Приложение № 1
Приказу АО «Экспобанк»
от 12.11.2021 № Пр-01/21-444

Утверждена
Решением Правления
АО «Экспобанк»
(протокол от 09.11.2021)

Политика
в отношении обработки персональных данных
в АО «Экспобанк»

Москва 2021

Оглавление

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных в АО «Экспобанк» (далее – Политика) определяет политику АО «Экспобанк» в отношении обработки и обеспечения безопасности персональных данных.

1.2. Политика разработана в соответствии с законодательством Российской Федерации в области персональных данных.

1.3. Целью настоящей политики является установление основных принципов и подходов к Обработке и обеспечению безопасности персональных данных в Банке.

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

1.5. Политика обязательна для ознакомления и исполнения всеми лицами, допущенными к обработке персональных данных в информационной системе персональных данных.

1.6. Банк включен в реестр операторов, осуществляющих обработку персональных данных.

1.7. Пересмотр и обновление настоящей Политики осуществляется в связи с изменениями законодательства Российской Федерации в области персональных данных, по результатам анализа актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, а также по результатам других контрольных мероприятий.

1.8. Текущая редакция Политики размещается на сайте Банка в общем доступе и вступает в силу с момента утверждения Правлением, если иное не будет предусмотрено новой редакцией Политики.

2. Перечень нормативных документов

- Трудовой кодекс Российской Федерации;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях Обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их Обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их Обработке в информационных системах персональных данных»;
- Приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- иные нормативные правовые акты Российской Федерации и нормативные документы исполнительных органов государственной власти.

3. Термины и определения

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

Банк – АО «Экспобанк», являющийся в рамках Федерального закона «О персональных данных» оператором по обработке персональных данных, а именно: организующий (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;

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

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

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

Обработка Персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Ответственный за организацию обработки персональных данных – сотрудник Банка, который назначается организационно-распорядительным документом по Банку, организующий принятие правовых, организационных и технических мер в целях обеспечения надлежащего выполнения функций по организации обработки персональных данных в Банке в соответствии с требованиями законодательства Российской Федерации в области персональных данных;

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

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

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

Субъект персональных данных – 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;

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.

4. Цели обработки персональных данных

4.1. Банк осуществляет Обработку Персональных данных в целях:

- осуществления банковских операций и сделок в соответствии с Уставом Банка, выданными Банку лицензиями на совершение банковских и иных операций, в соответствии с действующим законодательством Российской Федерации;
- заключения с Субъектом персональных данных любых договоров и их дальнейшего исполнения;
- предоставления Субъекту персональных данных информации об оказываемых Банком услугах, о разработке Банком новых продуктов и услуг;

- организации кадрового учета работников Банка, содействия работникам в обучении, пользовании различного вида льготами в соответствии с законодательством Российской Федерации;
- привлечения и отбора кандидатов на работу в Банке;
- формирования статистической отчетности, в том числе для предоставления Банку России;
- осуществления Банком административно-хозяйственной деятельности;
- осуществления Обработки биометрических Персональных данных (данных изображения лица, полученных с помощью фото- и видеоустройств, данных голоса, полученных с помощью звукозаписывающих устройств) с целью их передачи в единую биометрическую систему;
- проверки биометрических Персональных данных и передачи информации о степени их соответствия предоставленным биометрическим Персональным данным государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в единой биометрической системе;
- выявления случаев мошенничества, хищения денежных средств со счетов клиентов Банка, иных противоправных действий, предотвращения таких противоправных действий в дальнейшем и локализации последствий таких действий.

4.2. Обработка Персональных данных также осуществляется для достижения целей, предусмотренных международными договорами Российской Федерации или законами, для осуществления и выполнения, возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей.

5. Категории субъектов персональных данных

5.1. Банк осуществляет обработку следующих категорий Субъектов Персональных данных:

- физические лица, заключившие с Банком гражданско-правовые договоры на оказание услуг Банку;
- потенциальные клиенты - физические лица, индивидуальные предприниматели (физические лица, зарегистрированные в установленном порядке и осуществляющие предпринимательскую деятельность без образования юридического лица), физические лица, занимающиеся в установленном законодательством Российской Федерации порядке частной практикой, оформлявших согласие на Обработку персональных данных для получения продукта\услуги или заключения иного договора, но не заключивших соответствующие договоры, а также физические лица - выгодоприобретатели, бенефициарные владельцы, представители таких клиентов ;
- бывшие клиенты - физические лица, индивидуальные предприниматели (физические лица, зарегистрированные в установленном порядке и осуществляющие предпринимательскую деятельность без образования юридического лица), физические лица, занимающиеся в установленном законодательством Российской Федерации порядке частной практикой, которые ранее имели договорные отношения с Банком, а также физические лица - выгодоприобретатели, бенефициарные владельцы, представители таких клиентов;
- клиенты других юридических лиц, Обработка Персональных данных для которых осуществляется по поручению указанных юридических лиц в соответствии с законодательством Российской Федерации;
- работники Банка, в том числе уволенные работники, близкие родственники/члени семьи работников Банка;
- кандидат на вакантные должности в Банке, практиканты;

- работники партнеров Банка, субподрядчиков, поставщиков и других юридических лиц, имеющих договорные отношения с Банком, с которыми взаимодействуют работники Банка в рамках своей деятельности;
- пользователи сайта Банка;
- иные Субъекты персональных данных, вступившие или намеревающиеся вступить в договорные отношения с Банком;
- иные Субъекты персональных данных, обращающиеся в Банк (при необходимости Обработки их персональных данных для целей выполнения их запросов).

6. Перечень Персональных данных, обрабатываемых в Банке

6.1. Перечень Персональных данных, обрабатываемых в Банке, определяется в соответствии с законодательством Российской Федерации и внутренними нормативными и распорядительными документами Банка с учетом целей Обработки Персональных данных, указанных в разделе 5 настоящей Политики.

6.2. Обработка специальных категорий Персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни субъекта Персональных данных в Банке не осуществляется.

7. Основные принципы Обработки Персональных данных

7.1. Обработка Персональных данных Банком осуществляется на основе принципов:
- законности 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;
- точности и достаточности, а в необходимых случаях и актуальности Персональных данных по отношению к заявленным целям их обработки;
- уничтожения Персональных данных по достижении целей обработки способом, исключающим возможность их восстановления;
- недопустимости объединения баз данных, содержащих Персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

7.2. Работники Банка, допущенные к Обработке Персональных данных, обязаны:

7.2.1. Знать и неукоснительно выполнять требования:
- законодательства Российской Федерации в области Персональных данных;
- настоящей Политики;
- внутренних нормативных и распорядительных документов Банка по вопросам Обработки Персональных данных и обеспечения безопасности Персональных данных;

7.2.2. Обрабатывать Персональные данные только в рамках выполнения своих должностных обязанностей.

7.2.3. Не разглашать Персональные данные, обрабатываемые в Банке.

7.2.4. Сообщать о действиях других лиц, которые могут привести к нарушению положений настоящей Политики.

7.2.5. Сообщать об известных фактах нарушения требований настоящей Политики ответственному за организацию Обработки Персональных данных в Банке.

7.3. 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.

8. Организация Обработки Персональных данных

8.1. Банк осуществляет Обработку персональных данных как с использованием средств автоматизации, так и без использования средств автоматизации.
8.2. 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.
8.3. Банк вправе поручить Обработку Персональных данных другому лицу с согласия субъекта Персональных данных, если иное не предусмотрено законодательством Российской Федерации, на основании заключаемого с этим лицом договора, обязательным условием которого является соблюдение этим лицом принципов и правил Обработки Персональных данных, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».
8.4. Персональные данные не раскрываются третьим лицам и не распространяются иным образом без согласия субъекта Персональных данных, если иное не предусмотрено законодательством Российской Федерации.
8.5. 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.
8.6. Обработка Персональных данных в Банке осуществляется с согласия субъекта Персональных данных кроме случаев, установленных законодательством Российской Федерации.
8.7. В ходе своей деятельности Банк может осуществлять трансграничную передачу Персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

9. Права субъекта персональных данных

9.1. 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 законодательства РФ;
- состав Персональных данных, относящиеся к соответствующему субъекту Персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральными законами;
- сроки Обработки Персональных данных, в том числе сроки их хранения;
- порядок осуществления Субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче Персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего Обработку Персональных данных по поручению Банка, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

9.2. Право Субъекта персональных данных на получение информации, касающейся Обработки его Персональных данных, может быть ограничено в случаях, установленных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

9.3. 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 от 27.07.2006 № 152-ФЗ «О персональных данных».
9.4. Субъект персональных данных имеет также иные права, установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

10.Обязанности Банка

10.1. В случаях, установленных законодательством Российской Федерации в области Персональных данных, Банк обязан предоставить субъекту Персональных данных или его представителю при обращении либо при получении запроса от субъекта Персональных данных или его представителя информацию, предусмотренную п. 9.1 настоящей Политики.
10.2. Банк при сборе Персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение Персональных данных с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».
10.3. Банк несет иные обязанности, установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

11. Меры, направленные на обеспечение выполнения обязанностей Банка по обработке и защите персональных данных

11.1. Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.
11.2. В Банке принимаются следующие меры по обеспечению выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в области Обработки Персональных данных:

- назначается Ответственный за организацию обработки персональных данных;
- утверждаются внутренние нормативные документы в отношении Обработки Персональных данных, по вопросам Обработки Персональных данных, а также документы, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, устранение последствий таких нарушений;
- применяются правовые, организационные и технические меры по обеспечению безопасности Персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- осуществляется внутренний контроль и (или) аудит соответствия Обработки Персональных данных в Банке Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним внутренним нормативным и организационным документам, требованиям к защите Персональных данных, политике Банка в отношении Обработки Персональных данных, внутренним нормативным и организационным документам в области обработки и обеспечения безопасности Персональных данных;
- осуществляется ознакомление работников Банка, непосредственно осуществляющих Обработку Персональных данных, с положениями законодательства Российской Федерации о Персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Банка в отношении Обработки Персональных данных, внутренним нормативным и организационным

документам Банка по вопросам Обработки Персональных данных, и (или) обучение указанных работников.

11.3. С целью обеспечения безопасности Персональных данных при их обработке, Банк принимает необходимые и достаточные правовые, организационные и технические меры для защиты Персональных данных от неправомерного и случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения Персональных данных, а также от иных неправомерных действий в отношении Персональных данных, в частности:

- определяются угрозы безопасности Персональных данных при их обработке в информационных системах персональных данных;
- применяются организационные и технические меры по обеспечению безопасности Персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите Персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности Персональных данных;
- применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;
- осуществляется оценка эффективности принимаемых мер по обеспечению безопасности Персональных данных до ввода в эксплуатацию и информационной системы Персональных данных;
- осуществляется учет машинных носителей Персональных данных;
- проводятся мероприятия по обнаружению фактов несанкционированного доступа к Персональным данным и принятию соответствующих мер;
- обеспечивается возможность восстановления Персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- устанавливаются правила доступа к Персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивается регистрация и учет действий, совершаемых с Персональными данными в информационной системе персональных данных;
- осуществляется контроль за принимаемыми мерами по обеспечению безопасности Персональных данных и уровня защищенности информационных систем персональных данных.

12. Ответственность

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

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

12.3. Политика является общедоступной и подлежит размещению на официальном сайте Банка или иным образом обеспечивается неограниченный доступ к настоящему документу.