ЭКСПОРТНО-ИМПОРТНЫЙ БАНК (АКЦИОНЕРНОЕ ОБЩЕСТВО)
г. Санкт-Петербург

ПОЛОЖЕНИЕ
по обработке и обеспечению безопасности персональных данных в ЭКСИ-Банк (АО)

1. Общие положения

1.1. Настоящее Положение ЭКСИ-Банк (АО) по обработке и обеспечению безопасности персональных данных (далее – Положение) устанавливает политику и общие подходы к обработке персональных данных физических лиц в ЭКСИ-Банк (АО) (далее – Банк), определяет цели и правовое основание обработки персональных данных, а также категории персональных данных, обрабатываемых в Банке.

1.2. Положение разработано в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - № 152-ФЗ), а также учитывает требования:

- Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждено постановлением Правительства РФ от 15.09.2008 № 687);
- Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства РФ от 01.11.2012 №1119);
- Приказ ФСТЭК от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Роскомнадзора от 30.05.2017 N 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения».

1.3. Настоящее Положение регламентирует следующие вопросы:

- порядок обработки персональных данных в Банке;
- организацию приема и обработки обращений и запросов субъектов персональных данных;
- перечень мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в сфере обработки персональных данных, устранение последствий таких нарушений;
- порядок ознакомления работников Банка с законодательством и внутренними документами о персональных данных;
- порядок формирования и направления уведомлений об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных;
- перечень правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- порядок осуществления внутреннего контроля за соблюдением Банком и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

1.4. В целях обеспечения выполнения Банком обязанностей, предусмотренных законодательством РФ о персональных данных, в Банке назначается Ответственный по персональным данным.

1.5. Термины, используемые в настоящем Положении:

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

оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с Персональных данных. Банк является оператором;

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.

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в ИС персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

информационная система персональных данных (ИС персональных данных) - совокупность содержащихся в базах, данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

субъект персональных данных - физическое лицо, чьи персональные данные Банк обрабатывает, предполагает обрабатывать в будущем или ранее обрабатывал.

конфиденциальность персональных данных - обязательное для соблюдения Банком или иным лицом, получившим доступ к Персональных данных требование, не раскрывать третьим лицам и не допускать их распространения без согласия субъекта Персональных данных или наличия иного законного основания.

1.6. Права и обязанности Банка и субъекта персональных данных.

1.6.1. Банк вправе:

- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено требованиями действующего законодательства (налоговые, правоохранительные органы и др.);

- отказывать в предоставлении персональных данных субъекту персональных данных в случаях, предусмотренных законодательством;

- производить обработку персональных данных субъекта без его согласия в случаях, предусмотренных законодательством.

- защищать свои права и законные интересы в судебном порядке.

1.6.2. Банк обязан:

- производить обработку персональных данных при наличии правовых оснований;

- принимать меры по обеспечению конфиденциальности и безопасности персональных данных;

- обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных;

- сообщать 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;

- предоставлять ответы на запросы субъектов персональных данных;

- принимать меры по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных в случае их выявления.

- выполнять иные предусмотренные законодательством Российской Федерации обязанности.

1.6.3. Субъект персональных данных обладает правами, предусмотренными законодательством, в том числе:

1.6.3.1. Получать информацию, касающуюся обработки его персональных данных, включая:

- подтверждение факта обработки персональных данных Банком;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Банком способы обработки персональных данных;
- наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных федеральными законами;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные федеральными законами.

1.6.3.2. требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

1.6.3.3. обжаловать в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;

1.6.3.4. защищать свои права и законные интересы, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

1.6.4. При обращении в Банк с запросом о предоставлении информации, касающейся обработки его персональных данных, Субъект персональных данных обязан, указывать в запросе 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. Запрос должен содержать подписывать запрос субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

2. Цели сбора персональных данных

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

2.2. Объем, характер обрабатываемых персональных данных, способы обработки персональных данных в Банке соответствуют заявленным целям обработки персональных данных.

2.3. Цели обработки персональных данных в Банке определяются на основании, анализа правовых актов, регламентирующих деятельность Банка, целей фактически осуществляемой Банком деятельности, а также деятельности, которая предусмотрена учредительными документами Банка, и конкретных бизнес-процессов Банка в конкретных ИС персональных данных.

2.4. Обработка Персональных данных в Банке осуществляется в целях:

- осуществления банковской деятельности, в соответствие с требованиями - Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»;
- оказания клиентам полного комплекса банковских услуг;
- обязательного раскрытия информации на рынке ценных бумаг;
- раскрытия информации для целей соблюдения антимонопольного законодательства,
- соблюдения требований законодательства при выпуске и обращении ценных бумаг;
- осуществления прав владельцев ценных бумаг, выпущенных (выданных) Банком и иными лицами;
- соблюдения требований законодательства о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма;
- соблюдения требований налогового законодательства;

- соблюдение требований трудового законодательства;
- осуществления исполнительного производства,
- соблюдения банковской тайны;
- осуществления финансово-хозяйственной деятельности Банка;
- рекламы услуг Банка;
- соблюдения требований иных нормативных правовых актов Российской Федерации;

3. Правовые основания обработки персональных данных

3.1. Персональные данные в Банке обрабатываются на основании:

- Федеральных законов, в том числе Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»; Федерального закона от 02.12.1990 г. №395-1 «О банках и банковской деятельности»; Федерального закона от 07.08.2001 г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Федерального закона от 30.12.2004 г. №218-ФЗ «О кредитных историях»; Федерального закона от 22.04.1996 года №39-ФЗ «О рынке ценных бумаг», от 23.12.2003 года №177-ФЗ «О страховании вкладов физических лиц в банках РФ»; а также Трудового кодекса РФ; Гражданского кодекса РФ, Налогового кодекса РФ, и иных нормативных правовых актов государственных органов, Банка России, органов местного самоуправления, принятых на основании и во исполнение федеральных законов;
- настоящего Положения, иных внутренних документов Банка;
- Устава Банка;
- Договоров, заключаемых между Банком и субъектами персональных данных.
- Согласия на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям Банка).

4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

4.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.2. В Банке обрабатываются персональные данные, принадлежащие следующим категориям субъектов персональных данных:

4.2.1. клиентам/контрагентам Банка (представителям клиентов/контрагентов Банка),
4.2.2. работникам Банка,
4.2.3. кандидатам на вакантные должности в Банке,
4.2.4. владельцам ценных бумаг, выпущенных (выданных) Банком,
4.2.5. членам и кандидатам в члены органов управления и контроля Банка,
4.2.6. единоличному исполнительному органу Банка,
4.2.7. аффилированным лицам Банка,
4.2.8. лицам, являющимся владельцами и/или состоящим в органах управления юридических лиц - владельцев именных ценных бумаг Банка (в случаях, предусмотренных законодательством),

4.2.9. лицам, у которых может быть заинтересованность в совершении Банком сделок, согласно ст. 81 ФЗ от 26.12.1995 №208-ФЗ «Об акционерных обществах»,
4.2.10. руководителям, работникам, участникам (акционерам, товарищам, пайщикам) контрагентов (потенциальных контрагентов) Банка, юридических лиц - клиентов (потенциальных клиентов) Банка.
4.2.11. выгодоприобретателям, распорядителям, бенефициарным владельцам, поручителям.
4.3. В Банке обрабатываются следующие категории персональных данных: фамилия, имя, отчество; год рождения; дата и место рождения; адрес; семейное положение; имущественное положение; образование; профессия; доходы.

4.4. Другие категории персональных данных: кредитная история физических лиц; ИНН, СНИЛС, гражданство, данные документов, удостоверяющих личность, данные миграционных карт, данные документов, подтверждающих право пребывания на территории РФ, номера телефонов, факсов, адреса электронной почты, должность, место работы, адрес места работы, сведения о наличии (отсутствии) судимости субъектов персональных данных для случаев, прямо предусмотренных федеральными законами, данные о воинской обязанности и иные категории в соответствии с требованиями действующего законодательства.

4.5. В Банке запрещена обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

4.6. Обработка данных о состоянии здоровья допускается только в отношении персональных данных работников и кандидатов на работу в подразделения Банка в целях исполнения двусторонних договоров, регулирующих трудовые отношения Банка и его работника, а также в целях исполнения действующего трудового законодательства.

5. Порядок и условия обработки персональных данных

5.1. Обработка персональных данных в Банке осуществляется следующими способами: сбор; запись; систематизацию; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; передачу (предоставление, доступ); обезличивание; блокирование; удаление; уничтожение.

5.2. В случае необходимости взаимодействия с третьими лицами в рамках достижения целей обработки персональных данных указываются условия передачи персональных данных в адрес третьих лиц (например, наличие договора поручения на обработку персональных данных. Поручение содержит цели осуществляемой передачи, объем передаваемых персональных данных, перечень действий по их обработке, способы и иные условия обработки, включая требования к защите обрабатываемых персональных данных.)

5.3. Трансграничная передача персональных данных осуществляется в соответствии с условиями предоставления услуг и соблюдением требований законодательства.

5.4. Сроки обработки персональных данных определяются в соответствии со сроком действия договора с субъектом персональных данных, приказом Минкультуры РФ от 25 августа 2010 года № 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», сроком исковой

давности, а также иными требованиями законодательства РФ и нормативными документами Банка России.

5.5. Персональных данных являются конфиденциальной информацией, Банком строго соблюдаются требования конфиденциальности персональных данных, установленные ст. 7 Федерального закона «О персональных данных», а также принимаются меры по обеспечению безопасности персональных данных при их обработке, предусмотренные ч. 2 ст. 18.1, ч. 1 ст. 19 Федерального закона «О персональных данных», требованиями и рекомендациями по обеспечению безопасности персональных данных, предъявляемых Федеральной службой безопасности РФ, Федеральной службой по техническому и экспортному контролю РФ.

5.6. Банк вправе поручить обработку персональных данных другому лицу с согласия субъекта Персональных данных, если иное не предусмотрено Федеральным законом, на основании заключаемого с этим лицом договора, (далее - поручение оператора). Лицо, осуществляющее обработку прсональных данных по поручению Банка, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством. В поручении Банка должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 №152-ФЗ.

5.7. В Банке применяются следующие меры по обеспечению безопасности персональных данных:

5.7.1. технические меры:

- средства защиты от несанкционированного доступа (как встроенные в прикладное и системное программное обеспечение, так и дополнительные средства);
- антивирусное программное обеспечение;
- средства разграничения доступа к информационным ресурсам;
- межсетевые экраны;
- система обнаружения вторжений;
- средства обнаружения уязвимостей;
- система контроля почтового и веб-трафика.

2. организационные меры:

- определение уровней защищенности персональных данных при их обработке в ИС персональных данных;
- определение угроз безопасности персональных данных при их обработке в ИС персональных данных;
- назначение ответственных за обеспечение безопасности персональных данных и ответственного за организацию обработки персональных данных;
- учет лиц, допущенных к обработке персональных данных;
- получение согласия субъекта персональных данных на обработку его персональных данных, а также передачу персональных данных третьим лицам;
- утверждение внутренних документов, регламентирующих порядок получения и обработки персональных данных субъектов персональных данных;

- возложение на контрагентов обязанности соблюдения конфиденциальности и безопасности при обработке передаваемых им персональных данных;
- возложение на работников Банка, имеющих доступ к персональных данных, ответственности за соблюдение требований законодательства РФ и внутренних документов Банка в части, касающейся неразглашения конфиденциальной информации третьим лицам; - внутренний контроль и аудит соответствия обработки Персональных данных требованиям N-152-ФЗ и других нормативно-правовых актов;
- публикация политики в отношении обработки и защиты персональных данных на сайте Банка.

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

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

5.10. Обработка персональных данных осуществляется Банком с использованием баз данных находящихся на территории Российской федерации, в соответствие с требованиями ч.5 ст.18 № 152-ФЗ.

5.11. При обработке документов на бумажном носителе, содержащих сведения о субъектах персональных данных Банком соблюдаются требования, установленные Постановлением Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5.12. Банком соблюдаются условия хранения персональных данных, в том числе, при обработке персональных данных без использования средств автоматизации, а именно, определены места хранения, обеспечены условия, обеспечивающие сохранность Персональных данных и исключающие несанкционированный к ним доступ.

5.13. Работники Банка, осуществляющие обработку персональных данных, несут ответственность за исполнение требований законодательства, настоящего Положения и иных внутренних документов Банка, разработанных в развитие и дополнение настоящего Положения, при осуществлении конкретных видов банковской деятельности, связанных с обработкой персональных данных.

6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным.

6.1. В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональных данных подлежат их актуализации Банком, а обработка должна быть прекращена.

6.2. При достижении целей обработки персональных данных, а также в случае отзыва субъектом Персональных данных согласия на их обработку персональных данных подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- Банк не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных № 152-ФЗ или иными федеральными законами;
- иное не предусмотрено иным соглашением между Банком и субъектом персональных данных.

6.3. Банк обязан предоставить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу.

6.4. Порядок направления субъектом персональных данных таких запросов определен требованиями статьи 14 Федерального закона №152-ФЗ. Запрос субъекта Персональных данных должен содержать следующую информацию:

- серию, номер документа, удостоверяющего личность субъекта персональных данных, 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, и/или иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Банком;
- подпись субъекта персональных данных.

6.5. Обращение субъекта персональных данных по вопросам, связанным с обработкой персональных данных, оформленное в свободной форме может быть направлено Почтой России, на электронный адрес Банка в форме электронного документа, подписанного электронной подписью в соответствии с законодательством Российской Федерации, или представлено непосредственно в Банк.