



УТВЕРЖДЕНО

Приказом председателя правления

АО «БАНК ОРЕНБУРГ»

от «05» июня 2024 г. № 583

Введено в действие с

«05» июня 2024 г.

**ПОЛОЖЕНИЕ**  
**об организации обработки персональных данных**  
**в АО "БАНК ОРЕНБУРГ"**

(версия 2.2)

г. Оренбург 2024

## РЕКВИЗИТЫ ДОКУМЕНТА

| История изменений |            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                               |                                                                           |
|-------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------|
| Версия            | Дата       | Перечень федеральных законов, нормативных документов Банка России с учетом которых создается ВНД Банка                                                                                                                                                                                                                                                                                                                                                                  | Причина изменений             | Ответственное подразделение (кто разрабатывает документ/вносит изменения) |
| 1.0               | 26.01.2021 | Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Трудового кодекса Российской Федерации, Постановление Правительства от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" | Исходный документ (начальный) | Отдел информационной безопасности                                         |
| 2.0               | 31.08.2022 | Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Трудового кодекса Российской Федерации, Постановление Правительства от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" | Изменения в законодательстве  | Отдел информационной безопасности                                         |
| 2.1               | 16.02.2023 | Федеральный закон от 14.07.2022 № 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»<br>Приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»                                                              | Изменения в законодательстве  | Отдел информационной безопасности                                         |
| 2.2               | 05.06.2024 | Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Трудового кодекса Российской Федерации, Постановление Правительства РФ                                                                                                                                                                                                                                                                                                                                | Изменения в законодательстве  | Отдел информационной безопасности                                         |

|  |  |                                                                                                                                                                                                                                                                                             |  |  |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  | от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Информационное письмо Банка России от 16.04.2024 № ИН-03-25/27 «Об устранении (прекращении) последствий контрольных мероприятий Банка России» |  |  |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

## СОДЕРЖАНИЕ

|                                                                                                                                                  |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. ОБЩИЕ ПОЛОЖЕНИЯ .....                                                                                                                         | 5  |
| 2. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ .....                                                                                                      | 6  |
| 3. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ .....                                                                                        | 7  |
| 4. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ<br>ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ.....                                         | 7  |
| 5. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ .....                                                                                         | 10 |
| 6. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ<br>ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ<br>НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ..... | 15 |
| 7. СФЕРЫ ОТВЕТСТВЕННОСТИ .....                                                                                                                   | 21 |
| 8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ .....                                                                                                                | 22 |

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

### 1.1. Назначение Положения

1.1.1. Положение об организации обработки персональных данных в АО «БАНК ОРЕНБУРГ» (далее — Положение) разработано в соответствии с требованиями Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», других нормативных актов, определяющих случаи и особенности обработки персональных данных и обеспечения безопасности и конфиденциальности такой информации.

1.1.2. Настоящее Положение разработано в целях обеспечения необходимого и достаточного уровня информационной безопасности персональных данных и процессов, связанных с их обработкой в АО «БАНК ОРЕНБУРГ» (далее Банк), а также для обеспечения защиты прав и свобод субъектов персональных данных при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.1.3. Настоящее Положение регламентирует действия работников Банка по обеспечению конфиденциальности персональных данных граждан, обратившихся за оказанием банковских услуг, партнеров Банка по сделкам, безопасности данных при их обработке в информационной системе и является обязательным для исполнения всеми работниками Банка, имеющими доступ к персональным данным.

### 1.2. Цели Положения

1.2.1. Целью Положения является обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных Банком.

### 1.3. Основные понятия

1.3.1. В Положении используются следующие термины и определения:

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

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

**Биометрические персональные данные** — сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

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

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

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

**Оператор** — юридическое (Банк) или физическое (сотрудник Банка) лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

**Персональные данные, разрешенные субъектом персональных данных для распространения** — персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом.

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

**Распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

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

#### **1.4. Область действия**

1.4.1. Положения распространяются на все отношения, связанные с обработкой персональных данных, осуществляемой Банком:

— с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеке или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным;

— без использования средств автоматизации.

1.4.2. Настоящим Положением должны руководствоваться все сотрудники Банка, осуществляющие обработку персональных данных или имеющие к ним доступ.

## **2. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

### **2.1. Обработка персональных данных осуществляется Банком в следующих целях:**

- осуществления банковских операций и сделок в соответствии с Уставом Банка и выданными Банку лицензиями на совершение банковских и иных операций;
- заключения с субъектом персональных данных любых договоров и их дальнейшего исполнения;
- проведения Банком акций, опросов, исследований;
- предоставления субъекту персональных данных информации о деятельности Банка; об оказываемых Банком услугах, о разработке Банком новых продуктов и услуг; об услугах дочерних обществ Банка;
- информирования клиента о предложениях по продуктам и услугам Банка;
- ведения кадровой работы и организации учета работников Банка;
- привлечения и отбора кандидатов на работу в Банке;
- формирования статистической отчетности, в том числе для предоставления Банку России;
- осуществления Банком административно-хозяйственной деятельности;
- регулирования трудовых и иных, непосредственно связанных с ними отношений;
- выявления случаев мошенничеств, хищения денежных средств со счета, иных противоправных действий, предотвращения таких противоправных действий в дальнейшем и локализации последствий таких действий;

— в иных целях в соответствии с действующим законодательством РФ.

### 3. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Основанием обработки персональных данных в Банке являются следующие нормативные акты и документы:

- Налоговый кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- Закон РФ от 19.04.1991 № 1032-1 «О занятости населения в Российской Федерации»;
- Федеральный закон "О банках и банковской деятельности" от 02.12.1990 N 395-1;
- Иные Федеральные законы в рамках действующего законодательства РФ.

3.2. Обработка персональных данных прекращается при реорганизации или ликвидации Банка.

### 4. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В соответствии с целями обработки персональных данных, указанными в разделе 2 настоящего Положении, Банком осуществляется обработка следующих категорий субъектов персональных данных:

| Категории субъектов, персональных данных обрабатываемых в Банке                                                                                                                                                         | Сроки хранения                                | Цели обработки                                                                                                                                  | Перечень обрабатываемых ПДн                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Персональные данные клиента (потенциального Клиента, контрагента), а также персональные данные руководителя, участника (акционера) юридического лица, являющегося Клиентом (потенциальным Клиентом, контрагентом) Банка | 5 лет после окончания срока действия договора | Заключения с субъектом персональных данных любых договоров и их дальнейшего исполнения                                                          | Фамилия, имя, отчество, дата и место рождения, реквизиты документа, удостоверяющего личность, ИНН, адрес, телефон, адрес электронной почты, гражданство, пол, семейное, социальное, имущественное положение, образование, профессию, трудовую деятельность, доходы, сведения, характеризующие соблюдение законодательства Российской Федерации, информацию об индивидуальном лицевом счете застрахованного лица (СНИЛС), реквизиты банковского счета, данные изображения лица человека, полученные с помощью фото-видео устройств, данные голоса человека, полученные с помощью звукозаписывающих устройств, сведения, полученные от третьих лиц, в том числе государственных органов, государственных информационных систем, единой системы идентификации и аутентификации (ЕСИА), ПФРФ, в том числе через систему межведомственного электронного взаимодействия (СМЭВ) и/или из |
|                                                                                                                                                                                                                         | 5 лет после закрытия счета                    | Осуществления банковских операций и сделок в соответствии с Уставом Банка и выданными Банку лицензиями на совершение банковских и иных операций |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                                     |                                                                                    |                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     |                                                                                    |                                                                                                                                                                                                     | сети Интернет, и/или из иных общедоступных источников персональных данных и иную информацию, в том числе номер и дату выдачи полиса обязательного медицинского страхования (ОМС)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                                     | 5 лет после окончания срока действия договора                                      | Информирования клиента о предложениях по продуктам и услугам Банка                                                                                                                                  | Фамилия, имя, отчество, число, месяц, год и место рождения, реквизиты документа, удостоверяющего личность, адрес, телефон, финансовая информация о клиенте                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                                     |                                                                                    | Проведения Банком акций, опросов, исследований                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                     |                                                                                    | Предоставления субъекту персональных данных информации об оказываемых Банком услугах, о разработке Банком новых продуктов и услуг; об услугах дочерних обществ Банка                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                     |                                                                                    | Выявления случаев мошенничеств, хищения денежных средств со счета, иных противоправных действий, предотвращения таких противоправных действий в дальнейшем и локализации последствий таких действий | Фамилия, имя, отчество, число, месяц, год и место рождения, реквизиты документа, удостоверяющего личность, адрес, телефон, финансовая информация о клиенте, персональные данные клиента (потенциального Клиента, контрагента), а также персональные данные руководителя, участника (акционера) юридического лица, являющегося Клиентом (потенциальным Клиентом, контрагентом) Банка, персональные данные клиента (потенциального Клиента, контрагента), а также персональные данные руководителя, участника (акционера) юридического лица, являющегося Клиентом (потенциальным Клиентом, контрагентом) Банка                                                         |
| Персональные данные работника Банка | 3 года после увольнения, личные дела 50 лет (75 лет – если оформлены до 2003 года) | Ведения кадровой работы и организации учета работников Банка                                                                                                                                        | Фамилия, имя, отчество, число, месяц, год и место рождения, сведения о гражданстве, сведения об образовании, сведения о выполняемой работе с начала трудовой деятельности, сведения о стаже, сведения о заработной плате, адрес регистрации по месту жительства и адрес фактического проживания, номер телефона, паспортные данные, профессия, занимаемая должность, табельный номер, сведения о воинском учете, данные идентификационного номера налогоплательщика, данные страхового свидетельства пенсионного страхования, семейное положение, сведения о составе семьи (степень родства, фамилия, имя, отчество, год рождения), фотография, сведения о повышении |
|                                     | 3 года после увольнения                                                            | Осуществления Банком административно-хозяйственной деятельности                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                     | 3 года после увольнения                                                            | Регулирования трудовых и иных, непосредственно связанных с ними отношений                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|                                                                                                                                                                                  |                                                                                                  |                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                  |                                                                                                  |                                                                                                                                                                                         | квалификации и профессиональной подготовке иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                                                                                                                                                                                  | 3 года после увольнения                                                                          | Предоставления информации о деятельности Банка                                                                                                                                          | Фамилия, имя, отчество, данные о профессии и должности, фотографическое изображение, видеоизображение, аудиозапись голоса                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                                                                                                                                                                                  | в случае утраты необходимости в достижении этих целей 4 месяца с момента предоставления согласия | Привлечения и отбора кандидатов на работу в Банке                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Персональные данные аффилированного лица или персональные данные руководителя, акционера или сотрудника юридического лица, являющегося аффилированным лицом по отношению к Банку | 3 года после увольнения                                                                          | Формирования статистической отчетности, в том числе для предоставления Банку России                                                                                                     | Фамилию, имя, отчество, дату и место рождения, реквизиты документа, удостоверяющего личность                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Персональные данные уполномоченных представителей (служащих) Банка России и персональные данные третьих лиц, предоставленные в рамках проведения контрольных мероприятий         | не более 30 дней с момента завершения контрольных мероприятий                                    | Совершение сделки, либо создание условий для совершения сделки в рамках обычной хозяйственной деятельности Банка с проведением наличных или безналичных расчётов, или без их проведения | Фамилия, имя, отчество, дата и место рождения, реквизиты документа, удостоверяющего личность, ИНН, адрес, телефон, адрес электронной почты, гражданство, пол, семейное, социальное, имущественное положение, образование, профессию, трудовую деятельность, доходы, сведения, характеризующие соблюдение законодательства Российской Федерации, информацию об индивидуальном лицевого счета застрахованного лица (СНИЛС), реквизиты банковского счета, данные изображения лица человека, полученные с помощью фото-видео устройств, данные голоса человека, полученные с помощью звукозаписывающих устройств, сведения, полученные от третьих лиц, в том числе государственных органов, государственных информационных систем, единой системы идентификации и аутентификации (ЕСИА), ПФРФ, в том числе через систему межведомственного электронного взаимодействия (СМЭВ) и/или из сети Интернет, и/или из иных общедоступных источников персональных данных и иную информацию, в том числе номер и дату выдачи полиса обязательного медицинского страхования (ОМС) |

4.2. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Банк обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации, обрабатываемых в следующих информационных системах: автоматизированная банковская система, автоматизированное рабочее место клиента Банка России новое, дистанционного банковского обслуживания и АРМ ЦФТ-Госуслуги.

## **5. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

### **5.1. Принципы обработки персональных данных**

Обработка персональных данных осуществляется Банком в соответствии со следующими принципами:

- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- обработка персональных данных осуществляется в соответствии с конкретными, заранее определенными и законными целями и производится до момента достижения этих целей;
- объединение баз данных, содержащих персональные данные, цели, обработки которых не совместимы между собой, недопустимо;
- содержание и объем обрабатываемых персональных данных не противоречат заявленным целям обработки, не являются избыточными по отношению к ним;
- при обработке персональных данных в Банке обеспечиваются точность, достаточность, актуальность персональных данных по отношению к целям их обработки за счет применения необходимых мер по удалению или уточнению неполных, или неточных данных;
- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем это необходимо в соответствии с целями их обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не установлено федеральным законом.

### **5.2 Условия обработки персональных данных**

Условия обработки персональных данных, отличные от получения согласия субъекта персональных данных на обработку его персональных данных, являются альтернативными.

#### **5.2.1 Условия обработки специальных категорий персональных данных**

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, Банком не производится.

#### **5.2.2 Условия обработки биометрических персональных данных**

Обработка биометрических категорий персональных данных осуществляется Банком при наличии согласия в письменной форме субъекта персональных данных.

Представление биометрических персональных данных не может быть обязательным, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона «О персональных данных». Банк не вправе отказывать в обслуживании в случае отказа субъекта персональных данных предоставить биометрические персональные данные и (или) дать согласие на обработку персональных данных, если в соответствии с Федеральным законом «О персональных данных» получение оператором согласия на обработку персональных данных не является обязательным.

#### **5.2.3. Условия обработки иных персональных данных**

Обработка иных категорий персональных данных осуществляется Банком с соблюдением следующих условий:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для

осуществления и выполнения возложенных законодательством Российской Федерации на Банк, полномочий обязанностей;

— обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

— обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных, или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. 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.

#### 5.2.4. Поручение обработки персональных данных

5.2.4.1. Банк вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее – поручения).

5.2.4.2. Лицо, осуществляющее обработку персональных данных по поручению Банка, соблюдает принципы и правила обработки персональных данных, предусмотренные настоящим Положением, соблюдает конфиденциальность персональных данных, принимает необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных». В поручении Банка должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, способы и цели их обработки, установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статей 18.1 Федерального закона «О персональных данных», обязанность по запросу Банка в течение срока действия поручения, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятия мер и соблюдение в целях исполнения поручения Банка требований, установленных в соответствии с частью 3 статьи 6 Федерального закона «О персональных данных».

5.2.4.3. При поручении обработки персональных данных другому лицу ответственность перед субъектом персональных данных за действия указанного лица несет Банк. Лицо, осуществляющее обработку персональных данных по поручению Банка, несет ответственность перед Банком.

5.2.4.4. В случае, если Банк поручает обработку персональных данных иностранному физическому лицу или иностранному юридическому лицу, ответственность перед субъектом персональных данных за действия указанных лиц несет Банк и лицо, осуществляющее обработку персональных данных по поручению Банка.

#### 5.2.5. Передача персональных данных

5.2.5.1. Банк вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органом по основаниям, предусмотренным действующим законодательством Российской Федерации.

### 5.3. Конфиденциальность персональных данных

5.3.1 Сотрудник Банка, получивший доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.3.2 Банк определяет места хранения отдельных категорий персональных данных (их материальных носителей), обрабатываемых без использования средств автоматизации. При этом обеспечивается раздельное хранение персональных данных, обработка которых осуществляется в

различных целях. В подразделениях Банка назначаются ответственные за соблюдение порядка хранения персональных данных.

5.3.3. Сохранность персональных данных и исключение несанкционированного доступа к ним обеспечиваются путем:

— хранения документов, содержащих персональные данные в рабочее и нерабочее время в металлических запирающихся шкафах, либо специально выделенных для хранения помещениях с регламентированным доступом;

— передачей на архивное хранение либо уничтожением документов, содержащих персональные данные, при достижении целей их обработки.

5.3.4. Доступ к информационным системам, содержащим персональные данные, обеспечивается использованием средств защиты от несанкционированного доступа и копирования. Помещения, где осуществляется хранение, и обработка персональных данных отвечают требованиям, обеспечивающим их сохранность в соответствии с законодательством РФ.

#### **5.4. Общедоступные источники персональных данных**

5.4.1. В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

5.4.2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

#### **5.5. Согласие субъекта персональных данных на обработку его персональных данных**

5.5.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информативным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных проверяются Банком.

5.5.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Банком вправе продолжить обработку персональных данных без согласия субъекта персональных данных при выполнении альтернативных условий обработки персональных данных.

5.5.4. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство выполнения альтернативных условий обработки персональных данных возлагается на Банк.

5.5.5. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного

документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес Оператора;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Банком способов обработки персональных данных;

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

9) подпись субъекта персональных данных.

5.5.7. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

5.5.8. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

5.5.9. Персональные данные могут быть получены Банком от лица, не являющегося субъектом персональных данных, при условии предоставления Банку подтверждения наличия альтернативных условий обработки информации.

## **5.6. Трансграничная передача персональных данных**

5.6.1. Трансграничная передача персональных данных осуществляется в соответствии с 152-ФЗ «О персональных данных» и международными договорами Российской Федерации.

5.6.2. Трансграничная передача персональных данных осуществляется, как в страны, обеспечивающие адекватную защиту прав субъектов персональных данных, так и в страны, не обеспечивающие адекватную защиту прав субъектов персональных данных в целях осуществления переводов с использованием в платежных системах в рамках заключенных договоров.

5.6.3. Банк до начала осуществления деятельности по трансграничной передаче персональных данных уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных.

## **5.7. Обработка персональных данных, осуществляемая без использования средств автоматизации**

5.7.1 Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронные носители информации.

5.7.1.1. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

5.7.1.2. При неавтоматизированной обработке персональных данных на бумажных носителях:

— не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

— персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

— документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

— дела с документами, содержащими персональные данные, должны иметь внутренние

описи документов с указанием цели обработки и категории персональных данных.

5.7.1.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.7.1.4. Неавтоматизированная обработка персональных данных в электронном виде осуществляется с применением организационных (охрана посещений) и технических мер, исключающих возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.

К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

5.7.1.5. При несовместимости целей неавтоматизированной обработки персональных данных, блок зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

5.7.1.6. Документы и внешние электронные носители информации, содержание персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

5.7.1.7. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

## **6. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ**

### **6.1. Права субъекта персональных данных на доступ к его персональным данным**

#### **6.1.1. Право субъекта персональных данных на доступ к его персональным данным**

**6.1.1.1.** Субъект персональных данных имеет право на получение информации (далее – запрашиваемая субъектом информация), касающейся обработки его персональных данных, в том числе содержащей:

- 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 сотрудников 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 соответствующему 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 Федеральным законом «О персональных данных»;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка поручена или будет поручена такому лицу;
- 10) информацию о способах исполнения Банка обязанностей, установленных статьей 18.1 Федерального закона «О персональных данных»;
- 11) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

**6.1.1.2.** Субъект персональных данных имеет право на получение запрашиваемой субъектом информации, за исключением следующих случаев:

— обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

— обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо предъявившими субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательства Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

— обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

— доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

— обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного

вмешательства.

6.1.1.3. Субъект персональных данных вправе требовать от Банка уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите информации.

6.1.1.4. Запрашиваемая субъектом информация должна быть предоставлена субъекту персональных данных Банком в доступной форме, и в ней не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.1.1.5. Запрашиваемая информация предоставляется субъекту персональных данных или его представителю Банка в течение десяти рабочих дней с момента обращения либо получения Банком запроса субъекта персональных данных или его представителя. 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. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения подтверждающие участие субъекта персональных данных в отношениях с Банком (номер договора, дата заключения договора, условное словесное обозначения и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Банком, подпись субъекта персональных данных или его представителя (далее – необходимая для запроса информация). Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Банк предоставляет запрашиваемые сведения субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение или запрос, если иное не указано в обращении или запросе.

6.1.1.6. В случае если запрашиваемая субъектом информация, 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 запрашиваемой субъектом информации и ознакомления с такими персональными данными не ранее чем через тридцать дней (далее – нормативный срок запроса) после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативно правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.1.1.7. Субъект персональных данных вправе обратиться повторно в Банк или направить повторный запрос в целях получения запрашиваемой субъектом информации, а также в целях ознакомления с обрабатываемыми персональными данными до истечения нормативного срока запроса, 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 с необходимой для запроса информацией должен содержать обоснования направления повторного запроса.

6.1.1.8. Банк вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Банке.

6.1.2. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации

6.1.2.1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации Банком не осуществляется.

6.1.3. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

6.1.4. Право на обжалование действий или бездействия Банка

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

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

## **6.2. Обязанности оператора**

### **6.2.1. Обязанности оператора при сборе персональных данных**

6.2.1.1. При сборе персональных данных Банк предоставляет субъекту персональных данных по его просьбе запрашиваемую информацию, касающуюся обработки его персональных данных в соответствии с частью 7 статьи 14 Федерального закона «О персональных данных».

6.2.1.2. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение оператором согласия на обработку персональных данных являются обязательными, Банк разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

6.2.1.3. Если персональные данные получены не от субъекта персональных данных, Банк до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию (далее – информация, сообщаемая при получении персональных данных не от субъекта персональных данных):

- 1) наименование либо фамилия, имя, отчество и адрес Оператора или представителя Оператора;
- 2) цель обработки персональных данных и её правовое основание;
- 3) перечень персональных данных;
- 4) предполагаемые пользователи персональных данных;
- 5) установленные Федеральным законом «О персональных данных» права субъекта персональных данных;
- 6) источник получения персональных данных.

6.2.1.4. Банк не предоставляет субъекту информацию, сообщаемую при получении персональных данных не от субъекта персональных данных, в случаях, если:

- 1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных Банком;
- 2) персональные данные получены Банком на основании Федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;
- 3) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона «О персональных данных»;
- 4) предоставление субъекту персональных данных информации, сообщаемой при получении персональных данных не от субъекта персональных данных, нарушает права и законные интересы третьих лиц.

### **6.2.2. Меры, направленные на обеспечение выполнения Банком своих обязанностей**

6.2.2.1. Банк принимает меры, необходимые и достаточные для обеспечения выполнения своих обязанностей. Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, если иное не предусмотрено федеральными законами. К таким мерам, в частности, относятся:

- 1) назначение ответственного за организацию обработки персональных данных;
- 2) издание Положения, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных

данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям к защите персональных данных, Положению, локальным актам Банка;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

6) ознакомление сотрудников Банка, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, Положением, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.

#### 6.2.3. Меры по обеспечению безопасности персональных данных при их обработке

6.2.3.1. Банк при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, представления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

##### 6.2.3.2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением 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 Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением факторов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

6.2.3.3. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

#### 6.2.4. Обязанности оператора при обращении к нему субъекта персональных данных либо

при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

6.2.4.1. Банк сообщает в установленном порядке субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя. 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 представления запрашиваемой информации.

6.2.4.2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Банка дает в письменной форме мотивированный ответ в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. 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.

6.2.4.3. Банк предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Банк уничтожает такие персональные данные. Банк уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

6.2.4.4. Банк сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять дней в случае направления Банком в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.2.5. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных:

6.2.5.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Банк осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Банк осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы

субъекта персональных данных или третьих лиц.

6.2.5.2. В случае подтверждения факта неточности персональных данных Банк на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.2.5.3. В случае выявления неправомерной обработки персональных данных, осуществляемой Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению Банка. В случае если обеспечить правомерность обработки персональных данных невозможно, Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Банк уведомляет субъекта персональных данных или его представителя, а в случае, если обращения 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.

6.2.5.4. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Банком, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет 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, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также о лице, уполномоченном Банком на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным инцидентом;

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

6.2.5.5. В случае достижения цели обработки персональных данных Банк прекращает обработку персональных данных или обеспечивает её прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, 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 Федеральным законом «О персональных данных» или другими федеральными законами. При уничтожении персональных данных уполномоченных представителей Банка России, полученных в ходе контрольных мероприятий, Банк обязуется также информировать иных лиц, которым Банком были переданы указанные персональные данные, о необходимости подтверждения их уничтожения с учётом требований, установленных настоящим разделом Положения.

6.2.5.6. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Банком прекращает их обработку или обеспечивает прекращения такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по

поручению Банка) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

6.2.5.7. В случае обращения субъекта персональных данных с требованием о прекращении обработки персональных данных Банк в срок, не превышающий десяти рабочих дней с даты получения соответствующего требования, прекращает их обработку или обеспечивает прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2-11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона «О персональных данных». Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банка в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации

6.2.5.8. В случае отсутствия возможности уничтожения персональных данных в течении указанного срока, Банк блокирует такие персональные данные или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, по поручению Банка) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.2.5.9. Уничтожение документов на бумажных носителях, содержащих персональные данные, осуществляется путем шредирования. По итогам уничтожения документов составляется соответствующий акт, утверждаемый лицом, ответственным за соблюдение порядка хранения персональных данных в подразделении. Уничтожение документов, содержащих персональные данные, должно быть максимально надежным и конфиденциальным, исключая возможность последующего восстановления, уничтожение должно не допускать случайного или преднамеренного уничтожения актуальной документации.

6.2.5.10. В случае если обработка персональных данных осуществляется оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

6.2.5.11. В случае если обработка персональных данных осуществляется оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее – выгрузка из журнала).

6.2.5.12. Акт об уничтожении персональных данных и выгрузка из журнала должны соответствовать Требованиям к подтверждению уничтожения персональных данных, утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 №179.

## **7. СФЕРЫ ОТВЕТСТВЕННОСТИ**

### **7.1. Лица, ответственные за организацию обработки персональных данных в организациях**

7.1.1. Банком назначается лицо ответственное за организацию обработки персональных данных.

7.1.2. Лицо ответственное за организацию обработки персональных данных получает указание непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

7.1.3. Банк предоставляет лицу ответственному за организацию обработки персональных,

необходимые сведения.

7.1.4. Лицо ответственное за организацию обработки персональных данных, выполняет функции, предусмотренные законодательством Российской Федерации, а также нормативными документами Банка.

## **7.2. Ответственность**

7.2.1. Лица, виновные в нарушении требований Федерального закона «О персональных», несут предусмотренную законодательством Российской Федерации ответственность.

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

## **8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

8.1. Настоящее Положение подлежит размещению на официальном сайте Банка по адресу: <https://orbank.ru>.

8.2. Ответственность должностных лиц Банка, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Банка.

8.3. Пересмотр настоящего Положения должен производиться в случае изменения законодательства в области персональных данных и специальных нормативных документов по обработке и защите персональных данных, изменения бизнес-процессов Банка, требующих изменения перечня обрабатываемых персональных данных, а также по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности банковских информационных технологических процессов.

