



Политика АКБ «Форштадт» (АО) в отношении обработки персональных данных физических лиц

Версия 1.**10**

УТВЕРЖДЕНО

Решением Правления
АКБ «Форштадт» (ЗАО)
от 22.03.2012 г. № 41

История документа

Дата	Версия	Статус	Комментарий
22.03.2012 г.	1.0	Финальная версия	Утверждено Решением Правления от 22.03.2012 г. № 41 (вступает в силу с 22.03.2012 г.)
10.10.2013 г.	1.1	Изменения в действующую редакцию	Решение Правления от 10.10.2013 г. № 151 (вступает в силу 15.10.2013 г.)
11.03.2014 г.	1.2	Изменения в действующую редакцию	Решение Правления от 11.03.2014 г. № 47 (вступает в силу 12.03.2014 г.)
24.11.2014 г.	1.3	Изменения в действующую редакцию	Решение Правления Банка от 24.11.2014 г. № 192 (вступает в силу с 24.11.2014 г.)
10.02.2016 г.	1.4	Изменения в действующую редакцию	Решение Правления Банка от 10.02.2016 г. № 2/10/2 (вступает в силу с 11.02.2016 г.)
04.12.2018 г.	1.5	Изменения в действующую редакцию	Решение Правления Банка от 04.12.2018 г. № 12/04/1
19.02.2019 г.	1.6	Изменения в действующую редакцию	Решение Правления Банка от 19.02.2019 г. № 2/19/1
30.12.2021 г.	1.7	Изменения в действующую редакцию	Решение Правления Банка от 21.12.2021 г. № 04020911019
01.09.2022 г.	1.8	Изменения в действующую редакцию	Решение Правления Банка от 01.12.2022 г. № 04020911112
20.01.2023 г.	1.9	Изменения в действующую редакцию	Решение Правления Банка от 20.01.2023 г. № 04020911005

Оглавление

1.	ОБЩИЕ ПОЛОЖЕНИЯ	4
2.	ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ	4
3.	ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ	5
4.	ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ	7
5.	ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА	9
6.	МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ	14
7.	ОЦЕНКА ВРЕДА ПРИ НАРУШЕНИИ ФЕДЕРАЛЬНОГО ЗАКОНА «О ПЕРСОНАЛЬНЫХ ДАННЫХ»	15
8.	ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ФЕДЕРАЛЬНОГО ЗАКОНА «О ПЕРСОНАЛЬНЫХ ДАННЫХ»	15
9.	ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	15

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящая Политика АKB «Форштадт» (АО) (далее – Оператор) в отношении обработки всех персональных данных (далее – Политика), которые могут быть получены от субъекта персональных данных (его представителя), являющегося стороной по гражданско-правовому договору с Оператором либо от субъекта персональных данных – представителя юридического лица, вступившего с Оператором в гражданско-правовые отношения (далее – Клиент), от субъекта персональных данных, состоящего с Оператором в отношениях, регулируемых трудовым законодательством (далее – Работника), от иного субъекта персональных данных, разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «О персональных данных», Федеральным законом «Об информации, информационных технологиях и о защите информации», внутренними нормативными документами Оператора.
- 1.2. Настоящая Политика определяет основные вопросы, связанные с обработкой персональных данных Оператором с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе, и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.
- 1.3. Оператор вправе проводить идентификацию клиента - физического лица, представителя клиента - юридического лица, имеющего право без доверенности действовать от имени юридического лица и являющегося физическим лицом, без личного присутствия в случаях, установленных федеральными законами, путем установления и подтверждения достоверности сведений о них, определенных Федеральным законом от 07.08.2001г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», с использованием единой системы идентификации и аутентификации и единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее – единая биометрическая система)).
- Внимание!** До особого распоряжения Оператор не проводит идентификацию гражданина Российской Федерации без его личного присутствия на основании сведений, размещенных в единой биометрической системе.
- 1.4. Настоящая Политика определяет принципы, порядок и условия обработки персональных данных Клиентов и Работников Оператора и иных лиц, чьи персональные данные обрабатываются Оператором, а также устанавливает меры по обеспечению безопасности при обработке персональных данных.
- 1.5. Целью настоящей Политики является защита интересов Оператора, его Клиентов и Работников, а также выполнения Законодательства Российской Федерации о Персональных данных.

2. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

- 2.1. Оператор осуществляет обработку персональных данных (в том числе биометрических) в следующих целях:
- осуществления банковских операций и иной деятельности, предусмотренной Уставом и лицензиями Оператора, нормативными актами Банка России, действующим законодательством Российской Федерации, в том числе без личного присутствия физического лица после проведения идентификации в порядке, предусмотренном п.1.3 настоящей Политики;
 - заключения, исполнения и прекращения гражданско-правовых договоров с физическими, юридическими лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных действующим законодательством Российской Федерации и Уставом Оператора;
 - организации кадрового учета Оператора, обеспечения соблюдения законов Российской Федерации и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым и

гражданско-правовым договорам; ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами, исполнения требований налогового законодательства Российской Федерации в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства Российской Федерации при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, Федеральными законами Российской Федерации, Уставом и внутренними документами Оператора;

- размещения или обновления в электронной форме при личном присутствии клиента - физического лица с его согласия и на безвозмездной для него основе:
 - ✓ сведений, необходимых для регистрации физического лица в единой системе идентификации и аутентификации, и иных сведений, если такие сведения предусмотрены федеральными законами, – в единой системе идентификации и аутентификации;
 - ✓ биометрических персональных данных физического лица – в единой биометрической системе.

3. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных Оператором осуществляется на основе принципов:

- законности и справедливости целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;
- уничтожения либо обезличивания по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

3.2. Обработка персональных данных допускается в следующих случаях:

- обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных настоящей Политикой;
- обработка персональных данных осуществляется с согласия субъекта персональных данных 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 Оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для исполнения Оператором функций по предоставлению государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 г. № 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 персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных.

- 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 Оператора 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 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 продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации), при условии обязательного обезличивания персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом Российской Федерации;
- обработка персональных данных объектов государственной охраны и членов их семей осуществляется с их согласия и (или) с согласия органов государственной охраны, за исключением персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами.

- 3.3. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом Российской Федерации.
- 3.4. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.
- 3.5. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.
- 3.6. Обработка специальных категорий персональных данных Оператором производится только в случаях, предусмотренных Федеральным законом «О персональных данных», а также в случаях и порядке, определяемом иными федеральными законами.
- 3.7. Обработка биометрических персональных данных, на основании которых можно определить субъекта персональных данных у Оператора может производиться только с согласия субъекта персональных данных.
- 3.8. Оператор вправе поручить обработку персональных данных третьему лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом на основании заключаемого с этим лицом договором. При этом Оператор в договоре обязует лицо, осуществляющее обработку персональных данных по поручению Оператора, соблюдать принципы и

правила обработки персональных данных, конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, установленные настоящей Политикой и Федеральным законом «О персональных данных».

- 3.9. В случае, если Оператор поручил обработку данных третьему лицу, ответственность перед субъектом персональных данных за действия этого лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором.
- 3.10. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Оператор обязан обеспечить 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, установленных законодательством Российской Федерации.
- 3.11. Оператор вправе осуществлять трансграничную передачу персональных данных на территорию иностранного государства, обеспечивающего адекватную защиту прав субъектов персональных данных.
До начала осуществления деятельности по трансграничной передаче персональных данных Оператор уведомляет орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных.
Трансграничная передача персональных данных на территории иностранных государств осуществляется в соответствии с Федеральным законом «О персональных данных» и международными договорами Российской Федерации.
- 3.12. Трансграничная передача персональных данных на территорию иностранного государства, не обеспечивающего адекватную защиту прав субъектов персональных данных, осуществляется в случае:
- наличия согласия в письменной форме субъекта персональных данных;
 - исполнение договора, стороной которого является субъект персональных данных;
 - в иных случаях, предусмотренных законодательством РФ.

4. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

- 4.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом Российской Федерации.

Форма согласия на обработку персональных данных и биометрических персональных данных в целях размещения в электронной форме сведений о физическом лице в единой системе идентификации и аутентификации, биометрических персональных данных физического лица – в единой биометрической системе, утверждается Правительством Российской Федерации.

- 4.2. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:
- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
 - фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
 - наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом Российской Федерации;
- подпись субъекта персональных данных.

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

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

4.5. Субъект персональных данных имеет право:

- 1) 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 Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона Российской Федерации;
 - обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом Российской Федерации;
 - сроки обработки персональных данных, в том числе сроки их хранения;
 - порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
 - информацию об осуществленной или о предполагаемой трансграничной передаче данных;
 - наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
 - информацию о способах исполнения Банком обязанностей, предусмотренных п. 5.2. настоящего Положения.

Сведения должны быть предоставлены субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Сведения предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его

представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

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 Оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положения Федерального закона «О персональных данных» или иного федерального закона Российской Федерации, являющееся основанием 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 5 (пять) рабочих дней в случае направления Оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Обязанность представления доказательств обоснованности отказа в выполнении запроса лежит на Операторе.

Если в соответствии с Федеральным законом «О персональных данных» предоставление персональных данных и (или) получение Банком согласия на обработку персональных данных является обязательными, то Банк обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами Российской Федерации.

- 2) требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством Российской Федерации меры по защите своих прав.
- 3) если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.
- 4) 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.

5. ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА

5.1. Оператор вправе:

- 1) отстаивать свои интересы в судебных органах;
- 2) предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством Российской Федерации (правоохранительные, налоговые органы и др.), а также связано с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- 3) отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством Российской Федерации;
- 4) использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством Российской Федерации;
- 5) после направления уведомления, указанного в пп.3.11 п.3 настоящей Политики, осуществлять трансграничную передачу персональных данных на территории указанных в уведомлении иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных или включенных в перечень¹, предусмотренный п.2 ст.12 Федерального закона «О персональных данных», до принятия

¹ Перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, утвержденный Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.08.2022г. № 128

решения, указанного п.8 ст.12 или п.12 ст.12 Федерального закона «О персональных данных» после направления уведомления, указанного в п.3 ст.12 Федерального закона «О персональных данных».

5.2. Обязанности Оператора:

- 1) Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом «О персональных данных» или другими федеральными законами Российской Федерации. К таким мерам могут, в частности, относиться:
 - назначение Оператором ответственного за организацию обработки персональных данных; Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа Оператора и подотчетно ему;
 - издание Оператором документов, определяющих политику Оператора в отношении обработки персональных данных, внутренних нормативных документов Оператора по вопросам обработки персональных данных, а также устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
 - применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
 - осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, внутренним нормативным документам Оператора;
 - оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
 - ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, внутренними нормативными документами Оператора по вопросам обработки персональных данных, и (или) обучение указанных работников.
- 2) Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.
- 3) Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать 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. Обеспечение безопасности персональных данных 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, 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.
- 4) в случае получения персональных данных не от субъекта персональных данных Оператор, за исключением случаев, предусмотренных законодательством Российской Федерации, 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 персональных данных и ее правовое основание;
 - предполагаемые пользователи персональных данных;
 - установленные Федеральным законом «О персональных данных» права субъекта персональных данных;
 - источник получения персональных данных.

Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные выше, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
 - персональные данные получены Оператором на основании федерального закона Российской Федерации или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
 - персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
 - Оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
 - предоставление субъекту персональных данных сведений, предусмотренных выше, нарушает права и законные интересы третьих лиц.
- 5) при использовании и хранении биометрических персональных данных вне информационных систем персональных данных Оператор обязан применять только такие материальные носители 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;
- при обработке, включая сбор и хранение, биометрических персональных данных Оператор применяет информационные технологии и технические средства, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации»;

Оператор обеспечивает проверку соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным согласно методикам, утвержденным в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» (информацию о результатах проверки соответствия Оператор получает от оператора единой биометрической системы).

- 6) Оператор 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, Оператор обязан внести 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, Оператор обязан уничтожить такие персональные данные.

Оператор 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.

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

- 7) 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 Оператор 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 Оператора) 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 Оператор 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) в случае подтверждения факта неточности персональных данных Оператор 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 семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

- 9) в случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий 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, Оператор в срок, не превышающий 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 Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

В случае установления факта неправомерной или случайной передачи персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор обязан с момента выявления такого инцидента уведомить уполномоченный орган по защите прав субъектов персональных данных:

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

10) в случае достижения цели обработки персональных данных Оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и 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 достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами Российской Федерации.

11) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор 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 десяти рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами Российской Федерации.

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

12) в случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пп. 8-10 п. 5.2 настоящей Политики, Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами Российской Федерации.

Подтверждение уничтожения персональных данных в случаях, предусмотренных п. 5.2 настоящей Политики, осуществляется в соответствии с Приказом Роскомнадзора от 28.10.2022г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

13) Оператор обязан до начала осуществления деятельности по трансграничной передаче персональных данных уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных. Указанное уведомление направляется отдельно от уведомления о намерении осуществлять обработку персональных данных, предусмотренного ст. 22 Федерального закона «О персональных данных».

14) Оператор до подачи уведомления, предусмотренного п.3 ст.12 Федерального закона «О персональных данных», запрашивает сведения у лиц/органов в соответствии со п.5 ст.12 Федерального закона «О персональных данных».

В целях оценки достоверности сведений, содержащихся в уведомлении Оператора о своем намерении осуществлять трансграничную передачу персональных данных, сведения, предусмотренные п.п. 1-3 ст. 12 Федерального закона «О персональных данных», предоставляются Оператором по запросу уполномоченного органа по защите прав субъектов персональных данных в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

15) В случае изменения сведений, указанных в п.3 ст. 22 Федерального закона «О персональных данных», Оператор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения, обязан уведомить уполномоченный орган по защите прав субъектов персональных данных обо всех произошедших за указанный период изменениях. В случае прекращения обработки персональных данных Оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты прекращения обработки персональных данных.

6. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. При обработке персональных данных Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а так же от иных неправомерных действий в отношении персональных данных.

6.2. Обеспечение безопасности персональных данных 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, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применение 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 по исключению такого в дальнейшем;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.3. При обеспечении защиты персональных данных Оператор руководствуется требованиями Законодательства Российской Федерации.

6.4. В качестве базовой модели угроз безопасности персональных данных Оператора принята «Частая модель угроз безопасности персональных данных».

7. ОЦЕНКА ВРЕДА ПРИ НАРУШЕНИИ ФЕДЕРАЛЬНОГО ЗАКОНА «О ПЕРСОНАЛЬНЫХ ДАННЫХ»².

7.1. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» (далее – оценка вреда), осуществляется Оператором в соответствии с Приказом Роскомнадзора от 28.10.2022г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

7.2. Оператор определяет высокую, среднюю или низкую степень вероятного вреда. Если субъекту персональных данных могут причинить вред разных степеней, учитывается более высокая из них. Результаты оценки степени вреда отражаются в акте оценки вреда субъектам персональных данных в связи с нарушением Федерального закона «О персональных данных».

8. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ФЕДЕРАЛЬНОГО ЗАКОНА «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

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

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

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Настоящая Политика является внутренним документом Оператора, является общедоступной и подлежит размещению на официальном сайте Оператора;

9.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов Российской Федерации и специальных нормативных документов по обработке и защите персональных данных;

9.3. Контроль исполнения требований настоящей Политики осуществляется ответственным за обеспечение безопасности персональных данных Оператора.

² Вступает в силу с 01.03.2023г. и действует до 01.03.2029г.