки иных данных, зафиксированных на этом съемном носителе (удаление, вымарывание).

#### **9.4. Для обеспечения безопасности персональных данных при автоматизированной обработке предпринимаются следующие меры:**

- все действия при автоматизированной обработке персональных данных осуществляются только сотрудниками Банка и только в объеме, необходимом данным лицам для выполнения своей трудовой функции;
- доступ всех сотрудников Банка в локальную вычислительную сеть Банка и информационную систему осуществляется после ввода логина и пароля. Периодичность смены паролей определяется внутренним «Положением о защите информации при эксплуатации программного обеспечения, баз данных и ресурсов локальной вычислительной сети Банка», утверждаемым Правлением Банка;
- иные меры, предусмотренные настоящей Политикой.

**9.5.** Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, если иное не определено Законом о персональных данных.

## **ГЛАВА 10. ПРАВА И ОБЯЗАННОСТИ БАНКА В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

### **10.1. Банк обязан:**

- в случаях и в порядке, предусмотренных законодательством РФ, предоставлять субъекту персональных данных сведения и информацию, касающиеся обработки его персональных данных;
- руководствоваться законодательством РФ в сфере защиты персональных данных и обработки информации, Уставом Банка, настоящей Политикой и иными внутренними нормативными документами при определении объема и содержания обрабатываемых персональных данных;
- в течение 10 (десяти) рабочих дней с даты обращения/получения запроса подготовить ответ на обращение/запрос о предоставлении информации, касающейся обработки его персональных данных, в том числе содержащей в соответствии с ч. 7 ст. 14 Закона о персональных данных:
  - 1) подтверждение факта обработки персональных данных Банком;



- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые Банком способы обработки персональных данных;
- 4) наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных Законом о персональных данных;
- 8) информацию о способах исполнения Банком обязанности по принятию мер, направленных на обеспечение выполнения Банком обязанностей, предусмотренных Законом о персональных данных;
- 9) иные сведения, предусмотренные Законом о персональных данных или другими Федеральными законами.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Банк предоставляет сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

- осуществить блокирование **неправомерно обрабатываемых персональных данных** субъекта персональных данных с момента обращения субъекта персональных данных или его представителя, либо с момента получения запроса субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных, на период проверки;

- осуществить блокирование персональных данных субъекта персональных данных **в случае выявления неточных персональных данных** с момента обращения субъекта персональных данных или его представителя, либо с момента получения запроса субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных, на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц;

- при подтверждении факта неточности персональных данных Банк обязан их уточнить, на основании представленных сведений в течение 7 (семи) рабочих дней со дня представления уточненных сведений субъектом персональных данных или его законным представителем, либо уполномоченным органом по защите прав субъектов персональных данных;

- прекратить неправомерную обработку персональных данных субъекта персональных данных в срок, не превышающий 3 (трех) рабочих дней с даты выявления факта неправомерной обработки персональных данных;

Об устранении допущенных нарушений Банк обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

- в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Банк в соответствии с ч. 3.1 ст. 21 Закона о персональных данных обязан с момента выявления такого инцидента Банком, уполномоченным органом по защите прав субъектов персональных данных или иным

заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Банком на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Порядок уведомления приведен в Приложении 8 к настоящей Политике.

- осуществить обезличивание персональных данных путем замены части сведений персональных данных идентификаторами с созданием таблицы соответствия, изменения состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений, разбиение массива информации на несколько частей и раздельное хранение каждой из них, перемешивания, перестановка отдельных записей с персональными данными и групп таких записей в массиве персональных данных;

- прекратить обработку персональных данных субъекта персональных данных и уничтожить персональные данные в срок, не превышающий 10 (десяти) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных или иным соглашением между Банком и субъектом персональных данных, либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или другими федеральными законами;

- прекратить обработку персональных данных субъекта персональных данных в случае отзыва субъектом персональных данных согласия на обработку его персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий 10 (десяти) дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных, либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральными законами;

- прекратить обработку персональных данных в случае обращения субъекта персональных данных с требованием о прекращении обработки его персональных данных в срок, не превышающий 10 (десяти) рабочих дней с даты получения соответствующего требования, за исключением случаев, предусмотренных п. 6.3. настоящей Политики.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

- рассмотреть возражение субъекта персональных данных против решения, принятого на основании исключительно автоматизированной обработки его персональных данных, в течение 10-ти дней со дня его получения и уведомить субъекта персональных данных Банка о результатах рассмотрения такого возражения;

- обеспечивать защиту персональных данных субъекта персональных данных от неправомерного их использования или утраты за счет своих средств, в порядке, установленном законодательством Российской Федерации;

- принимать меры, необходимые и достаточные для обеспечения безопасности персональных данных субъектов персональных данных при их обработке и выполнения иных

обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами;

- предоставлять персональные данные субъектов персональных данных третьим лицам в случаях и в порядке, предусмотренном действующим законодательством Российской Федерации (налоговые, правоохранительные органы и др.), а также в случае если это предусмотрено договором с субъектом персональных данных, согласием субъекта персональных данных;

- размещать действующую редакцию настоящей Политики в неограниченном доступе на официальном сайте Банка в информационно-телекоммуникационной сети Интернет.

#### **10.2. Банк вправе:**

- запрашивать от субъекта персональных данных предоставления персональных данных и документов, их подтверждающих, в объеме, необходимом для качественного оказания ему финансовых услуг и в случаях, предусмотренных Федеральными законами;

- использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством Российской Федерации;

- отказывать в предоставлении персональных данных в случаях и порядке, предусмотренных законодательством Российской Федерации;

- самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено указанным законом или другими Федеральными законами.

Иные права и обязанности Банка определяются действующим законодательством Российской Федерации.

## **ГЛАВА 11. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

#### **11.1. Субъекты персональных данных имеют право:**

- на получение от Банка сведений и информации, касающихся обработки своих персональных данных, указанных в части 7 статьи 14 Закона о персональных данных, за исключением случаев, предусмотренных частью 8 статьи 14 указанного федерального закона;

- требовать от Банка уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. При отказе Банка исключить или исправить персональные данные субъекта персональных данных Банка, субъект персональных данных имеет право заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия;

- обжаловать действия или бездействия Банка в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если считает, что Банк осуществляет обработку его персональных данных с нарушением требований Закона о персональных данных или иным образом нарушает его права и свободы;

- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Иные права и обязанности субъекта персональных данных определяются действующим законодательством Российской Федерации.

**11.2. Сведения, касающиеся обработки персональных данных субъекта персональных данных, указанные в части 7 статьи 14 Закона о персональных данных, предоставляется Банком субъекту персональных данных или его представителю в течение 10 (десяти) рабочих дней с момента обращения либо получения Банком запроса субъекта персональных данных или его представителя в той форме, в которой направлены соответствующие обращения или запрос, если иное не указано в обращении или запросе. В нем не должно содержаться**

персональных данных, относящихся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления Банком в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, 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 законного представителя.

В случае если запрошенные сведения, а также обрабатываемые персональные данные, были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Банк или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Закона о персональных данных, и ознакомления с такими персональными данными не ранее чем через 30 (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 персональных данных.

Субъект персональных данных вправе обратиться повторно в целях получения сведений, указанных в части 7 настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения вышеуказанного в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в абзаце 3 настоящего пункта, должен содержать обоснование направления повторного запроса.

Банк вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным абзацами 3 и 5 настоящего пункта. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Банке.

**11.3.** Передача персональных данных субъектов персональных данных Банка третьим лицам осуществляется Банком только с письменного согласия субъектов персональных данных, за исключением случаев, если:

- передача необходима для защиты жизни и здоровья субъекта персональных данных Банка, либо других лиц и получение его согласия невозможно;
- по запросам органов дознания, следствия и суда в связи с проведением расследования или судебным разбирательством;
- при наличии оснований, позволяющих полагать, что права и интересы субъекта персональных данных Банка могут быть нарушены противоправными действиями других лиц;
- в целях организации работ с военными комиссариатами для постановки на воинский учет лиц, подлежащих призыву в порядке, установленном законодательством;
- в иных случаях, прямо предусмотренных Федеральными законами. Лица, которым в установленном законом порядке переданы сведения, составляющие персональные данные субъекта персональных данных Банка, за разглашение сведений несут

дисциплинарную, административную или уголовную ответственность в соответствии с законодательством РФ.

## **ГЛАВА 12. ОБРАБОТКА ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИХ ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ И УПОЛНОМОЧЕННЫХ ОРГАНОВ**

**12.1.** Порядок обработки обращений субъектов персональных данных, их законных представителей и уполномоченных органов, типовые формы обращений и ответов на обращения, Регламент действий при обращении субъектов персональных данных или Роскомнадзора определяется приложениями к настоящей Политике.

**12.2.** Обработка обращений субъектов персональных данных (за исключением обращений субъектов персональных данных, вступивших в договорные, трудовые и иные гражданско-правовые отношения с Банком и пользующихся услугами Банка) по телефонной линии связи осуществляется после предупреждения субъекта персональных данных до начала разговора фразой на автоответчике «Продолжая разговор, Вы подтверждаете свое согласие на обработку персональных данных». Если субъект персональных данных продолжит разговор после такого предупреждения, то будет считаться, что он дал фактическое согласие на обработку его персональных данных.

## **ГЛАВА 13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

**13.1.** Ответственность должностных лиц Банка, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством РФ и внутренними документами Банка и установлена в должностных инструкциях сотрудников, приказах по Банку, договорном обязательстве о неразглашении конфиденциальной информации.

**13.2.** Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта персональных данных Банка, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующими Федеральными законами.

#### Сведения о персональных данных физического лица, которые подлежат обработке в АО «ГОРБАНК»

1. Фамилия, Имя, Отчество (если иное не вытекает из закона или национального обычая);
  2. ИИН;
  3. Гражданство;
  4. Дата рождения;
  5. Место рождения;
  6. Данные о принадлежности к публичным должностным лицам, их близким родственникам, супругам;
  7. Данные документа, удостоверяющего личность:
    - наименование документа,
    - серия,
    - номер,
    - дата выдачи,
    - наименование органа, выдавшего документ, и код подразделения (если имеется);
  8. Данные миграционной карты:
    - номер карты,
    - дата начала срока пребывания,
    - дата окончания срока пребывания;
  9. Данные документа, подтверждающего право иностранного гражданина или лица без гражданства на пребывание (проживание) в РФ:
    - наименование документа,
    - серия (если имеется),
    - номер документа,
    - дата начала срока действия права пребывания (проживания),
    - дата окончания срока действия права пребывания (проживания);
  10. Адрес места жительства (регистрации);
  11. Адрес фактического проживания (места пребывания);
  12. Номера контактных телефонов и факсов;
  13. E-mail;
  14. Помимо вышеуказанных сведений: основания для признания физического лица бенефициарным владельцем физического лица;
  15. Помимо вышеуказанных сведений: основания, свидетельствующие о том, что клиент действует к выгоде другого лица при проведении банковских операций и иных сделок, необходимые для признания физического лица выгодоприобретателем физического лица;
  16. Сведения о месте работы и занимаемой должности;
  17. Сведения об участии в обществах;
- Дополнительно данные сотрудников:
18. О трудовой деятельности;
  19. О семейном положении;
  20. Об образовании;
  21. Сведения о полученных в Банке доходах;
  22. Сведения об участии в обществах;
- При предоставлении кредита Банк также может хранить:
23. Вышеперечисленные данные:
    - о поручителях,
    - о залогодателях,
    - о супругах,
    - о полученных доходах,
    - о правах собственности.



**«ПЕТЕРБУРГСКИЙ ГОРОДСКОЙ БАНК»  
АКЦИОНЕРНОЕ ОБЩЕСТВО  
(АО «ГОРБАНК»)**

**СОГЛАСИЕ  
на обработку персональных данных**

Я,

\_\_\_\_\_ ,  
(фамилия, имя, отчество полностью, дата рождения)

\_\_\_\_\_ ,  
(вид и реквизиты основного документа, удостоверяющего личность)

зарегистрированный(ая) по адресу: \_\_\_\_\_

в соответствии со ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» настоящим выражаю свое согласие на обработку Акционерным обществом «ПЕТЕРБУРГСКИЙ ГОРОДСКОЙ БАНК» (АО «ГОРБАНК»), зарегистрированному по месту нахождения по адресу: 191186, г. Санкт-Петербург, Итальянская ул., д. 15, литер «А», моих личных данных, а именно:

\_\_\_\_\_ ,  
*перечень персональных данных, на обработку которых дается согласие*

а также любой иной информации, относящейся к моей личности, доступной либо известной в любой конкретный момент времени АО «ГОРБАНК» (далее по тексту - «персональные данные»), предоставленных мной в АО «ГОРБАНК» в связи с

\_\_\_\_\_ ,  
*цели обработки персональных данных*

в объеме и порядке, предусмотренных Федеральным законом от 07.08.2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изменениями и дополнениями) и Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» (с изменениями и дополнениями).

Я разрешаю осуществление любых действий (операций) или совокупности действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств в отношении моих персональных данных, которые необходимы для достижения вышеуказанной(ых) цели(ей) обработки, включая (без ограничения) сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а также осуществление с моими персональными данными (включая полученные от меня и/или от любых третьих лиц) любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я уведомлен(а) о том, что настоящее Согласие может быть отозвано мной в любой момент на основании письменного заявления. Я уведомлен(а) о том, что ответственность за неблагоприятные последствия отзыва настоящего Согласия возлагается на меня. С момента получения отзыва настоящего Согласия, а также при достижении вышеуказанной(ых) цели(ей) обработки персональных данных АО «ГОРБАНК» прекращает обработку персональных данных и (или) уничтожает персональные данные в срок, установленный действующим законодательством Российской Федерации.

Настоящим подтверждаю, что мне известно, что:

- при отзыве мною настоящего Согласия АО «ГОРБАНК» вправе продолжить

обработку моих персональных данных в случаях, предусмотренных Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных»;

- требование об уничтожении не распространяется на персональные данные, для которых действующим законодательством Российской Федерации предусмотрена обязанность их хранения, в том числе после достижения вышеуказанных целей обработки персональных данных.

Письменное уведомление об уничтожении моих персональных данных в мой адрес прошу не направлять.

Настоящим я подтверждаю и гарантирую, что в случае предоставления мною Банку персональных данных третьих лиц мной получено согласие этих лиц на осуществление любых действий (операций) или совокупности действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств в отношении их персональных данных, которые необходимы для достижения вышеуказанных целей в объеме и порядке, предусмотренных Федеральным законом от 07.08.2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изменениями и дополнениями) и Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» (с изменениями и дополнениями). В случае возникновения необходимости я обязуюсь предоставить по запросу Банка указанные согласия.

Настоящим я признаю и подтверждаю, что в случае необходимости предоставления персональных данных для достижения вышеуказанных целей обработки третьим лицам, а равно как при привлечении третьих лиц к оказанию услуг в вышеуказанных целях обработки, АО «ГОРБАНК» вправе в необходимом объеме раскрывать для совершения вышеуказанных действий информацию обо мне лично (включая мои персональные данные) таким третьим лицам, их агентам и иным уполномоченным лицам, а также предоставлять таким лицам соответствующие документы, содержащие такую информацию, для обработки персональных данных на основании настоящего Соглашения. Также настоящим я признаю и подтверждаю, что настоящее Соглашение считается данным мною любым третьим лицам, указанным выше, с учетом соответствующих изменений, и любые такие третьи лица имеют право на обработку моих персональных данных на основании настоящего Соглашения.

Настоящее Соглашение действует до достижения вышеуказанных целей обработки персональных данных или до истечения сроков хранения АО «ГОРБАНК» соответствующей информации или документов, содержащих мои персональные данные.

Я подтверждаю, что настоящее Соглашение дано мной свободно, своей волей и в своем интересе.

---

*Ф.И.О. полностью (заполняется собственноручно)*

---

*подпись*

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ года





**«ПЕТЕРБУРГСКИЙ ГОРОДСКОЙ БАНК»**  
**АКЦИОНЕРНОЕ ОБЩЕСТВО**  
**(АО «ГОРБАНК»)**

**СОГЛАСИЕ**  
**на обработку персональных данных, разрешенных субъектом персональных**  
**данных для распространения**

Я, \_\_\_\_\_,  
*(фамилия, имя, отчество полностью)*

\_\_\_\_\_  
*(номер телефона, адрес электронной почты или почтовый адрес)*

в соответствии со ст. 9, 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» настоящим даю **свое согласие на распространение (действия, направленные на раскрытие персональных данных неопределенному кругу лиц)** Акционерному обществу «ПЕТЕРБУРГСКИЙ ГОРОДСКОЙ БАНК» (АО «ГОРБАНК») (далее по тексту – «Банк»), адрес: 191186, г. Санкт-Петербург, Итальянская ул., д. 15, литер А (ИНН 7831001239, ОГРН 1027800000348), моих персональных данных (относящейся ко мне прямо или косвенно информации) (далее по тексту – «Персональные данные» или «ПД») посредством информационного ресурса – официального сайта АО «ГОРБАНК» в информационно-телекоммуникационной сети «Интернет»: <https://www.gorbank.spb.ru>.

**Категории и перечень персональных данных, на обработку которых дается согласие:**

| № п/п                                     | Персональные данные                            | Согласие |     | Запреты и условия на обработку ПД <sup>1</sup> |     | Дополнительные условия <sup>2</sup> |
|---|--|----------|-----|--|-----|-------------------------------------|
|   |  | Да       | Нет | Да   | Нет |                                     |
| <b>1. Общие Персональные данные</b>       |  |          |     |  |     |                                     |
| 1   | Фамилия имя отчество (последнее - при наличии) |          |     |  |     |                                     |
| 2   | Год, месяц, дата рождения                      |          |     |  |     |                                     |
| 3   | Место рождения                                 |          |     |  |     |                                     |
| 4   | Адрес  |          |     |  |     |                                     |
| 5   | Семейное положение                             |          |     |  |     |                                     |
| 6   | Образование                                    |          |     |  |     |                                     |
| 7   | Профессия                                      |          |     |  |     |                                     |
| 8   | Социальное положение                           |          |     |  |     |                                     |
| 9   | Доходы   |          |     |  |     |                                     |
| <b>2. Специальные Персональные данные</b> |  |          |     |  |     |                                     |

<sup>1</sup> Запрет на передачу (кроме предоставления доступа) ПД неограниченному кругу лиц, на обработку или условия обработки (кроме получения доступа) ПД неограниченным кругом лиц

<sup>2</sup> Указать запреты и условия, если в столбце «Запреты и условия на обработку ПД» напротив ПД указано «Да»

|    |                    |  |  |  |  |  |
|----|--------------------|--|--|--|--|--|
| 10 | Состояние здоровья |  |  |  |  |  |
|    |                    |  |  |  |  |  |

В СВЯЗИ С

*(цели обработки персональных данных)*

Условия, при которых полученные Персональные данные могут передаваться Банком 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<sup>3</sup>:

Я уведомлен(а) о том, что настоящее Согласие может быть отозвано мной в любой момент на основании письменного заявления. Я уведомлен(а) о том, что ответственность за неблагоприятные последствия отзыва настоящего Согласия возлагается на меня. С момента получения отзыва настоящего Согласия, а также при достижении вышеуказанной(ых) цели(ей) обработки персональных данных АО «ГОРБАНК» прекращает обработку персональных данных и (или) уничтожает персональные данные в срок, установленный действующим законодательством Российской Федерации.

Настоящим подтверждаю, что мне известно, что при отзыве мною настоящего Согласия АО «ГОРБАНК» вправе продолжить обработку моих персональных данных без моего согласия при наличии оснований, предусмотренных Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» (с изменениями и дополнениями).

Настоящее Согласие действует до достижения вышеуказанных целей обработки персональных данных или до истечения сроков хранения АО «ГОРБАНК» соответствующей информации или документов, содержащих мои персональные данные.

Я подтверждаю, что настоящее Согласие дано мной свободно, своей волей и в своем интересе.

\_\_\_\_\_  
*Ф.И.О. полностью (заполняется собственноручно)*

\_\_\_\_\_  
*подпись*

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ года

<sup>3</sup> Заполняется по желанию

**Приложение 4**

Форма запроса Субъекта персональных данных/  
представителя субъекта персональных данных информации, касающейся  
обработки персональных данных

в АО «ГОРБАНК»

от \_\_\_\_\_

\_\_\_\_\_  
(ФИО)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
(номер основного документа,  
удостоверяющего личность, дата  
выдачи и выдавший орган)

**ЗАПРОС**

В соответствии с \_\_\_\_\_

(сведения о номере договора, дате заключения договора/условное словесное обозначение и (или) иные сведения, подтверждающие участие в отношениях с АО «ГОРБАНК»/сведения, иным образом подтверждающие факт обработки персональных данных АО «ГОРБАНК»)) АО «ГОРБАНК», расположенное по адресу: 191186, г. Санкт-Петербург, ул. Итальянская, д. 15, литер «А», производит обработку персональных данных \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
(ФИО субъекта персональных данных, номер основного документа, удостоверяющего личность, дата выдачи и выдавший орган).

Право получения информации, касающейся обработки персональных данных вышеуказанного субъекта персональных данных основано на (нужное отметить):

ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

доверенности \_\_\_\_\_  
(указать реквизиты доверенности)<sup>4</sup>.

На основании вышеизложенного прошу предоставить следующую информацию:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Ответ на настоящий запрос прошу направить мне по следующему адресу: \_\_\_\_\_

\_\_\_\_\_.

« \_\_\_ » \_\_\_\_\_ 20 \_\_\_ г.

\_\_\_\_\_ (Ф.И.О., подпись)

<sup>4</sup> Заполняется в случае обращения представителя субъекта персональных данных

**Приложение 5**  
Форма заявления Субъекта  
персональных данных на уточнение,  
блокировку, уничтожение  
персональных данных

в АО «ГОРБАНК»  
от

\_\_\_\_\_

\_\_\_\_\_

(ФИО)

\_\_\_\_\_

\_\_\_\_\_

(номер основного документа,  
удостоверяющего личность, дата  
выдачи и выдавший орган)

**ЗАЯВЛЕНИЕ**

В соответствии с \_\_\_\_\_  
(сведения о номере договора, дате заключения договора/условное словесное обозначение и (или) иные сведения, подтверждающие участие в отношениях с АО «ГОРБАНК»/сведения, иным образом подтверждающие факт обработки персональных данных АО «ГОРБАНК»)

**АО «ГОРБАНК», расположенное по адресу: 191186, г. Санкт-Петербург, ул. Итальянская, д. 15, литер «А», производит обработку моих персональных данных**

\_\_\_\_\_

\_\_\_\_\_

(ФИО субъекта персональных данных, номер основного документа, удостоверяющего личность, дата выдачи и выдавший орган).

В связи с тем, что обрабатываемые персональные данные являются (*выбрать нужное*):

\_\_\_\_\_  \_\_\_\_\_  \_\_\_\_\_  незаконно  не являются  
неполными, устаревшими, неточными, полученными, необходимыми для  
заявленной цели  
обработки

и на основании ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», прошу (*выбрать нужное*):

уточнить (внести изменения) в следующие персональные данные: \_\_\_\_\_

уничтожить следующие персональные данные: \_\_\_\_\_

произвести блокировку следующих персональных данные: \_\_\_\_\_

**Ответ на настоящий запрос прошу направить мне по следующему адресу:** \_\_\_\_\_

«\_\_» \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_ (Ф.И.О., подпись)

**Приложение 6**

**Форма заявления субъекта персональных данных  
об отзыве его согласия на обработку персональных данных**

в АО «ГОРБАНК»

от

\_\_\_\_\_  
\_\_\_\_\_  
*(ФИО)*  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
(номер основного документа,  
удостоверяющего личность, дата  
выдачи и выдавший орган)

Заявление

В соответствии с \_\_\_\_\_

**(сведения о номере договора, дате заключения договора, условное словесное обозначение и (или) иные сведения, подтверждающие участие в отношениях с АО «ГОРБАНК»/сведения, иным образом подтверждающие факт обработки персональных данных АО «ГОРБАНК»)**

АО «ГОРБАНК», расположенное по адресу: 191186, г. Санкт-Петербург, ул. Итальянская, д. 15, литер «А», производит обработку моих персональных данных. В соответствии с п. 2 ст. 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», я отзываю свое согласие на обработку персональных данных \_\_\_\_\_

Подтверждаю, что ознакомлен(а) с п. 2 ст. 9 Федерального закона от 27.07.2006 г. № 152 - ФЗ «О персональных данных».

Ответ на настоящий запрос прошу предоставить по адресу \_\_\_\_\_

«\_\_» \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_ (Ф.И.О., подпись)

**Регламент действий при обращении субъектов персональных данных или Роскомнадзора****1. Область применения**

Настоящий Регламент регулирует отношения, возникающие при выполнении обязательств согласно требованиям статей №№ 14, 20 и 21 Федерального закона «О персональных данных» № 152-ФЗ от 27 июля 2006 года Акционерным обществом «ПЕТЕРБУРГСКИЙ ГОРОДСКОЙ БАНК» (далее - Банк). Положения настоящего Регламента распространяются на действия при обращении либо при получении запроса субъекта персональных данных или его законного представителя, при обращении уполномоченного органа по защите прав субъектов персональных данных. Эти действия направлены на подтверждение наличия, ознакомление, уточнение, уничтожение или отзыв согласия на обработку персональных данных, а также на устранение нарушений законодательства, допущенных при обработке персональных данных.

Уничтожение персональных данных оформляется Актом об уничтожении в произвольной форме с соблюдением требований к подтверждению уничтожения персональных данных, утвержденных Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

**2. Определения**

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

**Оператор ПДн** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку таких данных, а также определяющие цели их обработки, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с данными/

**Обработка персональных данных** - 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.

**Информационная система персональных данных** (далее - ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**3. Ответственность**

Организация и проведение работ по ответам на запросы, устранению нарушений, а также уточнению, блокированию и уничтожению персональных данных возлагается на назначенного приказом Председателя Правления Банка лица, ответственного за организацию обработки персональных данных.

Ответственность за правильное применение настоящего Регламента несут руководители структурных подразделений.

**4. Действия в ответ на запросы по ПДн**

**4.1.** В случае поступления Запроса субъекта ПДн или его законного представителя по персональным данным необходимо выполнить следующие действия:

**4.1.1.** При получении запроса субъекта персональных данных или его представителя на наличие ПДн необходимо в течение 10 дней с даты получения запроса (согласно пункту 1 статьи 20 152-ФЗ) подтвердить обработку ПДн, в случае ее осуществления. Если обработка ПДн субъекта не ведется, то в течение 10 дней с даты получения запроса (согласно пункту 2 статьи 20 152-ФЗ) необходимо отправить уведомление об отказе подтверждения обработки ПДн.

При получении запроса субъекта персональных данных или его представителя на ознакомление с ПДн необходимо в течение 10 дней с даты получения запроса (согласно пункту 1 статьи 20 152-ФЗ) предоставить для ознакомления ПДн, в случае осуществления обработки этих

ПДн. Если обработка ПДн субъекта не ведется, то в течение 10 дней с даты получения запроса (согласно пункту 2 статьи 20 152-ФЗ) необходимо отправить уведомление об отказе предоставления информации по ПДн. Субъект ПДн или его законный представитель имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение обработки ПДн, а также правовые основания и цели такой обработки;
- способы обработки ПДн;
- сведения о лицах, которые имеют доступ к ПДн;
- перечень обрабатываемых ПДн и источник их получения;
- сроки обработки ПДн, в том числе сроки их хранения;

**4.1.2.** При получении запроса субъекта персональных данных или его представителя на уточнение ПДн необходимо внести в них необходимые изменения в срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными. По итогам проведенных мероприятий необходимо отправить уведомление о внесенных изменениях.

Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн субъекта являются неполными, неточными или неактуальными, необходимо в течение 10 дней с даты получения запроса отправить уведомление об отказе осуществления изменения ПДн.

**4.1.3.** При получении запроса субъекта персональных данных или его представителя на уничтожение ПДн необходимо их уничтожить в срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно пункту 3 статьи 20 152-ФЗ) и отправить уведомление об уничтожении. Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Банк, являются незаконно полученными или не являются необходимыми для заявленной цели обработки, также в силу необходимости обработки ПДн по требованиям иных законодательных актов, то необходимо в течение 10 дней с даты получения запроса отправить уведомление об отказе уничтожения ПДн.

**4.1.4.** При получении запроса на отзыв согласия на обработку ПДн необходимо прекратить их обработку и, в случае, если сохранение ПДн более не требуется для целей обработки персональных данных, уничтожить ПДн в срок, не превышающий 10 дней с даты поступления указанного отзыва (согласно пункту 5 статьи 21 152-ФЗ), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных, либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами (согласно пункту 5 статьи 21 152-ФЗ). В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5 настоящей статьи, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

**4.1.5.** При выявлении недостоверности ПДн при обращении или по запросу субъекта ПДн или его представителя необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, необходимо уточнить персональные данные в течение 7 рабочих дней со дня представления таких сведений и снять блокирование персональных данных (согласно пункту 2 статьи 21 152-ФЗ). Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения ПДн.

**4.1.6.** При выявлении неправомерных действий с ПДн при обращении или по запросу субъекта

ПДн или его представителя необходимо в срок, не превышающий 3 рабочих дней с даты этого выявления, прекратить неправомерную обработку персональных данных (согласно пункту 3 статьи 21 152-ФЗ). В случае если обеспечить правомерность обработки персональных данных невозможно, Банк в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных (согласно пункту 3 статьи 21 152-ФЗ), обязан уничтожить такие персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Банк обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

**4.1.7.** При достижении целей обработки ПДн Банк обязан незамедлительно прекратить обработку ПДн или обеспечить ее уничтожение в срок, не превышающий 10 дней с даты достижения цели обработки ПДн (согласно пункту 4 статьи 21 152-ФЗ), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

**4.2. В случае поступления Запроса Уполномоченного органа по защите прав Субъекта ПДн по персональным данным (Роскомнадзора)** необходимо выполнить следующие действия:

**4.2.1.** При получении запроса необходимо в течение 10 дней (согласно пункту 4 статьи 20 152-ФЗ) предоставить информацию, необходимую для осуществления деятельности указанного органа.

**4.2.2.** При выявлении недостоверных ПДн по запросу Уполномоченного органа по защите прав Субъекта ПДн или обращению Субъекта ПДн необходимо их блокировать с момента получения такого запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его законным представителем, необходимо в течении 7 рабочих дней уточнить ПДн и снять их блокирование (согласно пункту 2 статьи 21 152-ФЗ). Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения и снять блокирование ПДн.

**4.2.3.** При выявлении неправомерных действий с ПДн Банком по запросу Уполномоченного органа по защите прав Субъекта ПДн или обращению Субъекта ПДн необходимо прекратить неправомерную обработку в срок, не превышающий 3 рабочих дней, с момента получения такого запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ). В случае невозможности обеспечения правомерности обработки Учреждением ПДн в срок, не превышающий 10 рабочих дней, с даты выявления неправомерности действий с ПДн, необходимо уничтожить ПДн и отправить уведомление об уничтожении ПДн.

**4.2.4.** При достижении целей обработки ПДн Банк обязан незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в течение 10 дней с даты достижения цели обработки ПДн (согласно пункту 4 статьи 21 152-ФЗ), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных, либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами и отправить уведомление об уничтожении ПДн.

## **5. Прием запросов от субъектов ПДн или его законных представителей, а также от уполномоченного органа, по защите прав субъектов ПДн**

При получении запросов, перечисленных в разделе 4 настоящего Регламента сотрудники выполняют следующие действия:

**5.1.** В случае поступления запроса субъекта ПДн или его законного представителя необходимо зарегистрировать запрос в «Журнале жалоб/претензий», который ведется УОО.

При личном обращении субъекта персональных данных в Банк, сотрудник предоставляет форму запроса в соответствии с Приложениями 4-6 настоящей Политики для заполнения



субъектом ПДн или принимает запрос в произвольной форме. После принятия заполненной формы или запроса в произвольной форме сотрудник сверяет сведения в запросе с предоставленными ему документами. Необходимые сведения о субъекте ПДн, которые должны присутствовать в подаваемом запросе:

- Фамилия, имя и отчество субъекта ПДн;
- номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя.

В случае неправильной формы запроса или отсутствии документов, удостоверяющих личность субъекта ПДн или его законного представителя, сотрудник **вправе отказать** в приеме запроса и потребовать переделать запрос в соответствии с законом 152-ФЗ.

При отказе субъекта ПДн или его законного представителя переделать запрос, данный факт фиксируется в «Журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных».

Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

**Если запрос оформлен в соответствии с требованиями законодательства, он принимается к обработке и передается лицу, ответственному за организацию обработки персональных данных, в соответствии с разделом 3 настоящего Регламента.**

**5.2.** В случае поступления Запроса уполномоченного органа по защите прав субъектов персональных данных необходимо зарегистрировать запрос в «Журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных».

Запрос принимается к обработке и передается лицу, ответственному за организацию обработки персональных данных, в соответствии с разделом 3 настоящего Регламента.

## **Порядок уведомления уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзора)**

В соответствии с ч. 3.1 ст. 21 федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее – Закон № 152-ФЗ) в случае установления в факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, с момента выявления такого инцидента Банком, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом Банк уведомляет уполномоченный орган по защите прав субъектов персональных данных (далее – Роскомнадзор):

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Банком на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

### **В первичном уведомлении указываются сведения:**

✓ о произошедшем инциденте (дата и время его выявления, характеристики персональных данных, которые стали доступны третьим лицам, количество записей в базе данных, которая была скомпрометирована). При необходимости дополнительно сообщить об актуальности этой базы данных, а также о периоде, в течение которого были собраны персональные данные;

✓ о предполагаемых причинах, которые привели к нарушению прав субъектов персональных данных;

✓ о предполагаемом вреде, нанесенном правам субъектов персональных данных;

✓ о принятых мерах по устранению последствий инцидента;

✓ о лице, уполномоченном оператором персональных данных на взаимодействие с Роскомнадзором;

✓ иные сведения и материалы, в том числе об источнике получения информации об инциденте, а также подтверждающие принятие мер по устранению последствий инцидента (при наличии таких сведений).

Кроме того, в уведомлении приводятся данные оператора (Банка):

✓ полное и сокращенное наименование Банка;

✓ ИНН Банка;

✓ адрес Банка в пределах его места нахождения;

✓ адрес электронной почты ответственного за организацию обработки ПДн в Банке для направления информации от Роскомнадзора.

Если на момент направления первичного уведомления Банк располагает сведениями о результатах внутреннего расследования выявленного инцидента, он вправе указать такие сведения в первичном уведомлении.

### **В дополнительном уведомлении указываются сведения:**

✓ о результатах внутреннего расследования выявленного инцидента (о причинах, повлекших нарушение прав субъектов персональных данных и нанесенном им вреде, о дополнительно принятых мерах по устранению последствий инцидента (при наличии), а также о решении оператора о проведении внутреннего расследования с указанием его реквизитов);

✓ о лицах, действия которых стали причиной инцидента (Ф.И.О. физического лица или ИП, наименование юридического лица, IP-адрес компьютера или устройства, предполагаемое местонахождение таких лиц и устройств, иные сведения).

**Уведомления может быть направлено как на бумажном носителе, так и в форме электронного документа:**

✓ уведомление на бумаге направляется по адресу места нахождения Роскомнадзора в городе Санкт-Петербург;

✓ уведомление в электронном виде направляется путем заполнения формы на портале персональных данных Роскомнадзора (после прохождения идентификации и аутентификации через ЕСИА) и подписывается электронной подписью.

Получив первичное уведомление Банка, Роскомнадзор направляет на указанный в уведомлении адрес электронной почты информационное письмо, в котором называет дату и время передачи уведомления, а также его ключ и номер. Номер и ключ первичного уведомления нужно указать при подаче дополнительного уведомления.

При обнаружении неполных или некорректных сведений Роскомнадзор в течение трех рабочих дней направляет по адресу электронной почты Банка, указанному в первичном уведомлении запрос о предоставлении недостающих сведений или пояснений. Предоставить такие сведения или пояснения нужно в течение трех рабочих дней со дня получения запроса от Роскомнадзора.

Если Банк не предоставит дополнительное уведомление в установленные сроки, Роскомнадзор вправе потребовать сведения о результатах внутреннего расследования выявленного инцидента. Ответ на такое требование нужно представить в течение одного рабочего дня со дня его получения.

В случае если Роскомнадзор самостоятельно выявит факт утечки базы персональных данных, содержание которой указывает на ее принадлежность к Банку, то Банку направляется требование о необходимости предоставить первичное или дополнительные уведомления. Предоставить их нужно в сроки 24 часа – для первичного уведомления, 72 часа – для дополнительного соответственно.

Если Банк, получив требование Роскомнадзора, выяснит, что скомпрометированная база персональных данных ему не принадлежит, он направляет в Роскомнадзор дополнительное уведомление, к которому прикладывает акт о проведенном внутреннем расследовании, подтверждающий отсутствие факта неправомерной передачи или распространения персональных данных.

Если Банк выяснит, что сведения об утечке базы данных ранее уже направлялись в Роскомнадзор, он направляет в ведомство уведомление, в котором указывает дату и номер ранее направленного уведомления.

**Ответственность за утечку персональных данных (обработку без согласия субъектов персональных данных) установлена ч. 2 ст. 13.11 КоАП РФ.**