У Т В Е Р Ж Д Е Н А

Правлением
АКБ «Трансстройбанк» (АО)
Протокол от «05» февраля 2025 г.
№ 05-25

Председатель Правления

_____ С. П. Читипаховян

Вступает в силу с «06» февраля 2025 г.

ПУБЛИЧНАЯ ПОЛИТИКА

ПО ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ в АКБ «Трансстройбанк» (АО)

Версия 5.25

Москва, 2025

ОГЛАВЛЕНИЕ:

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Публичная политика по обработке и защите персональных данных в АКБ «Трансстройбанк» (АО) (далее, соответственно, – «Политика» и «Банк») определяет политику АКБ «Трансстройбанк» (АО) в отношении обработки и обеспечения безопасности персональных данных.

1.2. Настоящая Политика разработана в соответствии с действующим законодательством Российской Федерации, регламентирующим защиту персональных данных, а также нормативными документами Банка России в области информационной безопасности с учетом Рекомендаций Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее также – «Федеральный закон № 152-ФЗ»).

1.3. Настоящая Политика применяется к обработке персональных данных граждан Российской Федерации, осуществляемой иностранными юридическими лицами или иностранными физическими лицами, на основании договора, стороной которого являются граждане Российской Федерации, иных соглашений между иностранными юридическими лицами, иностранными физическими лицами и гражданами Российской Федерации либо на основании согласия гражданина Российской Федерации на обработку его персональных данных.

1.4. Важнейшими условиями достижения целей деятельности Банка являются обеспечение законности обработки персональных данных в технологических процессах Банка, а также обеспечение необходимого уровня безопасности информационных активов, к которым, в том числе, относятся персональные данные.

1.5. Целью настоящей Политики является установление основных принципов и подходов к обработке и обеспечению безопасности персональных данных в Банке в рамках 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.

1.6. Действие настоящей Политики распространяется на все процессы Банка, связанные с обработкой персональных данных.

1.7. Политика обязательна для ознакомления и исполнения всеми работниками и должностными лицами Банка, осуществляющими обработку или имеющими доступ к персональным данным, и по отношению ко всем персональным данным, обрабатываемым в Банке.

1.8. Настоящая Политика является общедоступным документом, декларирующим основные принципы деятельности Банка при обработке и защите персональных данных, сведения о реализуемых требованиях к защите персональных данных**,** а также определяет условия обработки персональных данных в Банке и подлежит размещению на информационном стенде Банка, обеспечивающем неограниченный доступ для ознакомления клиентами Банка, а также публикации на официальном информационном сайте Банка в сети «Интернет» по адресу **http://www.transstroybank.ru.**

1.9. Во всех случаях, не охваченных положениями настоящей Политики, работники Банка руководствуются требованиями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, и внутренними нормативными документами Банка, регулирующими отношения, связанные с обработкой персональных данных, в том числе с использованием средств автоматизации и без использования таких средств.

1.10. На основании приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Банк включен в реестр операторов, осуществляющих обработку персональных данных.

1.11. Пересмотр и обновление настоящей Политики осуществляется в связи с изменениями законодательства Российской Федерации, нормативно-правовых актов регуляторов в области персональных данных, процессов или способов обработки персональных данных, категорий субъектов персональных данных, целей и сроков обработки персональных данных, а также по результатам анализа актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности и/или по результатам других контрольных мероприятий, проводимых Банком.

1.12. Регламенты (порядки) реагирования на запросы/обращения субъектов персональных данных и их представителей, уполномоченных органов по поводу неточности персональных данных, неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к своим данным, а также соответствующие формы уведомлений, журналов, актов, особенности обработки персональных данных, осуществляемой с использованием и без использования средств автоматизации и др. установлены в Банке иными внутренними локальными документами в области обработки персональных данных.

1.13. Перечень нормативных документов.

Настоящая Политика разработана в соответствии с требованиями действующего законодательства Российской Федерации, нормативными документами Банка России, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе с использованием следующих документов:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями) (далее также – «Федеральный закон № 152-ФЗ»);
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями);
- Федерального закона от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»;
- Федерального закона от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее – «Федеральный закон от 29.12.2022 № 572-ФЗ»);
- Федерального закона от 08.08.2024 № 233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»;
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об

утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановления Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Распоряжения Правительства РФ от 09.04.2024 № 856-Р «Об изменении распоряжения Правительства РФ от 30.06.2018 № 1322-Р»;
- Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения «СТО БР ИББС-1.0-2014» (принят и введен в действие Распоряжением Банка России от 17.05.2014 № Р-399);
- Положения Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями);
- Приказа ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- иных нормативных правовых актов Российской Федерации и нормативных документов исполнительных органов государственной власти;
- Рекомендаций Роскомнадзора по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящей Публичной политике использованы следующие термины с соответствующими определениями:

Банк – Акционерный коммерческий банк Трансстройбанк (Акционерное общество), являющийся в рамках Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» оператором по обработке персональных данных (организующий и (или) осуществляющий самостоятельно или совместно с другими лицами обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными);

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Администратор ИБ ИСПДн – администратор информационной безопасности

информационной системы ПДн (работник Банка, назначаемый приказом Председателя Правления Банка);

Биометрические персональные данные – данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;

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

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Конфиденциальность персональных данных – обязанность оператора, а также иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

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

Обработка персональных данных/Обработка – 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 – государственный орган, муниципальный орган, юридическое или физическое 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;

Ответственный за организацию обработки персональных данных – должностное лицо Банка, назначенное Приказом Председателя Правления Банка и организующее принятие правовых, организационных и технических мер в целях обеспечения надлежащего выполнения функций по организации обработки персональных данных в Банке в соответствии с положениями законодательства Российской Федерации в области персональных данных;

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

Персональные данные, разрешенные для распространения (ПДРР) – это 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;

Работник Банка – физическое лицо, состоящее с Банком в трудовых отношениях (на основании трудового договора) или заключившее с Банком договор подряда, договор возмездного оказания услуг или иной документ, определяющий прочие имущественные взаимоотношения и другие вопросы взаимодействия, и исполняющее служебные/договорные обязанности, принятое по основному месту работы, по совместительству или оказывающее Банку услуги по договору гражданско-правового характера;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных;

Субъект персональных данных (Субъект ПДн) – физическое лицо, прямо или косвенно определенное или определяемое на основании относящихся к нему персональных данных;

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановление содержания персональных данных в информационной системе персональных данных, и (или) в результате которых уничтожаются материальные носители персональных данных;

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

3.2. Цели обработки персональных данных в Банке происходят, в том числе, из анализа правовых актов, регламентирующих деятельность Банка, целей фактически осуществляемой Банком деятельности, а также деятельности, которая предусмотрена учредительными документами Банка, и конкретных бизнес-процессов Банка в конкретных информационных системах персональных данных (по структурным подразделениям Банка и их процедурам в

отношении определенных категорий субъектов персональных данных).

3.3. Банк осуществляет обработку полученных в установленном законом порядке персональных данных, принадлежащих:

кандидатам на работу и работникам Банка, клиентам - физическим лицам (владельцу счета, открытого в Банке, заемщику, вкладчику, выгодоприобретателю и иным лицам, пользующимся финансовыми услугами Банка), в том числе потенциальным клиентам, уполномоченным представителям клиентов (физических и юридических лиц, индивидуальных предпринимателей и др. категорий клиентов); уполномоченным представителям юридических лиц, являющихся клиентами Банка (владелец счета, открытого в Банке, заемщик), поручителям, залогодателям, физическим лицам, заключившим с Банком гражданско-правовые договоры на оказание услуг Банку; работникам партнеров Банка, субподрядчиков, поставщиков и других юридических лиц, имеющих договорные отношения с Банком, с которым взаимодействуют работники Банка в рамках своей деятельности; посетителям Банка; бенефициарным владельцам (физическим лицам) клиентов Банка; контрагентам клиентов – физическим лицам, **в следующих целях**:

3.3.1. осуществления банковской деятельности в соответствии с Уставом и Лицензиями Банка;

3.3.2. рассмотрение резюме соискателей на должность и принятие решения о возможности заключения трудового договора с ними;

3.3.3. заключение и исполнение трудовых договоров;

3.3.4. обеспечение соблюдения законов и иных нормативных правовых актов, в том числе исполнение требований трудового, пенсионного, страхового и социального законодательства РФ;

3.3.5. противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

3.3.6. предоставление информации по запросам органов, указанных в ст. 26 Федерального закона № 395-1 «О банках и банковской деятельности»;

3.3.7. участие в создании кредитных историй;

3.3.8. осуществление мероприятий по возврату просроченной задолженности;

3.3.9. ведение кадрового делопроизводства и организация учета работников;

3.3.10. содействие работникам в трудоустройстве, получении образования и продвижении по службе, а также пользовании различного вида льготами в соответствии с законодательством Российской Федерации;

3.3.11. контроль количества и качества выполняемой работы;

3.3.12. обеспечение личной безопасности работников;

3.3.13. обеспечение сохранности имущества Банка;

3.3.14. принятие решения о заключении договора с потенциальным клиентом/контрагентом Банка;

3.3.15. заключение, исполнение и прекращение гражданско-правовых договоров с физическими лицами: гражданами и индивидуальными предпринимателями, юридическими лицами;

3.3.16. продвижение услуг Банка на рынке;

3.3.17. защита законных прав и интересов Банка, в том числе в судах судебной системы РФ;

3.3.18. ведение Банком административно-хозяйственной деятельности;

3.3.19. ведение архива Банка;

3.3.20. осуществление иных функций, возложенных на Банк законодательством Российской Федерации, нормативными актами Банка России.

4. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Правовыми основаниями обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Банк осуществляет обработку персональных данных.

4.2. В зависимости от цели обработки персональных данных правовыми основаниями для такой обработки в Банке являются:

4.2.1. Устав Банка;

4.2.2. Лицензии Банка;

4.2.3. договор, заключенный между Банком и субъектом персональных данных;

4.2.4. согласие субъекта на обработку персональных данных (включая случаи, прямо не предусмотренные законодательством Российской Федерации, но соответствующие полномочиям Банка как оператора персональных данных);

4.2.5. общедоступность персональных данных субъекта;

4.2.6. Конституция РФ (в том числе статьи 23, 24);

4.2.7. трудовое законодательство РФ;

4.2.8. налоговое законодательство РФ;

4.2.9. пенсионное законодательство РФ;

4.2.10. страховое законодательство РФ;

4.2.11. социальное законодательство РФ;

4.2.12. Федеральный закон «О бухгалтерском учете» от 06.12.2011 № 402-ФЗ (с изменениями и дополнениями);

4.2.13. Федеральный закон «О защите прав потребителей» от 07.02.1992 № 2300-1 (с изменениями и дополнениями);

4.2.14. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» (с изменениями и дополнениями);

4.2.15. Федеральный закон 23.12.2003 № 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации» (с изменениями и дополнениями);

4.2.16. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изменениями и дополнениями);

4.2.17. Федеральный закон от 30.12.2004 № 218-ФЗ «О кредитных историях» (с изменениями и дополнениями);

4.2.18. Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах» (с изменениями и дополнениями);

4.2.19. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями);

4.2.20. Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изменениями и дополнениями);

4.2.21. Федеральный закон от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле» (с изменениями и дополнениями);

4.2.22. Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг» (с изменениями и дополнениями);

4.2.23. Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ (с изменениями и дополнениями);

4.2.24. Федеральный закон «О потребительском кредите (займе)» от 21.12.2013 № 353-ФЗ (с изменениями и дополнениями);

4.2.25. Федеральный закон «Об ипотеке (залоге недвижимости)» от 16.07.1998 № 102-ФЗ (с изменениями и дополнениями);

4.2.26. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

4.2.27. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4.2.28. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015);

4.2.29. Положение Банка России от 02.03.2012 № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

4.2.30. Положение Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств» (с изменениями и дополнениями);

4.2.31. Положение Банка России от 28.06.2017 № 590-П «О порядке формирования кредитными организациями резервов на возможные потери по ссудам, ссудной и приравненной к ней задолженности»;

4.2.32. Положение Банка России от 23.10.2017 № 611-П «О порядке формирования кредитными организациями резервов на возможные потери»;

4.2.33. Положение Банка России от 29 января 2018 г. № 630-П «О порядке ведения кассовых операций и правилах хранения, перевозки и инкассации банкнот и монеты Банка России в кредитных организациях на территории Российской Федерации» (с изменениями и дополнениями);

4.2.34. Указание Банка России от 15.07.2021 № 5861-У «О порядке представления кредитными организациями в уполномоченный орган сведений и информации в соответствии со статьями 7, 7.5 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

4.2.35. Указание Банка России от 16.08.2017 № 4498-У «О порядке передачи уполномоченными банками, государственной корпорацией «Банк развития и внешнеэкономической деятельности (ВНЕШЭКОНОМБАНК)» органам валютного контроля информации о нарушениях лицами, осуществляющими валютные операции, актов валютного законодательства Российской Федерации и актов органов валютного регулирования»;

4.2.36. Инструкция Банка России от 30.06.2021 № 204-И «Об открытии, ведении и закрытии банковских счетов и счетов по вкладам (депозитам)»;

4.2.37. Указание Банка России от 10.04.2023 № 6406-У «О формах, сроках, порядке составления и представления отчетности кредитных организаций (банковских групп) в Центральный банк Российской Федерации, а также о перечне информации о деятельности кредитных организаций (банковских групп)»;

4.2.38. Указание Банка России от 02.02.2021 № 5720-У «О порядке уведомления лиц, включенных в список инсайдеров, об их включении в такой список и исключении из него»;

4.2.39. Приказ Федеральной службы безопасности Российской Федерации (ФСБ России) от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

4.2.40. иные Приказы и руководящие документы регулирующих органов – Роскомнадзор, ФСТЭК и ФСБ России;

4.2.41. иные федеральные законы и нормативные правовые акты Российской Федерации и регуляторов, в целях исполнения которых и в соответствии с которыми Банк осуществляет обработку персональных данных.

5. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Объем и содержание (категории) обрабатываемых персональных данных в Банке соответствуют заявленным целям их обработки и не являются избыточными по отношению к заявленным целям их обработки.

5.2. Перечень персональных данных, обрабатываемых в Банке, определяется в соответствии с законодательством Российской Федерации и локальными актами Банка с учетом целей обработки персональных данных.

5.3. Банк обрабатывает персональные данные следующих категорий субъектов персональных данных:

5.3.1. кандидаты на вакантные должности Банка;

5.3.2. работники Банка;

5.3.3. ближайшие родственники работников Банка;

5.3.4. бывшие работники Банка;

5.3.5. физические лица, входящие в состав органов управления Банка;

5.3.6. аффилированные лица или представители юридического лица, являющегося аффилированным по отношению к Банку;

5.3.7. физические лица - клиенты Банка;

5.3.8. представители, учредители, акционеры юридических лиц – клиентов Банка;

5.3.9. физические лица – контрагенты Банка;

5.3.10. представители, учредители, акционеры юридических лиц – контрагентов Банка;

5.3.11. лица, попадающие в зону действия системы видеонаблюдения Банка в общественных местах;

5.3.12. лица, посещающие помещения ограниченного доступа Банка;

5.3.13. супруг/супруга клиента Банка, поручитель, залогодатель клиента Банка;

5.3.14. физические лица - получатели перевода денежных средств от клиентов Банка;

5.3.15. иные физические лица, обработка персональных данных которых необходима Банку для осуществления и выполнения возложенных на него законодательством РФ функций, полномочий и обязанностей.

5.4. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность **(биометрические персональные данные)** и которые используются Банком для установления личности субъекта персональных данных, **обрабатываются только при наличии согласия в письменной форме субъекта персональных данных**, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона № 152-ФЗ.

5.5. Обработка биометрических персональных данных может осуществляться в Банке без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

5.6. Предоставление биометрических ПДн не может быть обязательным, за исключением случаев, предусмотренных пунктом 5.5 настоящей Политики. Банк не вправе отказывать в обслуживании в случае отказа Субъекта ПДн предоставить биометрические ПДн и (или) дать согласие на обработку ПДн, если в соответствии с федеральным законом получение Банком согласия на обработку ПДн не является обязательным.

5.7. Банк, в целях оказания услуг с использованием Единой Биометрической Системы (ЕБС), в соответствии с Приказом Министерства цифрового развития, связи и массовых коммуникаций от 10 сентября 2021 г. № 930, осуществляет обработку, включая сбор и хранение следующих биометрических ПДн:

– данные изображения лица субъекта ПДн;

- данные голоса, собранные текстозависимым методом.

5.8. В Банке **не осуществляется обработка специальных категорий персональных данных**, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных частями 2 и 2.1 статьи 10 Федерального закона № 152-ФЗ.

5.9. Обработка специальных категорий персональных данных, указанных в пункте 5.8 настоящей Политики, допускается в следующих случаях из числа предусмотренных частями

2 и 2.1 статьи 10 Федерального закона № 152-ФЗ, а именно:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
2) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона № 152-ФЗ.
3) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации.

5.10. Обработка специальных категорий ПДн, осуществлявшаяся в случаях, предусмотренных пунктом 5.9 настоящей Политики, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено Федеральным законом № 152-ФЗ.

6. ПОРЯДОК, ОСНОВНЫЕ ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных Банком осуществляется на основе следующих принципов:

- ❒ законности и справедливость целей и способов обработки персональных данных;
- ❒ добросовестности Банка, как оператора персональных данных, что достигается путем выполнения требований законодательства Российской Федерации в отношении обработки персональных данных;
- ❒ соответствия состава и объема обрабатываемых персональных данных, а также способов обработки персональных данных заявленным целям обработки;
- ❒ обеспечения точности и достаточности, а в необходимых случаях и актуальности обрабатываемых персональных данных по отношению к заявленным целям обработки;
- ❒ уничтожения персональных данных по достижении целей обработки способом, исключающим возможность их восстановления (обработка персональных данных ограничивается достижением конкретных, заранее определенных целей обработки, не допускается нецелевая обработка персональных данных);
- ❒ недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- ❒ осуществления сбора и дальнейшей обработки только тех персональных данных, которые отвечают заявленным целям обработки;
- ❒ осуществления уничтожения или обезличивания персональных данных по достижении целей обработки или, в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.2. Обработка персональных данных допускается при выполнении хотя бы одного из следующих условий:

- ❒ обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- ❒ обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей;
- ❒ обработка персональных данных осуществляется в связи с участием лица в

конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

- ❒ обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);
- ❒ обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
- ❒ 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 ПДн, устанавливающие случаи обработки ПДн несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие Субъекта ПДн;
- ❒ обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- ❒ обработка персональных данных необходима для осуществления прав и законных интересов Банка или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- ❒ обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
- ❒ обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона № 152-ФЗ, при условии обязательного обезличивания персональных данных;
- ❒ осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

6.3. Персональные данные не раскрываются третьим лицам, не распространяются иным образом без согласия субъекта, за исключением случаев, предусмотренных действующим

законодательством РФ.

6.4. С согласия Субъекта ПДн Банк вправе поручить обработку ПДн другому лицу, 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 – «поручение Банка»). Лицо, осуществляющее обработку ПДн по поручению Банка, обязано соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом № 152-ФЗ, соблюдать конфиденциальность ПДн, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ. В поручении Банка должны быть определены перечень ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федерального закона № 152-ФЗ, обязанность по запросу Банка в течение срока действия поручения Банка, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Банка требований, установленных в соответствии с настоящей статьей, обязанность обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона № 152-ФЗ, в том числе требование об уведомлении Банка о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона № 152-ФЗ.

6.5. Лицо, осуществляющее обработку ПДн по поручению Банка, не обязано получать согласие Субъекта ПДн на обработку его ПДн.

6.6. В случае если Банк поручает обработку ПДн другому лицу, ответственность перед Субъектом ПДн за действия указанного лица несет Банк. Лицо, осуществляющее обработку ПДн по поручению Банка, несет ответственность перед Банком.

6.7. В случае если оператор поручает обработку ПДн иностранному физическому лицу или иностранному юридическому лицу, ответственность перед Субъектом ПДн за действия указанных лиц несет Банк и лицо, осуществляющее обработку ПДн по поручению Банка.

6.8. Банк вправе передавать персональные данные третьим лицам без получения согласия субъекта в случаях, предусмотренных действующим законодательством РФ.

6.9. Работники Банка, допущенные к обработке персональных данных, обязаны:

а) знать и неукоснительно выполнять положения:

- законодательства Российской Федерации в области персональных данных, настоящей Политики;
- внутренних документов Банка по вопросам обработки и обеспечения безопасности персональных данных;

б) обрабатывать персональные данные только в рамках выполнения своих должностных обязанностей;

в) не разглашать персональные данные, обрабатываемые в Банке;

г) сообщать о действиях других лиц, которые могут привести к нарушению положений настоящей Политики;

д) сообщать об известных фактах нарушения требований настоящей Политики Ответственному за организацию обработки персональных данных в Банке.

6.10. Безопасность персональных данных в Банке обеспечивается выполнением согласованных мероприятий, направленных на предотвращение (нейтрализацию) и

устранение угроз безопасности персональных данных, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и работы информационных систем персональных данных в случае реализации угроз.

6.11. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

7. ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Банк осуществляет обработку персональных данных с использованием средств автоматизации и без использования средств автоматизации, а также смешанным способом (включающим как автоматизированную, так и неавтоматизированную обработку).

7.2. В Банке запрещается принятие решений на основании исключительно автоматизированной обработки персональных данных, которые порождают юридические последствия в отношении субъекта персональных данных, или иным образом затрагивают его права и законные интересы, кроме случаев и условий, предусмотренных законодательством Российской Федерации в области персональных данных.

7.3. Представители органов государственной власти (в том числе, контролирующих, надзорных, правоохранительных и иных органов) получают доступ к персональным данным, обрабатываемым в Банке, в объеме и порядке, установленном законодательством Российской Федерации.

7.4. Банк осуществил уведомление уполномоченного органа по защите прав субъектов (Роскомнадзор) об осуществлении обработки персональных данных. Банк добросовестно и в соответствующий срок осуществляет актуализацию сведений, указанных в уведомлении.

8. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку ПДн может быть дано Субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя Субъекта ПДн полномочия данного представителя на дачу согласия от имени Субъекта ПДн проверяются Банком.

8.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- ❒ подтверждение факта обработки персональных данных Банком;
- ❒ правовые основания и цели обработки персональных данных;
- ❒ цели и применяемые Банком способы обработки персональных данных;
- ❒ 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;
- ❒ обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- ❒ порядок осуществления субъектом персональных данных прав, предусмотренных

Федеральным законом № 152-ФЗ;

- ❒ сроки обработки персональных данных, в том числе сроки их хранения;
- ❒ информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- ❒ наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка поручена или будет поручена такому лицу;
- ❒ информацию о способах исполнения Банком обязанностей, установленных статьей 18.1 Федерального закона № 152-ФЗ;
- ❒ иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими нормативными документами Банка России.

8.3. Сведения, указанные в пункте 8.2 настоящей Политики, должны быть предоставлены Субъекту ПДн Банком в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим Субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

8.4. Субъект ПДн, обработка персональных данных которого осуществляется Банком, имеет также право на:

- ❒ уточнение, блокирование или уничтожение персональных данных в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или используются для достижения целей, отличных от заявленной цели обработки;
- ❒ отзыв согласия на обработку персональных данных;
- ❒ иные права, установленные Федеральным законом № 152-ФЗ.

8.5. Право Субъекта персональных данных на получение информации, касающейся обработки его персональных данных, может быть ограничено в случаях, установленных Федеральным законом № 152-ФЗ.

8.6. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва Субъектом персональных данных согласия на обработку персональных данных Банк вправе продолжить обработку персональных данных без согласия Субъекта персональных данных при наличии оснований, указанных в Федеральном законе № 152-ФЗ.

8.7. Субъект персональных данных имеет также иные права, установленные Федеральным законом № 152-ФЗ.

8.8. Запросы/обращения Субъектов персональных данных по вопросам обработки персональных данных могут быть направлены в письменном виде по адресу Банка. Информация об адресах местонахождения размещена на официальном сайте Банка в сети «Интернет» по адресу: **https://www.transstroybank.ru**. Запрос может быть направлен в форме электронного документа, подписанного электронной подписью в соответствии с законодательством Российской Федерации.

8.9. Сведения, указанные в пункте 8.2 настоящей Политики, предоставляются Субъекту ПДн или его представителю Банком в течение 10 (Десяти) рабочих дней с момента обращения либо получения оператором запроса Субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на 5 (Пять) рабочих дней в случае направления Банком в адрес Субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Банк предоставляет сведения, указанные в пункте 8.2 настоящей Политики, Субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

8.10. Запрос Субъекта персональных данных должен содержать:

- ❒ серию и номер основного документа, удостоверяющего личность Субъекта персональных данных или его представителя;
- ❒ сведения о дате выдачи указанного документа и выдавшем его органе;
- ❒ сведения, подтверждающие наличие гражданско-правовых отношений между Банком и Субъектом ПДн (номер, дата заключения гражданско-правого договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Банком;
- ❒ подпись Субъекта ПДн или его представителя.

8.11. В случае, если сведения, указанные в пункте 8.2 настоящей Политики, а также обрабатываемые персональные данные были предоставлены для ознакомления Субъекту ПДн по его запросу, Субъект ПДн вправе обратиться повторно к Банку или направить ему повторный запрос в целях получения сведений, указанных в пункте 8.2 настоящей Политики, и ознакомления с такими ПДн не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект ПДн.

8.12. Субъект ПДн вправе обратиться повторно к Банку или направить ему повторный запрос в целях получения сведений, указанных в пункте 8.2 настоящей Политики, а также в целях ознакомления с обрабатываемыми ПДн до истечения 30 дней с даты первого запроса, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 8.9 настоящей Политики, должен содержать обоснование направления повторного запроса (причина его повторного (досрочного) направления).

8.13. Банк вправе отказать Субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 8.11 и 8.12 настоящей Политики. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Банке.

8.14. Право Субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка ПДн, включая ПДн, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
2) обработка ПДн осуществляется органами, осуществившими задержание Субъекта ПДн по подозрению в совершении преступления, либо предъявившими Субъекту ПДн обвинение по уголовному делу, либо применившими к Субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

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

4) доступ Субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

5) обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

8.15. Субъект вправе обратиться с требованием об уточнении, блокировке или уничтожении персональных данных, в случае, если персональные данные являются неполными, устаревшими, неточными, получены незаконно или не являются необходимыми для использования в заявленных целях.

8.16. 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 обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому Субъекту персональных данных, или обеспечить 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 обязан осуществить блокирование персональных данных, относящихся к этому Субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) 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.

8.17. 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 обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение 7 (Семи) рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

8.18. В случае выявления неправомерной обработки персональных данных, осуществляемой Банком или лицом, действующим по поручению оператора, Банк в срок, не превышающий 3 (Трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, Банк в срок, не превышающий 10 (Десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. 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.

8.19. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав Субъектов ПДн, Банк обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав Субъектов персональных данных или иным заинтересованным лицом уведомить Роскомнадзор:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав Субъектов ПДн, и предполагаемом вреде, нанесенном правам Субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с Роскомнадзором, 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).

8.20. В случае достижения цели обработки персональных данных Банк обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий 30 (Тридцати) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн, иным соглашением между Банком и Субъектом ПДн либо если Банк не вправе осуществлять обработку персональных данных без согласия Субъекта ПДн на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

8.21. В случае отзыва Субъектом персональных данных согласия на обработку его персональных данных Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) 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 либо если Банк не вправе осуществлять обработку персональных данных без согласия Субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

8.22. В случае обращения Субъекта персональных данных к Банку с требованием о прекращении обработки персональных данных Банк обязан в срок, не превышающий 10 (десяти) рабочих дней с даты получения Банком соответствующего требования, прекратить их обработку или обеспечить 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 № 152-ФЗ. 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.

8.23. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного выше, Банк 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 6 (Шесть) месяцев, если иной срок не установлен федеральными законами.

8.24. Подтверждение уничтожения персональных данных в случаях, предусмотренных пунктами 8.16 – 8.23 настоящей Политики осуществляется в соответствии с требованиями, установленными Роскомнадзором.

9. ОБЯЗАННОСТИ БАНКА КАК ОПЕРАТОРА

9.1. Обязанность предоставить доказательство получения согласия Субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в пунктах 2 – 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ, возлагается на Банк.

9.2. Банк при сборе персональных данных, в том числе посредством информационно телекоммуникационной сети «Интернет», обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

9.3. Банк как оператор персональных данных, определяет и принимает необходимые и достаточные меры для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, а также меры по обеспечению безопасности персональных данных при их обработке. Информация о принимаемых Банком мерах содержится в Разделе 11 настоящей Политики.

9.4. Банк несет иные обязанности, установленные Федеральным законом № 152-ФЗ.

9.5. Банк обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

9.6. Указанная в пункте 9.5 настоящей Политики информация (за исключением информации, составляющей государственную тайну) передается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, в Роскомнадзор.

9.7. Порядок передачи информации в соответствии с пунктом 9.6. настоящей Политики устанавливается совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и Роскомнадзором.

9.8. Для учета информации об инцидентах, предусмотренных частью 3.1 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ, Роскомнадзор ведет реестр учета инцидентов в области ПДн, определяет порядок и условия взаимодействия с Банком в рамках ведения указанного реестра.

9.9. Информация о компьютерных инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) ПДн, в порядке, установленном совместно федеральным органом исполнительной власти, уполномоченным в области

обеспечения безопасности, и Роскомнадзором, передается в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности.

10. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Сроки обработки и хранения персональных данных определяются целями их обработки, сроком действия договорных отношений с Субъектом ПДн (или юридическим лицом, представителем которого является Субъект ПДн), сроками, установленными в согласиях на обработку персональных данных, прекращением/изменением направления основной деятельности Банка, требованиями федеральных законов Российской Федерации, сроками исковой давности, а также правилами ведения архива Банка и в соответствии с Уведомлением об обработке персональных данных, направленным Банком в Роскомнадзор.

10.2. Хранение персональных данных осуществляется в форме, позволяющей определить Субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является Субъект персональных данных.

10.3. 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.

11. МЕРЫ, НАПРАВЛЕННЫЕ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОБЯЗАННОСТЕЙ БАНКА ПО ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. При обработке персональных данных Банк принимает необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом № 152-ФЗ или другими федеральными законами. К таким мерам, в частности, относятся:

1) назначение Банком ответственного за организацию обработки персональных данных;

2) издание Банком документов, определяющих Политику Банка в отношении обработки персональных данных, внутренних нормативных актов Банка по вопросам обработки ПДн, определяющих для каждой цели обработки ПДн категории и перечень обрабатываемых ПДн, категории Субъектов ПДн, ПДн 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. Такие документы и локальные акты не могут содержать положения, ограничивающие права Субъектов ПДн, а также возлагающие на Банк не предусмотренные законодательством Российской Федерации полномочия и обязанности;

3) ознакомление работников Банка, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе, с требованиями к защите персональных данных, с документами, определяющими

политику Банка в отношении обработки персональных данных, а также иными внутренними локальными документами Банка по вопросам обработки персональных данных и (или) обучение указанных работников;

4) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ, достигается, в частности:

5) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Банка в отношении обработки персональных данных, локальным актам Банка;

6) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом № 152-ФЗ;

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

11.2. 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, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

11.3. Обеспечение безопасности персональных данных, обрабатываемых в Банке, достигается, в частности, применением следующих мер по обеспечению выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ в области обработки персональных данных:

- ❒ определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- ❒ 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;
- ❒ применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- ❒ оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- ❒ учетом машинных носителей персональных данных;
- ❒ обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;
- ❒ восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- ❒ 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;
- ❒ контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

11.4. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных:

1) уровнем защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
2) требований к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
3) требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

11.5. В целях осуществления контроля соблюдения требований законодательства Российской Федерации и координации действий по обеспечению безопасности персональных данных Приказом Председателя Правления назначено лицо, ответственное за организацию обработки персональных данных в Банке.

11.6. В Банке осуществляется внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Банка в отношении обработки персональных данных, локальным актам в области обработки и обеспечения безопасности персональных данных.

11.7. Оценка вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав Субъектов ПДн, который может быть причинен Субъектам ПДн в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ.

11.8. Банк по запросу Роскомнадзора обязан представить документы и локальные акты, регулирующие осуществление им мероприятий, направленных на принятие мер, предусмотренных в пункте 11.3 настоящей Политики, и (или) иным образом подтвердить выполнение мер, указанных в пункте 11.3 настоящей Политики.

12. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕЙ ПОЛИТИКИ

12.1. Контроль исполнения требований настоящей Политики осуществляется Ответственным за организацию обработки персональных данных в Банке.

12.2. Лица, виновные в нарушении норм, регулирующих получение, обработку, хранение и защиту обрабатываемых в Банке персональных данных, несут ответственность, предусмотренную законодательством Российской Федерации.

13. ЛИСТ СОГЛАСОВАНИЯ

НАЗВАНИЕ:	Публичная политика по обработке и защите персональных данных в АКБ «Трансстройбанк» (АО)
ВЕРСИЯ:	5.25
ПОДРАЗДЕЛЕНИЕ – ОТВЕТСТВЕННЫЙ РАЗРАБОТЧИК:	Отдел информационной безопасности

Согласовано:

Должность	ФИО	Подпись	Дата
Заместитель Председателя Правления Банка	С. Ю. Фабрин		
Заместитель Председателя Правления Банка	Е. В. Морозова		
Начальник Управления информационных технологий	А. А. Евсеев		
Начальник Отдела информационной безопасности	Р. Г. Фалалеев		
Начальник Юридического упраления	О. Е. Калёнова		