Приложение № 1
к Приказу № 160 от 21 января 2025 г.

ПОЛИТИКА
в отношении обработки персональных данных
ЭКСИ-Банк (АО)

г. Санкт-Петербург

СОДЕРЖАНИЕ

1. Общие положения

1.1. Политика в отношении обработки персональных данных ЭКСИ-Банк (АО) (далее – Политика) определяет стратегию и принципы обработки персональных данных в ЭКСИ-Банк (АО).

1.2. Обработка персональных данных осуществляется в соответствии с положениями нормативно-правовых актов РФ:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Налогового кодекса Российской Федерации;
- Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 02 декабря 1990 г. № 395-1 «О банках и банковской деятельности»;
- Федерального закона от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях»;
- Федерального закона от 07 июля 2001 N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Приказа Росархива от 20.12.2019 №236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;
- Федерального закона от 06 апреля 2011 №63-ФЗ «Об электронной подписи»;
- Приказа Роскомнадзора от 05 сентября 2013 №996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- Федерального закона от 29 ноября 2010 №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» (Федеральный закон №326-ФЗ);
- Постановления Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства РФ от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- иных нормативно - правовых актов Российской Федерации в области защиты персональных данных.

1.5. Настоящая Политика направлена на:

- установление принципов обработки персональных данных;
- публикацию сведений о реализуемых требованиях к защите обрабатываемых Банком персональных данных;
- обеспечение защиты обрабатываемых Банком персональных данных;
- минимизацию рисков разглашения (распространения) персональных данных без согласия субъекта персональных данных;
- создание положительной репутации Банка;

– обеспечение конституционных прав субъектов персональных данных по сохранению Банком конфиденциальности персональных данных.

1.6. В Банке разрабатываются и поддерживаются в актуальном состоянии иные внутренние нормативные документы, определяющие порядок обработки, хранения, защиты и уничтожения персональных данных.

1.7. Соблюдение настоящей Политики является элементом корпоративной этики Банка. Лицо, ответственное за организацию обработки персональных данных обеспечивает повышение осведомленности персонала.

1.8. Политика обязательна для ознакомления и исполнения всеми лицами, допущенными к обработке персональных данных в Банке.

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

1.10. Настоящая Политика является общедоступным документом. Неограниченный доступ к настоящей Политике обеспечивается путем размещения Политики на информационных WEB-сайтах, принадлежащих Банку и его филиалам.

2. Термины и определения

2.1. В настоящей Политике информационной безопасности ЭКСИ-Банк (АО) используются следующие термины и определения:

Наименование термина или сокращение	Определение
Банк	ЭКСПОРТНО-ИМПОРТНЫЙ БАНК (АКЦИОНЕРНОЕ ОБЩЕСТВО), сокр. ЭКСИ-Банк (АО).
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)
Документ	материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения
Информация	сведения (сообщения, данные) независимо от формы их представления
Информационная система персональных данных (ИСПДн)	совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Оператор 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

Наименование термина или сокращение	Определение
	данных, подлежащих обработке, действия (операции), совершаемые с персональными данными
Обработка персональных данных	любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе: – сбор; – запись; – систематизацию; – накопление; – хранение; – уточнение (обновление, изменение); – извлечение; – использование; – передачу (распространение, предоставление, доступ); – обезличивание; – блокирование; – удаление; – уничтожение.
Обезличивание персональных данных	действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
Персональные данные (ПДн)	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
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, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом
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

Наименование термина или сокращение	Определение
Риск	мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.
РФ	Российская Федерация
СКЗИ	средства криптографической защиты информации.
НСД	несанкционированный доступ.

3. Правовые основания обработки персональных данных

3.1. Банк является оператором персональных данных, о чем имеется регистрационная запись в Реестре операторов, осуществляющих обработку персональных данных.

3.2. Обработка персональных данных осуществляется Банком по следующим основаниям:

- на основании согласия субъекта на обработку его персональных данных;
- обработка персональных данных 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 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;
- обработка персональных данных необходима для осуществления прав и законных интересов Банка или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- 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;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4. Принципы и условия обработки персональных данных

4.1. Обработка персональных данных осуществляется Банком в соответствии с требованиями Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятых в соответствии с ним иных нормативных правовых актов, регулирующих вопросы обработки и защиты персональных данных. При обработке персональных данных Банк как оператор придерживается принципов, установленных законодательством Российской Федерации в области защиты персональных данных.

4.2. В Банке определены следующие принципы обработки персональных данных:

- обработка персональных данных осуществляется на законной и справедливой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональных данных, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональных данных, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки и не являются избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивается их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки. Принимаются необходимые меры по удалению или уточнению неполных или неточных данных;
- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки, если срок хранения персональных данных не установлен федеральным законом или нормативным актом Банка России;
- обрабатываемые персональные данные по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом, подлежат уничтожению либо обезличиванию.

4.3. Обработка персональных данных осуществляется при наличии правовых оснований, указанных в п. 3.2 настоящей Политики.

4.4. Банк праве 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 - поручение оператора).

4.5. Если Банк поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Банк как оператор. Лицо, осуществляющее обработку персональных данных по поручению Банка как оператора, несет ответственность перед Банком.

4.6. Обработка персональных данных прекращается в случаях:

- достижения целей обработки персональных данных;
- истечения срока действия согласия;
- отзыв согласия субъекта персональных данных на обработку его персональных данных;
- выявление неправомерной обработки персональных данных.

5. Цели обработки персональных данных

5.1. Банк обрабатывает иную категорию[1] персональных данных.

5.2. Банк не обрабатывает персональные данные, относящиеся к категории биометрических персональных данных. В связи с чем установление целей обработки для категорий биометрических персональных данных не требуется.

5.3. В Банке установлены указанные ниже цели обработки в отношении общей категории персональных данных.

- в целях идентификации лиц, обратившихся в Банк для получения банковских услуг;
- осуществления банковских операций и сделок в соответствии с Уставом Банка и выданными Банку лицензиями на совершение банковских и иных операций, а также выполнение иных договоров гражданско-правового характера;
- соблюдения Банком действующего законодательства Российской Федерации и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей;
- 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;
- 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»;
- исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- исполнения условий трудовых договоров и договоров гражданско-правового характера, заключенных между Банком и работниками Банка, а также иными лицами;
- предоставления субъекту персональных данных с его согласия информации об оказываемых Банком услугах, о разработке новых продуктов и услуг;
- ведения бухгалтерского, налогового, управленческого, кадрового и воинского учета;
- формирования и предоставления в соответствующие органы необходимой статистической, бухгалтерской, налоговой, банковской и иной отчетности по установленным законодательством формам;
- ведения документооборота, информационного взаимодействия с органами государственной власти.

[1] Не входящие в следующие категории: общедоступные, специальные категории, биометрические персональные данные.

6. Категории обрабатываемых персональных данных

6.1. Банк обрабатывает персональные данные следующих категорий субъектов:

- физические лица, состоящие в договорных и иных гражданско-правовых отношениях с Банком;
- уволенные работники;
- субъекты персональных данных, предоставившие согласие на обработку персональных данных;
-
- физических лиц, являющихся пользователями web-сайтов Банка

6.2. Банк обрабатывает следующие персональные данные:

- фамилия, имя, отчество,
- год рождения, месяц рождения,
- дата рождения,
- место рождения,
- пол,
- адрес электронной *почты,*
- адрес места жительства,
- адрес регистрации,
- номер телефона,
- СНИЛС,
- ИНН,
- гражданство,
- данные документа, удостоверяющего личность,
- данные документа, удостоверяющего личность за пределами Российской Федерации,
- должность,
- отношение к воинской обязанности, сведения о воинском учете,
- сведения об образовании;
- сведения, указанные в актах гражданского состояния (рождение, заключение брака, расторжение брака, усыновление (удочерение), установление отцовства, перемена имени и смерть),
- отношение к государственной (муниципальной, военной) службе;
- данные разрешения на работу,
- сведения о доходах; сведения о налоговых и иных отчислениях;
- номер расчетного счета;
- номер банковской карты,
- сведения о повышении квалификации,
- сведения об аттестации,
- сведения о пройденных курсах и тестах;

- сведения о социальных льготах и о социальном статусе (сведения о документе, являющимся основанием для предоставления льгот и статуса);
- сведения из полиса обязательного (добровольного) медицинского страхования

6.3. В Банке внутренним документом «Перечень обрабатываемых персональных данных и цели обработки персональных данных в ЭКСИ-Банк (АО)» для каждой цели обработки персональных данных определены**:**

- категории и перечень обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- способы, сроки обработки и хранения персональных данных;
- порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований.

7. Порядок обработки персональных данных

7.1. Банк обрабатывает персональные данные с использованием и без использования средств автоматизации.

7.2. Обработка и хранение персональных данных с использованием средств автоматизации выполняется с использованием баз данных информационных систем персональных данных, при этом базы данных находятся на территории Российской Федерации.

7.3. Обработка персональных данных без использования средств автоматизации при непосредственном участии человека выполняется с использованием специальных стандартизированных форм (журналов, бланков). При этом обеспечивается выполнение требований Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

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

7.5. Хранение персональных данных, фиксируемых на специальных формах (журналах, бланках) обеспечивается с соблюдением требований конфиденциальности, не допуская возможности ознакомления с персональными данными неуполномоченных лиц.

7.6. Хранение и обработка персональных данных в информационных системах и базах данных обеспечивается с соблюдением требований конфиденциальности, требующей выполнения идентификации, аутентификации и авторизации при осуществлении доступа. Доступ работникам Банка к персональным данным, обрабатываемым в информационных системах, предоставляется в минимальном объеме, необходимом для выполнения ими должностных обязанностей.

7.7. Банк обрабатывает персональные данные с соблюдением требований к их актуальности, точности и правомерности. В случае выявления фактов неточности персональных данных производится их актуализация. В случае выявления неправомерной обработки персональных данных их обработка прекращается в установленный законодательством срок.

7.8. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если иное не предусмотрено:

- договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных;
- требованиями законодательства Российской Федерации;
- иным соглашением между Банком и субъектом персональных данных.

7.9. Согласно статье 6 часть Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных» допускается обработка персональных данных для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей. По требованиям Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» на Банк возложены обязанности по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения предупреждению, выявлению и пресечению деяний, связанных с легализацией (отмыванием) доходов, полученных преступным путем, финансированием терроризма и финансированием распространения оружия массового уничтожения. Статья 7 раздел 4 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» устанавливает требование «*Документы, содержащие сведения, указанные в настоящей статье, и сведения, необходимые для идентификации личности, подлежат хранению* ***не менее пяти лет****. Указанный срок исчисляется со дня прекращения отношений с клиентом*». В связи с чем обработка персональных данных клиентов в целях исполнения Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» может быть продолжена Банком в течение 5 лет после прекращения действия договора, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

7.10. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5.1 статьи 21 Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», 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 шесть месяцев, если иной срок не установлен федеральными законами.

8. Права субъекта персональных данных

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

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;

- наименование и место нахождения подразделений Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора 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;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка как оператора, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения Банком обязанностей по защите его персональных данных
- иные сведения, предусмотренные федеральными законами.

8.2. Сведения предоставляются субъекту персональных данных или его представителю Банком 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.

8.3. Запрос субъекта на получение информации, касающейся обработки его персональных данных 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 обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Банком, подпись субъекта персональных данных или его представителя.

8.4. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Банк предоставляет сведения субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

8.5. В случае, если сведения, указанные в п. 8.1, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно или направить ему повторный запрос в целях получения сведений, указанных в п. 8.1, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более

короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом.

8.6. Субъект персональных данных вправе обратиться повторно в Банк или направить ему повторный запрос в целях получения сведений, указанных в п 8.1, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в 8.5, 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 дополнительно к сведениям п. 8.3 должен содержать обоснование направления повторного запроса

8.7. Банк вправе отказать субъекту персональных данных в выполнении повторного запроса в случае, если запрос не соответствует условиям, указанным в п. 8.5 и 8.6. При этом Банк указывает причину отказа в выполнении повторного запроса.

8.8. Обработка персональных данных в целях продвижения банковских услуг на рынке путем осуществления прямых контактов с клиентами Банка с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных. Банк обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в указанных целях.

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

8.10. Банк обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

8.11. Банк обязан рассмотреть возражение субъекта персональных данных, указанное в п 8.10 в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

8.12. 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.

9. Трансграничная передача персональных данных

9.1. Банк осуществляет трансграничную передачу персональных данных.

9.2. Банк уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществить трансграничную передачу персональных данных.

9.3. До подачи уведомления о намерении осуществить трансграничную передачу персональных данных Банк выполняет оценку соблюдения органами власти иностранных государств, иностранными физическими лицами, иностранными юридическими лицами, которым планируется трансграничная передача персональных

данных, конфиденциальности персональных данных и обеспечения безопасности персональных данных при их обработке.

9.4. До подачи уведомления о намерении осуществить трансграничную передачу персональных данных Банк получает сведения о принимаемых органами власти иностранного государства, иностранными физическими лицами, иностранными юридическими лицами, которым планируется трансграничная передача персональных данных, мерах по защите передаваемых персональных данных и об условиях прекращения их обработки.

9.5. До подачи уведомления о намерении осуществить трансграничную передачу персональных данных Банк получает сведения о правовом регулировании в области персональных данных иностранного государства, под юрисдикцией которого находятся органы власти иностранного государства, иностранные физические лица, иностранные юридические лица, которым планируется трансграничная передача персональных данных.

9.6. До подачи уведомления о намерении осуществить трансграничную передачу персональных данных Банк получает сведения об органах власти иностранного государства, иностранных физических лицах, иностранных юридических лицах, которым планируется трансграничная передача персональных данных.

9.7. В случае, если трансграничная передача персональных данных осуществляется на территорию иностранных государств, перечня иностранных государств, не включенных в состав государств, обеспечивающих адекватную защиту прав субъектов персональных данных, трансграничная передача персональных данных осуществляется только после получения положительного решения уполномоченного органа по защите прав субъектов персональных данных.

10. Обязанности Банка как оператора персональных данных

10.1. Банк обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить 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 оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. При сборе персональных данных Банк обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную п. 8.1.

10.2. 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 Банк обязан дать в письменной форме мотивированный ответ с указанием основания для такого отказа, 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 оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

10.3. Банк обязан предоставить 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 или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Банк вносит в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Банк обязан уничтожить такие персональные данные.

10.4. Банк обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

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

10.6. Если персональные данные получены не от субъекта персональных данных, Банк до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки таких персональных данных и ее правовое основание;
- перечень персональных данных;
- предполагаемые пользователи персональных данных;
- права субъекта персональных данных;
- источник получения персональных данных.

10.7. Банк освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п 10.6, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных Банком как оператором;
- 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;
- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- Банк осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- предоставление субъекту персональных данных сведений, предусмотренных п 10.6, нарушает права и законные интересы третьих лиц.

10.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

10.9. Во исполнение обязанностей Банк принимает следующие меры:

- назначает ответственного за организацию обработки персональных данных;
- разрабатывает внутренние нормативные документы по вопросам обработки персональных данных, определяющие 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 внутренние нормативные документы, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, порядок устранения последствий таких нарушений. Такие документы и внутренние нормативные документы не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагать на Банк как оператор не предусмотренные законодательством Российской Федерации полномочия и обязанности;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с разделом 11 настоящей Политики;
- осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике в отношении обработки персональных данных, внутренним нормативным документам, касающихся обработки персональных данных;
- выполняет оценку вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных в случае нарушения Банком Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом РФ от 27.07.2006 г. № 152-ФЗ №152-ФЗ «О персональных данных»;
- ознакомляет работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о

персональных данных, в том числе требованиями к защите персональных данных, с настоящей Политикой в отношении обработки персональных данных, внутренними нормативными документами по вопросам обработки персональных данных, и (или) обеспечивает обучение указанных работников.

11. Меры по обеспечению безопасности персональных данных при их обработке

11.1. Банк при обработке персональных данных принимает необходимые правовые, организационные и технические меры и обеспечивает их выполнение 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.

11.2. Обеспечение безопасности персональных данных Банком достигается, в частности:

- 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
- 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.

11.3. Банк обеспечивает взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации посредством ФинЦЕРТ Банка России, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

12. Порядок контроля и пересмотра

12.1. Контроль осуществляется путем проведения текущего мониторинга информационной безопасности Банка, по результатам оценки выполнения требований по информационной безопасности, а также в рамках иных контрольных мероприятий.

12.2. Настоящая Политика утверждается приказом генерального директора.

12.3. Пересмотр Политики должен осуществляться на периодической и внеплановой основе.

12.4. На периодической основе настоящая Политика должна пересматриваться не реже одного раза в два года.

12.5. Все изменения в Политику вносятся на основе приказа генерального директора.