

УТВЕРЖДАЮ

Председатель Правления

АКБ «Энергобанк» (ОАО)

Приказ № 116 от «27» июля 2011г.



/ Вагизов Д.И.

О персональных данных, порядке их обработки и обеспечения безопасности в АКБ «Энергобанк» (ОАО)

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом №152-ФЗ от 27.07.2006 г. «О персональных данных», требованиями стандартов Банка России, иными законодательными и нормативными актами, регулирующими обработку и защиту персональных данных.

1.2. Настоящее Положение определяет принципы и порядок работы подразделений АКБ «Энергобанк» (ОАО) (далее – Банк) с персональными данными.

1.3. Под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.4. Банк осуществляет обработку персональных данных в ходе выполнения функций кредитной организации, работодателя, профессионального участника рынка ценных бумаг.

1.5. Банк, как оператор персональных данных, самостоятельно определяет должностных лиц, имеющих доступ к обработке персональных данных в целях разграничения доступа к персональным данным.

1.6. Сотрудники Банка, в соответствии со своими полномочиями владеющие персональными данными, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

1.7. Банк учитывает требования настоящего Положения при разработке и утверждении типовой документации, затрагивающей сферу обработки персональных данных.

1.8. Сотрудники Банка, осуществляющие операции с персональными данными, обязаны знать и применять нормы настоящего Положения.

1.9. Ответственность за обеспечение норм законодательства и настоящего Положения при обработке персональных данных возлагается на руководителей подразделений, осуществляющих обработку персональных данных.

1.10. Текущий контроль над выполнением норм настоящего Положения возлагается на назначаемого Приказом по Банку сотрудника, ответственного за организацию обработки персональных данных. К функциям указанного сотрудника относятся:

- осуществление внутреннего контроля над соблюдением Банком и его сотрудниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- организация процедуры доведения до сведения работников Банка положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- осуществление контроля над приемом и обработкой обращений и запросов субъектов персональных данных.

2. Принципы работы с персональными данными

2.1. Принцип добровольности предоставления.

2.1.1. Банк признаётся обладателем персональных данных по причине добровольного и самостоятельного предоставления персональных данных самими субъектами персональных данных либо их доверенными лицами. Банк не вправе заставлять субъектов персональных данных к предоставлению таковых, однако вправе требовать этого, если подобные обязательства прямо вытекают из договорных отношений с субъектами персональных данных или требований нормативных и законодательных актов или является условием предоставления банковской услуги. Персональные данные могут быть получены Банком от лица, не являющегося субъектом персональных данных в установленных законом случаях (пункт 2 - 11 части 1 статьи 6, часть 2 статьи 10 и часть 2 статьи 11 Федерального закона «О персональных данных».

2.1.2. Субъект персональных данных может в любой момент отозвать своё согласие на предоставление персональных данных, при условии, что подобная процедура не нарушает требований законодательства РФ и допускается условиями договора, сторонами по которому являются субъект персональных данных и Банк.

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 пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона «О персональных данных».

2.2. Принцип информированности субъекта персональных данных.

2.2.1. Банк обязан обеспечивать субъекту персональных данных возможность ознакомления в доступной форме с документами и материалами, непосредственно к нему относящимися (если запрет прямо не установлен действующим законодательством) при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

Персональные данные субъекта также могут быть предоставлены его законному представителю в рамках полномочий данного законного представителя.

2.2.2. При сборе персональных данных, по просьбе субъекта персональных данных, сотрудники Банка, осуществляющие сбор персональных данных обязаны предоставить ему следующую информацию:

- правовые основания и цели обработки персональных данных;
- цели и применяемые Банком способы обработки персональных данных;
- наименование и место нахождения Банка;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- иные сведения, предусмотренные действующим законодательством.

2.2.3. Сотрудники Банка, осуществляющие сбор персональных данных обязаны разъяснить субъекту персональных данных юридические последствия отказа предоставить персональные данные.

2.3. Принцип необходимости и добросовестности.

2.3.1. Банк осуществляет обработку персональных данных исключительно в целях соблюдения законодательных и нормативных актов, минимизации банковских рисков (включая сохранность ресурсов Банка), зависящих от персональных характеристик клиента/сотрудника.

2.3.2. Запрещается получать, обрабатывать и приобщать к делам персональные данные о политических, религиозных и иных убеждениях клиента/сотрудника, иные персональные данные не соответствующие целям деятельности Банка.

2.3.3. Данные о здоровье обрабатываются Банком только в том случае, если эти данные прямо относятся к трудовым отношениям, возможности клиента исполнять свои обязательства перед Банком, либо используются в целях исполнения требований социального законодательства.

2.3.4. Недопустимо фиксирование в рамках одного документа персональных данных, обработка которых преследует заведомо несовместимые цели.

2.3.5. Излишне полученные персональные данные, не соответствующие заявленным при получении персональных данных целям, подлежат, по возможности, уничтожению, специальная обработка подобных данных недопустима.

2.5. Принцип защищённости.

2.5.1. Банк несёт ответственность за распространение персональных данных и обязан обеспечивать их защиту. Любые случаи неправомерного разглашения (вероятность разглашения) персональных данных лицом, осуществляющим обработку персональных данных, должны являться предметом служебного расследования. Аналогичному расследованию подлежат случаи нарушения организационного, технического и технологического порядка обработки персональных данных.

Ответственность за общую организацию процесса обеспечения безопасности персональных данных возлагается на Отдел обеспечения информационной безопасности.

2.5.2. Передача персональных данных в распоряжение третьей стороне (включая надзорные органы) возможна только в случаях, прямо предусмотренных законодательными и нормативными актами, либо в случае прямого согласия субъекта персональных данных.

2.5.4. Базы данных, являющихся хранилищем персональных данных, созданные для исполнения конкретной декларируемой Банком цели, запрещается объединять с базами данных, созданными для исполнения иной, несовместимой с первой, цели.

2.5.5. Хранение персональных данных, получение которых осуществляется на основании законодательных и нормативных актов, осуществляется в нормативно утверждённой форме в соответствии с законодательно утверждёнными сроками. Прочие персональные данные подлежат на бумажном носителе хранению в сроки, указанные в утверждённой Банком Номенклатуре дел, но не менее 5 лет по истечении срока действия договора, при условии, что все обязательства, вытекающие из договора, прекращаются с истечением срока действия договора или при расторжении договора.

2.6. Принцип согласия субъекта.

2.6.1. Персональные данные должны обрабатываться только с согласия субъектов персональных данных. Указанные согласия не требуется, если обработка этих данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных, а также в силу иных требований законодательства.

2.6.3. При недееспособности субъекта персональных данных письменное согласие на обработку его данных дает его законный представитель. В случае смерти субъекта персональных данных такое согласие оформляют его наследники, если оно не было получено от самого субъекта при жизни.

3. Состав персональных данных

3.1. АКБ «Энергобанк» (ОАО) обрабатывает персональные данные в соответствии с «Перечнем персональных данных, обрабатываемых в АКБ «Энергобанк» (ОАО)» (приложение 1 к настоящему Положению), в котором изложены типовые виды персональных данных. Для каждой банковской операции/небанковской операции характерен свой набор персональных данных, необходимых для её надлежащего выполнения.

3.2. Состав персональных данных, обрабатываемых Банком в процессе операций различен, обработке подлежат только персональные данные, необходимые для проводимой операции.

3.3. Основным оценочным критерием, для определения полноты и достаточности состава персональных данных является возможность на основании указанных персональных данных произвести идентификацию (аутентификацию) субъекта, а также оказать субъекту банковскую услугу. В случае если Персональные данные относятся к указанным в «Перечне персональных данных, обрабатываемых в АКБ «Энергобанк» (ОАО)», однако на их основании невозможно определить конкретного субъекта персональных данных (в силу их неточно-

сти/искажения, либо недостаточности), такие персональные данные не попадают под действие настоящего Положения.

4. Права и обязанность оператора по обработке персональных данных

4.1. Права оператора:

4.1.1. Получать полные и достоверные персональные данные от субъекта персональных данных, в случае, если субъект персональных данных выразил свое согласие, либо этого требуют договорные отношения. В первом случае основанием для получения от субъекта персональных данных является согласие субъекта персональных данных на обработку (приложение 2 к настоящему Положению), во втором случае – договор, заключенный между Банком и субъектом персональных данных, на основании и во исполнение которого такая обработка проводится.

5.1.2. Осуществлять обработку персональных данных только способами и только с помощью методов, соответствующих положениям законодательства и локальных актов, но в соответствии с конкретными требованиями проводимой операции.

5.1.3. Отказать в услуге лицу, обратившемуся за ней, в случае, если субъект персональных данных, после полученных разъяснений, отказывается от предоставления персональных данных, когда их получение необходимо для выполнения операции и без наличия персональных данных субъекта Банку произвести операцию невозможно.

5.1.4. Осуществлять передачу персональных данных третьим лицам, в случае наличия согласия субъекта персональных данных на такую передачу. Передача персональных данных субъекта может производиться только в целях надлежащего исполнения договора. Банк не предоставляет третьим лицам персональные данные субъектов, определяя такую передачу конечной целью обработки персональных данных.

5.2. Обязанности оператора:

5.2.1. Сообщать субъекту персональных данных по его запросу о целях обработки его персональных данных, а также о способах такой обработки, путем устных объяснений сотрудников Банка, либо путем размещения публичной информации на сайте www.energobank.ru

5.2.2. Сообщать сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ по обращению субъекта персональных данных (приложение 3 к настоящему Положению.).

5.2.3. Сообщать субъекту персональных данных перечень его персональных данных, обрабатываемых Банком в текущий момент времени в проводимой операции, а также способ их получения, в том случае, если в допустимых случаях данные по независящим от Банка причинам были предоставлены без согласия субъекта персональных данных.

5.2.4. Сообщать субъекту персональных данных цели, для достижения которых необходимо предоставление его персональных данных.

5.2.5. Сообщать субъекту персональных данных сроки обработки персональных данных, а также сроки их хранения.

5.2.6. Разъяснять субъекту персональных данных о юридических последствиях, которые может повлечь за собой обработка его персональных данных.

5.2.7. Разъяснять субъекту персональных данных о юридических последствиях, которые может повлечь отказ в предоставлении персональных данных.

5.2.8. Получать письменное согласие на обработку персональных данных, в случае, если субъект персональных данных согласен на такую обработку. Разъяснять субъекту персональных данных о возможности отзыва разрешения на обработку персональных данных, а также о порядке заявления такого отзыва.

5.2.9. Принять все возможные меры по обеспечению безопасности передачи персональных данных, если такая передача требуется.

6. Права и обязанности субъекта персональных данных

6.1. Права субъекта персональных данных:

6.1.1. Предоставить данные оператору персональных данных в запрашиваемые сроки, в полном объеме.

6.1.2. Получить информацию о целях и способах обработки персональных данных, о дальнейшем хранении и использовании, в объеме, не затрагивающем права Банка на конфиденциальную информацию.

6.1.3. Получить информацию о лицах, непосредственно осуществляющих обработку персональных данных.

6.1.4. Получить разъяснения о возможности отзыва согласия на обработку персональных данных, и о юридических последствиях такого отзыва.

6.1.5. Отозвать согласие на обработку персональных данных (приложение 5 к настоящему Положению).

6.1.6. В случае если персональные данные были изменены, уведомить об этом оператора (приложение 4 к настоящему Положению).

6.2.7. На ознакомление с персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя (приложение 9 к настоящему Положению).

6.2. Обязанности субъекта персональных данных:

6.2.1. Гарантировать достоверность данных, предоставляемых для обработки оператору. Оператор по обработке персональных данных не несет ответственности в случае, если предоставленные субъектом персональных данных данные недостоверны, и их использование повлекло наступление неблагоприятных последствий для субъекта персональных данных, либо для третьих лиц.

6.2.2. В случае согласия на предоставления персональных данных для их обработки оператором, подписать письменное соглашение, подготовленное оператором по обработке персональных данных.

7. Обработка персональных данных

7.1. Порядок обработки персональных осуществляется в соответствии с настоящим Положением, а также на основании Инструкций по обработке персональных данных (Приложение 6 к настоящему Положению).

7.2. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

7.3. Целью обработки персональных данных является исключительно осуществление функций кредитной организации, профессионального участника рынка ценных бумаг, работодателя.

Допускаются иные цели обработки персональных данные в случае, если указанные действия не противоречат деятельности Банка как кредитной организации и на проведение указанной обработки получено согласие субъекта персональных данных.

7.4. Обработка персональных данных осуществляется в строгом соответствии целям обработки персональных данных

7.5. Общие принципы обработки персональных данных предусмотрены в настоящем Положении.

7.6. Перечнем персональных данных предусмотрены виды и категории персональных данных, которые вправе обрабатывать АКБ «Энергобанк» (ОАО).

7.7. Общий перечень лиц, имеющих право доступа и обработки персональных данных, изложен в Приказе Председателя Правления АКБ «Энергобанк» (ОАО). Лица, имеющих непосредственный доступ персональным данным, подписывают соглашение о неразглаше-

нии персональных данных (Приложение 7 к настоящему Положению), и несут ответственность за разглашение. Ответственность сотрудника, разгласившего персональные данные, определяется в соответствии с законодательством РФ.

7.8. Оператор персональных данных признает приоритет безопасности при обработке персональных данных перед коммерческими целями и получением экономической выгоды.

7.9. Оператор персональных данных не несет ответственности за достоверность данных, предоставляемых для обработки, а также за наступление неблагоприятных последствий, вызванных предоставлением недостоверных данных.

7.10. Оператор персональных данных сообщает субъекту персональных данных о целях и методах обработки данных, а также разъясняет последствия отказа от предоставления персональных данных.

7.11. Обработка персональных данных может проводиться с применением автоматизированных систем и без таковых.

7.12. Обработкой персональных данных без применения средств автоматизации считаются использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека.

Под автоматизированной обработкой персональных данных понимаются действия, которые выполняются без участия человека, т.е. полностью автоматически. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что эти персональные данные содержались в информационной системе персональных данных либо были извлечены из нее.

7.13. Банк при обработке персональных данных принимает организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

7.14. Обработку персональных данных осуществляют сотрудники Банка, уполномоченные на то должностными инструкциями, иными внутренними документами Банка или организационно-распорядительными документами по Банку.

7.15. Сотрудники Банка, осуществляющие обработку персональных данных, должны знать о факте такой обработки, категориях обрабатываемых данных, об особенностях и правилах такой обработки, установленных законодательными и нормативными актами и внутренними банковскими документами.

В рамках информирования сотрудников Банка о факте обработки персональных данных, Банк обязывает сотрудников Банка самостоятельно изучать и соблюдать внутренние нормативные документы, регламентирующие как общий порядок работы с персональными данными, так и специальные нормы, касающиеся совершения отдельных действий, связанных с обработкой персональных данных.

7.16. Сотрудники Банка имеют право получать только те персональные данные, которые необходимы им для выполнения конкретной функции по должности.

7.17. Распространение (передача) персональных данных осуществляется с учётом следующего:

7.17.1. В случае если обязанность либо возможность предоставления имеющихся в распоряжении Банка персональных данных иным лицам (включая органы государственной и муниципальной власти) установлена законодательством и необходимость такой передачи прямо подтверждена уполномоченными сотрудниками Банка – Банк обязан предоставить указанные данные в составе, виде и сроки, указанные в законодательных или нормативных актах.

7.17.2. Передача персональных данных третьей стороне не в силу закона возможна только с письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных законодательными и нормативными актами.

7.17.3. Договоры с лицами, которым передаются персональные данные во исполнение договора, должны обязательно содержать условие об обеспечении конфиденциальности и безопасности передаваемых персональных данных.

7.17.4. Трансграничная передача персональных данных осуществляется только кредитным организациям, зарегистрированным в странах, являющихся сторонами Конвенции Совета Европы по защите физических лиц при автоматизированной обработке персональных данных.

Трансграничная передача персональных данных также может быть осуществлена в адрес кредитных организаций, зарегистрированных в иных странах, при условии, что законодательство указанных стран позволяет сделать вывод об адекватной защите персональных данных. Оценку возможности подобной передачи осуществляет Отдел обеспечения информационной безопасности.

Иная трансграничная передача осуществляется исключительно с письменного согласия субъекта персональных данных.

7.17.5. Субъект персональных данных вправе обратиться в Банк устно или с составленным с соблюдением требования законодательства запросом об обработке Банком.

Запрос должен содержать паспортные данные субъекта персональных данных, сведения, подтверждающие участие субъекта в отношениях с Банком, подпись субъекта или его представителя.

Запрос должен быть зарегистрирован в Журнале учета обращений граждан по вопросам предоставления доступа к персональным данным, который ведется Начальником отдела информационной безопасности Банка, и передан на визирование Юридическому отделу на предмет соответствия требованиям законодательства.

В случае если запрос не соответствует требованиям к оформлению запроса, либо в случае, если сведения по аналогичному запросу предоставлялись не позднее тридцати календарных дней от даты получения запроса, Юридический отдел отказывает в принятии запроса, о чём формирует мотивированный отказ за подписью Заместителем председателя правления по правовым вопросам и передаёт его для отправки субъекту персональных данных.

В случае соответствия запроса требованиям настоящего пункта, Юридический отдел визирует запрос и передаёт его для исполнения Начальнику Отдела обеспечения информационной безопасности.

Начальник Отдела обеспечения информационной безопасности готовит ответ субъекту персональных данных с указанием следующей информации:

- 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 сотрудников 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 настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные действующим законодательством.

Ответ подписывается Начальником Отдела обеспечения информационной безопасности и направляется для отправки субъекту персональных данных.

Сведения должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные иных субъектов, если иное не установлено законодательством.

7.17.6. Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Банком, а также цель такой обработки;
- способы обработки персональных данных, применяемые Банком;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Факты устного обращения также подлежат фиксации в Журнале учета обращений граждан.

7.18.1. Хранение персональных данных осуществляется на бумажных и электронных носителях.

Порядок хранения персональных данных определен в Положении о хранении Персональных данных. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении сроков их хранения, или продлевается на основании заключения экспертной комиссии Банка.

7.18.2. Хранение персональных данных осуществляется не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по достижении целей обработки, в случае утраты необходимости в их достижении или в случае получения отзыва согласия на обработку персональных данных от субъекта персональных данных. Удаление оформляется Актом об уничтожении персональных данных. (Приложение 8 к настоящему Положению).

7.19. Уточнение персональных данных производится сотрудниками, ответственными за обработку соответствующих персональных данных.

Уточнение персональных данных производится на основании:

- документов, предоставленных субъектом персональных данных либо его доверенным лицом в процессе исполнения договорных отношений;
- документов уполномоченного органа по защите прав субъектов персональных данных;
- данных из общедоступных источников.

Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Уточнение персональных данных должно быть произведено не позднее семи рабочих дней от даты получения Банком от субъекта персональных данных информации, подтверждающей необходимость уточнения персональных данных.

7.20. Блокирование персональных данных представляет собой деятельность Банка по временному прекращению обработки персональных данных. Блокирование осуществляется в случае если субъектом персональных данных (его законным представителем) либо уполномоченным органом по защите прав субъектов персональных данных выявлена недостоверность персональных данных.

7.20.1. Блокирование осуществляется руководителем подразделения, осуществляющего обработку персональных данных при условии уведомления Начальника Отдела обеспечения информационной безопасности, контролирующего правильность процесса блокирования.

7.20.2. Блокирование данных на электронных носителях может быть осуществлено путём установления специальных прав доступа к персональным данным либо путём копирования данных на специальное рабочее место с ограниченным доступом с одновременным удалением данных из первоначального места хранения.

7.20.3. Блокирование бумажного носителя производится путём его изъятия и хранения у Начальника Отдела обеспечения информационной безопасности в обособленном месте, исключающем возможность его обработки.

7.20.4. Блокирование бумажного носителя информации содержащего персональные данные как подлежащие, так и не подлежащие блокированию, осуществляется копирование бумажного носителя способом, исключающим совместное копирование данных типов информации (удаление, вымарывание заблокированного фрагмента). В дальнейшей деятельности используется копированный материальный носитель, не содержащий заблокированной информации, заблокированный материальный носитель передаётся на хранение Начальнику Отдела обеспечения информационной безопасности.

7.20.5. Снятие блокирования осуществляется после уточнения персональных данных на основании информации, переданной субъектом персональных данных или уполномоченным органом по защите прав субъектов персональных данных.

7.20.6. Снятие блокирования сопровождается уведомлением сотрудника, ответственного за хранение заблокированной информации, о снятии блокирования после уточнения персональных данных. Блокированные документы на магнитных носителях подлежат разблокировке и уточнению, блокированные документы на материальных носителях подлежат возврату в подразделение, передавшее персональные данные для блокирования.

7.21. Уничтожение персональных данных производится Банком:

- при выявлении неустраняемых неправомерных действий с персональными данными;
- при истечении сроков обработки персональных данных;
- при получении от субъекта персональных данных отзыва согласия на обработку персональных данных, которые не были использованы в рамках договорных отношений, стороной по которым является субъект персональных данных;
- по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных – если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Уничтожению подлежат вся необходимая к уничтожению персональная информация, зафиксированная на бумажных либо магнитных носителях.

Уничтожение персональных данных на бумажных носителях в связи с истечением срока обработки персональных данных производится в соответствии со стандартными внутрибанковскими процедурами.

Уничтожение персональных данных на магнитных носителях в связи с истечением срока обработки персональных данных производится должностным лицом в порядке установленном настоящим положением, использовавшим указанные данные. Начальник обеспечения информационной безопасности при проверках по направлениям деятельности контролирует полноту уничтожения указанных данных на рабочих местах и сетевых ресурсах Банка.

7.21.1. Решение об уничтожении персональных данных по иным основаниям принимается Председателем Правления Банка по представлению руководителя подразделения, ответственного за обработку соответствующих персональных данных, признанных необходимыми к уничтожению. Решение об уничтожении должно быть принято не позднее дня, следующего за днём появления оснований к уничтожению персональных данных.

7.21.2. Немедленно при получении соответствующей санкции на уничтожение персональных данных Председателя Правления Банка, руководитель подразделения, осуществляющего обработку персональных данных, обязан уведомить об этом Начальника отдела обеспечения информационной безопасности Банка (для данных, хранящихся на материальных носителях) с предоставлением полной информации обо всех местах хранения соответствующих персональных данных.

7.21.3. Уничтожение персональных данных производится руководителем подразделения (для данных, хранящихся в электронной форме) или Комиссией Банка по уничтожению персональных данных (для данных, хранящихся на материальных носителях).

В случае если согласно имеющейся у Банка информации, персональные данные были направлены третьим лицам, руководитель подразделения, осуществляющего обработку соответствующих персональных данных, обязан уведомить в письменной форме указанных третьих лиц о необходимости уничтожения персональных данных с изложением оснований для подобного уничтожения.

7.21.4. После уничтожения данных Заместитель Председателя Комиссии Банка по уничтожению персональных данных обязан письменно уведомить о данной операции подразделение, передавшее информацию на уничтожение.

7.21.5. При получении информации об уничтожении либо после самостоятельного уничтожения, подразделение, осуществлявшее обработку персональных данных, обязано уведомить о факте уничтожения субъект персональной информации, в случае если уничтожение происходило по инициативе субъекта персональных данных, и, если уничтожение произведено по запросу уполномоченного органа по защите персональной информации, указанный орган.

Уведомление должно содержать перечень мер, предпринятых Банком по результатам обнаружения случаев неправомерной обработки персональных данных.

7.21.6. Начальник Отдела обеспечения информационной безопасности в рамках проверок по направлениям деятельности контролирует своевременность и полноту уничтожения персональных данных руководителями подразделений.

7.22.1. Сроки обработки персональных данных клиентов (работников) Банка определяются в соответствии со сроком действия договора с субъектом персональных данных, с Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утвержденным Приказом Минкультуры России от 25.08.2010 г. №558, Положением о порядке и сроках хранения документов акционерных обществ, утвержденным Постановлением Федеральной комиссии по рынку ценных бумаг от 16.07.2003 г. № 03-33/пс, сроком исковой давности, а также иными требованиями законодательства и нормативными документами Банка; при этом срок хранения персональных данных субъекта не может быть менее 5 лет по истечении срока действия договора, при условии, что все обязательства, вытекающие из договора, прекращаются с истечением срока действия договора или при расторжении договора.

7.22.2. Сроки обработки персональных данных клиентов (работников) Банка обрабатываемых в автоматизированных банковских системах определяются сроком действия договора, срок хранения персональных данных субъекта в автоматизированных банковских системах не может быть менее 10 лет по истечении срока действия договора с субъектом персональных данных, при условии, что все обязательства, вытекающие из договора, прекращаются с истечением срока действия договора или при расторжении договора.

8. Общие требования к обеспечению безопасности персональных данных

8.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный и динамичный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

8.2. Для обеспечения безопасности Банк применяет следующие методы и способы защиты информации в информационных системах:

8.2.2. Ограничение и контроль доступа в помещения Банка.

Банк осуществляет контроль и ограничение доступа в помещения Банка в соответствии с нормами Положения «О пропускном режиме и контроле доступа в помещения АКБ «Энергобанк» (ОАО)» путём разграничения доступа по зонам и установления процедур доступа в различные зоны.

В конце рабочего дня помещения, в которых осуществляется обработка персональных данных, должны быть закрыты на ключ и переданы под сигнализацию сотрудниками охраны в порядке, означенном в вышеуказанном Положении.

8.2.3. Определение специальных требований к помещениям, в которых осуществляется обработка персональных данных.

Помещения, в которых осуществляется обработка персональных данных, должны быть оборудованы по возможности запираемыми шкафами для хранения источников персональных данных и также должны обеспечивать отсутствие возможности несанкционированного доступа третьих лиц путём запираения либо опечатывания помещений во внерабочее время либо на время отсутствия сотрудников Банка в соответствующих помещениях.

Все хранилища с материальными носителями персональных данных, должны размещаться в служебном помещении, так что бы каждый сотрудник помещения мог визуально контролировать доступ к хранилищам. В случае выявления нештатной ситуации, сотрудник обязан оповестить непосредственного руководителя и Начальника отдела обеспечения информационной безопасности Банка. В рабочее время, помещения которые не оборудованы дверьми с магнитными замками, при выходе из помещения сотрудников подразделения, должны запирается на ключ. Ключ сдаётся на хранение поста охраны. Доступ к ключам предоставляется исключительно лицам, чьё рабочее место находится в означенном помещении.

8.2.4. Регистрация действий.

Регистрация действий сотрудников в информационных системах ведется в электронной базе приложений. Доступ по администрированию электронных журналов возлагается на Начальника отдела обеспечения информационной безопасности Банка, в соответствии с должностными инструкциями.

Ограничение по объему и ведению электронного журнала в информационных системах не устанавливается. По мере заполнения журнала, все данные в автоматическом режиме и с простановкой даты создания, помещается в архив.

В электронных журналах должны быть гибко прописаны действия пользователей: вход\выход, перечень информации по данным относительно того, кто и когда ввел его в систему, редактировал, а также прочую служебную информацию.

8.2.5. Учёт и хранение съёмных/бумажных носителей информации.

Персональные данные, обработка которых осуществляется в несовместных целях подлежат отдельному хранению в целях обеспечения разграничения доступа.

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Все находящиеся на хранении и в обращении съёмные технические носители с персональными данными подлежат учёту. Каждый съёмный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

Учёт и выдачу съемных носителей персональных данных осуществляют руководитель структурного подразделения Банка, на которого возложены функции обеспечения контроля хранения носителей персональных данных. Сотрудники Банка получают учтенный съемный носитель от руководителя подразделения для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ сотрудник сдает съемный носитель для хранения руководителю подразделения, о чем делается соответствующая запись в журнале учета.

Хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам, выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому запрещено.

Съемные/бумажные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, утративших свое практическое значение и не имеющих исторической ценности подлежат уничтожению. Уничтожение съемных/бумажных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт.

Бумажные носители персональных данных хранятся в помещениях, оборудованных средствами пожаротушения, охранной и противопожарной сигнализацией; с применением специального оборудования для хранения документов (стеллажей, сейфов, коробок и т.д.);

8.2.6. Резервирование.

Для предотвращения рисков полной или частичной утери информации в информационных системах, в случаях форс-мажора (выход из строя аппаратного комплекса, жестких дисков и т.д.) в Банке реализовано резервное дублирование аппаратных систем и баз данных. Требования по организации и обеспечению безопасности при резервировании информации изложены Регламенте резервного копирования.

8.2.7. Использование криптографических средств защиты.

Для обеспечения информационной безопасности при осуществлении передачи персональных данных по открытым каналам связи Банк использует сертифицированные средства криптографической защиты. Электронные документы снабжаются ключами электронной цифровой подписи и шифрования. Порядок использования указанных средств защиты определяется на основании заключенных договоров.

8.2.8. Обеспечение безопасности персональных данных средствами антивирусной защиты.

Для осуществления информационной безопасности при осуществлении обработки персональных данных в информационных системах в автоматическом или не автоматическом режиме должен применяться комплекс мер антивирусного программного обеспечения. На этапах разработки и внедрения той или иной системы обработки персональных данных, производится анализ возможного внедрения антивирусного программного обеспечения на все стадии комплексной обработки, от ввода до удаления информации.

Система мер и мероприятий, направленных на защиту рабочих мест, определяется Антивирусной политикой Банка и Инструкцией по защите от компьютерных вирусов.

Перед использованием в работе в информационных систем, все съемные носители, используемые для предоставления электронных данных надзорным органам, должны в строгом порядке проходить предварительное сканирование антивирусным программным обеспечением.

При предварительном сканировании, в случае обнаружения вредоносных программ на съемных носителях, сотрудники обязаны прекратить любые действия со съемными носителями и оповестить непосредственного руководителя. Зараженные носители в опечатанном конверте передаются Начальнику отдела обеспечения информационной безопасности. Начальник отдела обеспечения информационной безопасности производит с помощью встроенных средств антивирусного обеспечения лечение зараженных файлов. В случае успешного лечения производит возврат носителя ответственному сотруднику, в случае невозможности лечения, производит форматирование съемного носителя, после чего он направляется ответственному сотруднику.

8.2.9. Требования по обеспечению информационной безопасности центров обработки данных.

В качестве централизованного хранилища персональных данных могут использоваться только серверные станции, прошедшие все стадии внедрения информационных систем от анализа технической документации разработчика, до установки в серверное помещение.

Обеспечение информационной безопасности серверных станций обеспечивается комплексом мер центра обработки данных (ЦОД):

Специальное оборудование и охрана помещения, в котором оборудован ЦОД, обеспечивают невозможность неконтролируемого проникновения в эти помещения посторонних лиц. На входные двери установлены замки, гарантирующие надежную защиту помещений в нерабочее время, а для контроля за входом в помещение установлены автоматические магнитные замки. Подходы к помещению оборудовано системой видеонаблюдения. Двери ЦОД должны быть постоянно закрыты на магнитный замок и могут открываться только для прохода уполномоченных сотрудников Банка. По окончании рабочего дня помещение ЦОД должно быть закрыто. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещение ЦОД посторонних лиц, должно быть немедленно сообщено Начальнику отдела обеспечения информационной безопасности. Доступ в серверные помещения строго ограничен. Список лиц, допущенных в серверное помещение, утверждается руководством Банка.

9. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

9.1. В соответствии с Законом «О персональных данных» № 152-ФЗ, настоящим Положением лица, нарушившие требования Закона, а также внутренних документов Банка, привлекаются к ответственности.

9.2. Размер ответственности, формы, способы привлечения к ней определяются работодателем в соответствии с действующим законодательством.

10. Прочие условия

10.1. Настоящее положение вступает в силу с даты его утверждения.

10.2. Изменения в настоящее положения утверждаются Приказом Председателя Правления Банка.

10.3. В обязанности работников, осуществляющих первичную обработку персональных данных, входит получение согласия субъекта на обработку его персональных данных.



2011 г.

**Перечень персональных данных, обрабатываемых в
Акционерном коммерческом банке «Энергобанк»
(открытое акционерное общество)**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Перечень персональных данных, подлежащих обработке и защите в АКБ «Энергобанк» (ОАО) (далее – Перечень), разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О защите персональных данных» и Уставом АКБ «Энергобанк» (ОАО) (далее – Банк).

1.2. Настоящий перечень является основным документом, определяющим, какие именно персональные данные проходят обработку АКБ «Энергобанк» (ОАО) и из каких категорий данных они состоят, а также цели, сроки, порядок такой обработки.

1.3. Перечень вводится в действие и изменяется приказом Председателя Правления Банка.

**2. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ
ДАнные**

2.1. Сведениями, составляющими персональные данные, и обрабатываемые в АКБ «Энергобанк» (ОАО) (далее – Банк), является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

В случае если на основании полученных сведений провести идентификацию (аутентификацию) субъекта персональных данных невозможно (вследствие их ограниченного объема, либо искажения) такие сведения не являются персональными данными обработка таких сведений не подпадает под действие Федерального закона «О защите персональных данных» и вне зависимости от наличия их в настоящем перечне.

Банк не обрабатывает биометрические персональные данные; обработка специальных персональных данных допускается в соответствии с трудовым законодательством.

2.1.1. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, а именно:

2.1.2. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.1.3. Паспортные данные или данные иного документа, удостоверяющего личность (предусмотренные законодательством Российской Федерации), (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.

2.1.4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.

2.1.5. Номера телефонов (мобильного и домашнего), в случае их регистрации на имя субъекта персональных данных или по адресу его места жительства (регистрации по паспорту).

2.1.6. Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения, дата начала и завершения обуче-

ния, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения).

2.1.7. Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения).

2.1.8. Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и ее наименования, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, характеристика личностных качеств работника и его образа жизни).

2.1.9. Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней.

2.1.10. Содержание и реквизиты трудового договора с работником Организации или гражданско-правового договора с гражданином.

2.1.11. Сведения о заработной плате (номера счетов для расчета с работниками, данные зарплатных договоров с клиентами, в том числе номера их спецкартсчетов, данные по окладу, надбавкам, налогам и другие сведения).

2.1.12. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии\снятии на(с) учет(а) и другие сведения).

2.1.13. Сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2НДФЛ супруга(и), данные документов по долговым обязательствам, степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения).

2.1.14. Сведения об имуществе (имущественном положении):

- автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств) – сведения в составе ПТС и СоПТС ;

- недвижимое имущество (вид, тип, способ получения, общие характеристики, стоимость, полные адреса размещения объектов недвижимости и другие сведения) – сведения в составе Свидетельства о регистрации прав на недвижимость, правоустанавливающих документов и технического и кадастрового паспортов объекта недвижимости;

- банковские вклады (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов, вид, срок размещения, сумма вклада и остаток по вкладу);

2.1.15. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

2.1.16. Сведения об идентификационном номере налогоплательщика.

2.1.17. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).

2.1.18. Сведения, указанные в оригиналах и копиях приказов по личному составу Банка и материалах к ним.

2.1.19. Сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) работников Банка.

2.1.20. Материалы по аттестации и оценке работников Банка.

2.1.21. Материалы по внутренним служебным расследованиям в отношении работников Организации.

2.1.22. Внутрибанковские материалы по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами.

2.1.23. Сведения о временной нетрудоспособности работников Банка.

2.1.24. Табельный номер работника Банка.

2.1.25. Сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения).

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Целями обработки персональных данных в Банке является:

3.1. Осуществление банковских операций (оказание банковских услуг) на условиях, определяемых договором, 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;

3.2. Организация учета работников Банка для целей, определяемых Банком (учет уровня соответствия профессиональных навыков Субъекта ПДн требованиям Банка, фактов нарушения трудовой дисциплины и материалы расследований по таким фактам) в соответствии с внутренними нормативными актами Банка,

3.3. Продвижение банковских услуг на рынке.

4. Сроки обработки

Сроки обработки персональных данных определяются в соответствии с Положением о персональных данных, порядке их обработки и обеспечении безопасности в АКБ «Энергобанк» (ОАО).

Приложение 2

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Казань

« ____ » _____ 20__ г.

Я, _____,
(Фамилия, Имя, Отчество полностью)

дата рождения _____, _____ серия _____ № _____
(наименование документа)

выдан _____ дата _____

проживающий(ая) по адресу: _____, действуя свободно, своей волей, настоящим даю свое сознательное согласие Акционерному коммерческому банку «Энергобанк» (Открытое акционерное общество), 420031, г. Казань, ул. Сары Садыковой, д. 32, (далее - Банк) на обработку в полном объеме всех персональных данных (перечень персональных данных, на обработку которых дается настоящее согласие) как любой относящейся ко мне прямо или косвенно информации, доступной и/или известной Банку в любой момент времени, кроме специальных категорий персональных данных по п.1 ст. 10 Федерального закона «О персональных данных» (далее - «Персональные данные») для целей получения и совершения банковских услуг, операций и сделок, заключения и исполнения с Банком любых договоров, предоставления информации об оказываемых Банком услугах в целях продвижения услуг на рынке, принятия решений или совершения иных действий на основании в т.ч. исключительно автоматизированной, а также смешанной обработки персональных данных, порождающих юридические последствия в отношении меня или других лиц.

Настоящее согласие предоставляется на осуществление любых действий (операций) в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, в т.ч. в случае привлечения для исполнения договора третьих лиц, включая: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение, а также трансграничную передачу Персональных данных во исполнение договоров, а также осуществление любых иных действий с моими Персональными данными с учетом и в объеме действующего законодательства, с применением следующих основных способов (но, не ограничиваясь ими): хранение, запись на электронные носители и их хранение, составление перечней, маркировка, на любых материальных носителях, в том числе электронных, с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без таковых. Настоящим я выражаю согласие на раскрытие и передачу персональных данных Банком для достижения указанных целей любым третьим лицам, их агентам и уполномоченным лицам, на условиях сохранения конфиденциальности.

Настоящее согласие действует не менее 5 лет после прекращения сроков действия всех заключенных между мной и Банком договоров и вытекающих из них обязательств сторон, но не менее сроков хранения соответствующей информации или материальных носителей, содержащих вышеуказанную информацию, определяемых в соответствии с законодательством Российской Федерации, и не менее, чем того требуют цели обработки персональных данных. Согласие может быть отозвано путем предоставления мною Банку письменного уведомления об отзыве согласия, что не препятствует продолжению обработки персональных данных, связанных с исполнением договора и хранением материальных носителей в установленном законодательством порядке.

Я гарантирую, что персональные данные иных субъектов, необходимые для установления и осуществления моих прав и законных интересов, в т.ч. для заключения договора (в т.ч. по которым стороной, выгодоприобретателем или поручителем прямо или косвенно становится субъект персональных данных), указанные или предоставленные мной устно и в документах, передаются мною Банку при гарантированном наличии предусмотренных законом оснований, с согласия и уведомления субъекта персональных данных об их обработке АКБ «Энергобанк» (ОАО), факт наличия которых подтверждается в т.ч. полномочиями из обстановки (в т.ч. ст. 182 ГК РФ, фактом знания полных персональных данных), может быть мною подтверждены предоставлением письменных согласий и/или уведомлений указанных лиц на обработку их персональных данных.

Я знаю, что при отказе от согласия на обработку персональных данных Банк вправе отказать в предоставлении услуги и/или заключении договора.

_____/_____
(подпись) (расшифровка подписи: фамилия, имя, отчество указывается собственноручно)

Заполняется в случае дачи согласия на обработку персональных данных представителем субъекта персональных данных.

_____, дата рождения _____,
(Фамилия, Имя, Отчество полностью)

серия _____ № _____, выдан _____,
(наименование документа)

дата _____, проживающий(ая) по адресу: _____,
являясь представителем _____ и имеющий право на дачу согласия от его
(Ф.И.О. субъекта персональных данных)
имени на основании _____.

/ _____

гр. _____

Уважаемый _____ !

В ответ на Ваш запрос № _____ от _____, АКБ «Энергобанк» (ОАО) сообщает:

« ____ » _____ г. АКБ «Энергобанк» (ОАО) получил от _____ сведения, содержащие персональные данные:

1. ФИО: _____,

2. паспортные данные: _____

3. дата и место рождения: _____

4. _____

5. _____

Указанные данные были получены АКБ «Энергобанк» (ОАО) в целях оказания банковской услуги _____, на что предварительно было получено Ваше письменное согласие (копия прилагается); либо в целях исполнения договора, заключенного в Вами, либо по которому Вы являетесь выгодоприобретателем или поручителем, а также для заключения договора по Вашей инициативе или договора, по которому Вы будет являться выгодоприобретателем или поручителем

В настоящее время, материальные носители, содержащие Ваши персональные данные – _____, хранятся в _____ по адресу _____.

Непосредственный доступ к ним имеют следующие лица: _____,

обязанность работы с персональными данными субъектов на них предусмотрена характером выполняемых трудовых обязанностей, а также Приказом № _____ Председателя Правления АКБ «Энергобанк» (ОАО). Необходимость хранения Ваших персональных

данных связана с текущим исполнением условий договора и/или не достижением целей обработки персональных данных.

Вы можете безвозмездно ознакомиться с указанными персональными данными в срок не позднее 30 дней с даты подачи заявления на ознакомление с персональными данными по адресу _____.

**Председатель Правления
АКБ «Энергобанк» (ОАО)**

/Д.И.Вагизов/

Приложение 4.
Председателю Правления
АКБ «Энергобанк» (ОАО)
Вагизову Д.И.

от _____
(ФИО субъекта ПДн)

_____ (адрес регистрации субъекта ПДн)

_____ (паспортные данные субъекта ПДн)

ЗАПРОС

**(о предоставлении/ изменении / исключении
персональных данных субъекта)**

Мною, _____ (ФИО), «___» _____ г. (дата предоставления ПДн) в связи с осуществлением обязательств по договору _____ №___ от «___» _____ 20__ г. в АКБ «Энергобанк» (ОАО) были предоставлены следующие _____ персональные _____ дан-
ные _____

_____ (указать, какие сведения были предоставлены в Банк, например: ФИО, паспортные данные, сведения о дате и месте рождения и т.п.).

Указанные данные были предоставлены мною для _____

_____ (указать, для проведения какой операции были предоставлены данные).

1. В настоящее время сообщая об изменении/исключении следующих моих персональных данных в связи _____ с

_____ :

- _____

- _____

- _____

- _____

- _____

_____ (указать какие данные, каким образом поменялись, например: - ФИО изменение Иванова И.И, на Петрова И.И.)

В срок не позднее 7 (Семи) рабочих дней с даты получения документального подтверждения об изменении персональных данных прошу внести изменение/ исключить персональные данные в связи с _____

_____ (прекращении отношений с Банком, утратой сведениями достоверности и т.д).

Уведомить о факте изменения прошу по телефону номер _____.

приложение:

- _____
- _____
- _____

(ФИО)

(подпись)

(дата)

Приложение 5.
**Председателю Правления
АКБ «Энергобанк» (ОАО)
Вагизову Д.И.**

от _____
(ФИО субъекта ПДн)

(адрес регистрации субъекта ПДн)

(паспортные данные субъекта ПДн)

О Т З Ы В
согласия на обработку персональных данных

Настоящим я, _____
(указать ФИО), отзываю согласие на обработку моих персональных данных, предостав-
ленное АКБ «Энергобанк» (ОАО) в целях _____

(указать в каких целях оно было предоставлено).

Прошу прекратить обработку моих персональных *данных предоставленных для за-
ключения договора и заключения банковских услуг* немедленно, после получения настоя-
щего Отзыва.

Подтверждаю, что уведомлен о юридических последствиях получения АКБ «Энер-
гобанк» (ОАО) настоящего отзыва, а именно, о невозможности продолжения получения
банковской услуги/исполнения условий договора, в связи с необходимостью обработки
моих персональных данных.

Подтверждаю, что уведомлен о невозможности для АКБ «Энергобанк» (ОАО) пре-
кращения обработки персональных данных, в том случае, если обработка персональных
данных необходима для исполнения договора, в котором я являюсь стороной либо выго-
доприобретателем или поручителем, а также для заключения договора по моей
инициативе, по которому я буду являться выгодоприобретателем или поручителем, а так-
же если мои персональные данные были получены в целях, по которым АКБ «Энерго-
банк» (ОАО) не является оператором обработки персональных данных.

Фамилия, Имя, Отчество _____

Подпись _____

дата _____



2011 г.

Инструкция о порядке неавтоматизированной и смешанной обработки ПДн.

1. Общие положения

1.1. Настоящая инструкция разработана на основании ст. 19 Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», во исполнение требований Комплекса БР ИББС, для приведения деятельности АКБ «Энергобанк» (ОАО) (далее - Банк) в соответствие с требованиями законодательства в области персональных данных, для исполнения требований локальных актов АКБ «Энергобанк» (ОАО) в области защиты персональных данных.

1.2. Основная цель Банка, в связи с исполнением своих обязанностей по обработке персональных данных – обеспечение безопасности персональных данных, необходимых для выполнения текущей деятельности, оказания банковских услуг и надлежащего выполнения договорных обязательств, а также продвижение банковских услуг на рынке.

1.3. Обеспечение безопасности персональных данных означает, что персональные данные признаются конфиденциальной информацией, и Банку необходимо исключить:

- несанкционированный (в том числе случайный, стихийный) доступ к персональным данным,
- несанкционированное уничтожение персональных данных,
- несанкционированное изменение персональных данных,
- несанкционированное блокирование персональных данных,
- несанкционированную утрату конфиденциальности персональных данных,
- несанкционированное распространение персональных данных (сообщение персональных данных неуполномоченным на получение такой информации лицам),
- искажение персональных данных,
- иные несанкционированные ответственными лицами действия, которые могут угрожать утрате сведений, в т.ч. их целостности, либо их несанкционированной модификации, передачи.

1.4. Общее управление по вопросу безопасности персональных данных осуществляется лично Председателем Правления Банка. Ответственность за принятие превентивных мер по обеспечению безопасности персональных данных возлагается на отдел обеспечения информационной безопасности Банка. Ответственность за обеспечение безопасности персональных данных при их обработке возлагается на лиц, допущенных к их обработке.

1.5. Обработка персональных данных осуществляется путем автоматизированной, неавтоматизированной и смешанной обработке.

1.6. Порядок обработки персональных данных в ИСПДн (в информационных системах персональных данных) осуществляется в соответствии с Инструкцией пользователя ИСПДн. Превентивные меры по обеспечению безопасности осуществляет Администратор ИСПДн.

1.7. Настоящая инструкция распространяется на случаи неавтоматизированной и смешанной обработки.

1.8. Лицам, ответственным за обработку персональных данных в подразделениях Банка, необходимо обеспечить фиксацию каждого случая нарушения данной инструкции

в Журнале угроз безопасности персональных данных (приложение к настоящей инструкции).

2. Обеспечение безопасности перед началом работы с персональными данными.

2.1. Работник вправе осуществлять обработку персональных данных только в порядке исполнения своих прямых трудовых обязанностей, либо обязанностей, вытекающих из характера трудовых обязанностей, и должен знать, каковы цели, задачи и порядок обработки персональных данных.

2.2. Перед началом обработки персональных данных необходимо удостовериться, что материальные носители персональных данных не повреждены, не изменены и не утрачены и имеют подпись субъекта персональных данных или лица, предоставившего их в установленном порядке. В случае, если материальные носители были утрачены, изменены или повреждены, следует письменно немедленно доложить об этом непосредственному руководителю, а, в случае его отсутствия, Руководителю отдела обеспечения информационной безопасности Банка.

2.3. Необходимо убедиться, что рабочее место, на котором будет осуществляться обработка персональных данных, свободно от посторонних лиц, либо лиц, не имеющих прямого распоряжения и не допущенных до обработки персональных данных. Запрещается приступать к обработке персональных данных, в случае, если в помещении имеются посторонние лица, и их присутствие может создать угрозы безопасности персональных данных.

2.4. В случае, если при обработке используются технические средства ввода информации и защиты персональных данных, необходимо убедиться, что, в случае, если, они находятся в рабочем состоянии, исправно функционируют. Категорически запрещается приступать к обработке персональных данных с использованием неисправных технических средств. Обо всех неисправностях следует немедленно сообщить непосредственному руководителю, а, в случае его отсутствия, Руководителю отдела обеспечения информационной безопасности Банка письменно.

2.5. Необходимо убедиться, что к персональным данным (в том числе с момента последней работы с ними), не был осуществлен несанкционированный доступ. В случае, если такой доступ по мнению работника был осуществлен, необходимо незамедлительно сообщить об этом непосредственному руководителю, а, в случае его отсутствия, Руководителю отдела обеспечения информационной безопасности Банка письменно. Обработка персональных данных, к которым был осуществлен несанкционированный доступ, не производится до того момента, как поступят пояснения и распоряжения отдела обеспечения информационной безопасности Банка.

2.6. Необходимо убедиться, что персональные данные, подлежащие обработке в целях проведения конкретной операции, не содержат избыточных, ненужных и незапрашиваемых в целях выполнения текущей операции сведений. Категорически запрещается обрабатывать персональные данные, в случае, если их объем превышает объем необходимых персональных данных.

3. Обеспечение безопасности в процессе обработки персональных данных

3.1. В процессе обработки персональных данных необходимо контролировать и не допускать нахождения в помещении лиц, не имеющих прав на обработку персональных данных (лиц, не допущенных к обработке персональных данных приказом Председателя Правления АКБ «Энергобанк» (ОАО)). В случае, если посторонние лица пытаются проникнуть к рабочим местам, необходимо предупредить об этом непосредственного руководителя, либо незамедлительно сообщить Руководителю отдела обеспечения информационной безопасности Банка.

3.2. Необходимо не допускать воздействия на технические средства автоматизированной обработки персональных данных, способного нарушить их функционирование. При этом запрещается как нарушение исправности этого оборудования физическим способом, так и использование указанного оборудования в других целях, а также использова-

ние в помещениях с техническими средствами автоматизированной обработки персональных данных принесенных технических средств. В случае возникновения такой ситуации необходимо предупредить об этом непосредственного руководителя, либо незамедлительно сообщить Руководителю отдела обеспечения информационной безопасности Банка.

3.3. Необходимо осуществлять постоянный контроль над использованием средств защиты информации, предусмотренных эксплуатационной и технической документацией. Не допускается осуществлять обработку персональных данных без использования средств защиты информации, или в случае повреждения средств защиты информации.

3.4. Необходимо предотвращать несанкционированный доступ к персональным данным, а также доступ лиц, не допущенных к обработке персональных данных. В случае, если такой доступ произошел либо имеется его угроза, необходимо доложить об этом непосредственного руководителя, либо незамедлительно сообщить Руководителю отдела обеспечения информационной безопасности Банка.

3.5. Необходимо обеспечить конфиденциальность персональных данных в процессе их обработки. Для этого запрещается несанкционированно: сообщать персональные данные третьим лицам и лицам, не допущенным к обработке персональных данных, устно, а также на материальных носителях (как оригиналов, так и копий, снимать ксерокопии с материальных носителей документов, отправлять их по факсу, делать фотографий документов, передавать их посредством почтовых, в т.ч. электронных отправлений).

4. Обеспечение безопасности при завершении обработки персональных данных

4.1. После завершения использования персональных данных необходимо обеспечить исключение несанкционированного доступа к персональным данным, (в том числе и в помещения, где хранятся материальные носители персональных данных). Для этого необходимо, чтобы после завершения работы с материальными носителями, все они были убраны в запирающиеся шкафы и в сейфы в соответствии с нормами хранения, все изменения в программных средствах были сохранены, и зафиксированы.

4.2. Необходимо убедиться, что все средства защиты информации, которые должны функционировать после завершения работы с персональными данными, при отсутствии лиц, осуществляющих такую обработку, функционируют.

4.3. Необходимо проверить, что все нарушения указанной инструкции были зафиксированы в Журнале угроз обеспечению безопасности персональных данных, в случае, если в течение рабочего дня происходили нарушения данной инструкции.

5. Обеспечение безопасности персональных данных в экстремальных ситуациях

5.1. Необходимо предпринять все возможные меры к обеспечению незамедлительного восстановления персональных данных при их модификации или уничтожении, произошедших вследствие несанкционированного доступа к ним или сбоя.

5.2. Необходимо приостановить обработку персональных данных, а также их получение, в случае, если был нарушен порядок обработки и получения персональных данных, в связи с каким-либо чрезвычайным происшествием, если последствия этого происшествия не ликвидированы.

5.3. В случае, если работник обнаружил, что к персональным данным осуществляется несанкционированный доступ, необходимо немедленно прервать этот доступ, и сообщить об этом непосредственному руководителю, а, при его отсутствии – начальнику отдел обеспечения информационной безопасности Банка.

5.4. В случае несоблюдения условий обработки персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных необходимо произвести служебное разбирательство и составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

5.5. Обо всех экстремальных ситуациях необходимо немедленно поставить в известность Начальника отдела обеспечения информационной безопасности Банка.

6. Порядок реагирования в ситуации угрозы безопасности персональных данных

6.1. При возникновении угрозы безопасности персональных данных, в каждом случае необходимо незамедлительно сообщить о возникновении такой угрозы непосредственному руководителю, а, в случае его отсутствия, начальнику отдела обеспечения информационной безопасности Банка.

6.2. До того, как были предприняты меры по устранению угрозы безопасности персональных данных, каждый сотрудник, осуществляющий обработку персональных данных, обязан предпринять все возможные меры для устранения неблагоприятных последствий угрозы безопасности персональных данных.

6.3. При расследовании инцидента угрозы безопасности персональных данных, каждый сотрудник обязан оказывать всестороннее содействие отделу обеспечения информационной безопасности Банка в расследовании угрозы.

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации
(персональных данных лиц, клиентов и работников АКБ «Энергобанк» (ОАО))

Я, _____

(ФИО сотрудника банка / лица, работающего по гражданско-правовому договору)

исполняющий (ая) должностные обязанности по занимаемой должности:

(должность, наименование структурного подразделения Банка)

предупрежден (а), что в целях исполнения должностных обязанностей в АКБ «Энергобанк» (ОАО), мне будет предоставлен допуск к персональным данным физических лиц, клиентов, сотрудников Банка (конфиденциальной информации), которые могут содержать также сведения, составляющие банковскую и/или коммерческую тайну.

Настоящим признаю и обязуюсь придерживаться принципов:

- законности целей и способов обработки персональных данных,
- принципов разумности и добросовестности обработки персональных данных,
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных,
- соответствия обработки персональных данных моим полномочиям,
- 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 информационных систем персональных данных.
- приоритета сохранности персональных данных перед проведением рискованных операций.

Добровольно принимаю на себя обязательства:

1. Ни при каких условиях и никаким способом не передавать несанкционированно третьим лицам персональные данные и иные конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня персональные данные, либо документы, их содержащие, сообщать об этом непосредственному начальнику (руководителю), и в Управление Информационной безопасности.

3. Никогда не использовать персональные данные с целью получения выгоды, в корыстных целях, для проведения операций, не связанных с оказанием банковской услуги и исполнением Договора, на которые не давал согласия субъект персональных данных.

4. Выполнять требования комплекса РС СТО БР ИББС, Федерального закона № 152-ФЗ «О персональных данных», внутренних инструкций, Положения о персональных данных, порядке их обработки и обеспечения безопасности, а также иных нормативных правовых актов и внутренних локальных актов, регламентирующих вопросы защиты персональных данных.

5. В течение 3 (трех) лет после прекращения права на допуск к персональным данным (либо после увольнения из Банка) не разглашать и не передавать третьим лицам известные мне персональные данные.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен (а) к административной, дисциплинарной и/или уголовной ответственности в зависимости от характера нарушения, в соответствии с законодательством Российской Федерации.

(фамилия, инициалы)

« _____ » _____ 20__ г.

(подпись)

Приложение 8
«Разрешаю уничтожить»
Председатель Правления
АКБ «Энергобанк» (ОАО)
Д.И. Вагизов

«__» _____ 201_ г.

Акт об уничтожении персональных данных

Комиссия в составе:

	ФИО	Должность
Председатель	Вагизов Д.И.	Председатель Правления АКБ «Энергобанк» (ОАО)
Члены комиссии		

провела отбор электронных носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации: Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006 г., Стандарта Банка России СТО БР ИББС – 1.2.-2010, Положения «О персональных данных» АКБ «Энергобанк» (ОАО) информация, записанная на них в процессе эксплуатации, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего подлежит уничтожению _____ носителей/единиц хранения
(цифрами и прописью)

После утверждения акта перечисленные носители/единицы хранения сверены с записями в акте и на указанных носителях персональные данные уничтожены путем _____.

После утверждения акта перечисленные носители сверены с записями в акте и уничтожены путем

_____.
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Уничтоженные носители с книг и журналов учета списаны.

Председатель комиссии:

Члены комиссии:

_____ /	/
_____ /	/
_____ /	/
_____ /	/
_____ /	/
_____ /	/
_____ /	/
_____ /	/
_____ /	/
_____ /	/
_____ /	/
_____ /	/

Примечание:

1. Акт составляется отдельно на каждый тип носителей информации.
2. Акт составляется отдельно на каждый способ уничтожения носителей.
3. Все листы акта, а так же все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

Приложение 9.
Председателю Правления
АКБ «Энергобанк» (ОАО)
Вагизову Д.И.

от _____
(ФИО субъекта ПДн)

_____ (адрес регистрации субъекта ПДн)

_____ (паспортные данные субъекта ПДн)

ЗАПРОС

(о предоставлении доступа к персональным данным)

Мною, _____ (ФИО), «__» _____ г. (дата предоставления ПДн) в связи с осуществлением обязательств по договору

_____ (номер договора, его дата, условное словесное обозначение, либо сведения иным образом

_____ подтверждающие факт обработки персональных данных Банком)

в АКБ «Энергобанк» (ОАО) были предоставлены следующие персональные данные

Прошу предоставить возможность ознакомления с моими персональными данными в течение 30 (Тридцати) дней с даты подачи настоящего заявления, предварительно уведомив меня по телефону номер _____.

_____ (ФИО)

_____ (подпись)

_____ (дата)

Заполняется в случае подачи запроса представителем субъекта персональных данных.

_____, дата рождения _____,
(Фамилия, Имя, Отчество полностью)

_____ серия _____ № _____, выдан _____,
(наименование документа)

дата _____, проживающий(ая) по адресу: _____,
являясь представителем _____ и имеющий право на подачу запроса от его
(Ф.И.О. субъекта персональных данных)
имени на основании _____.

/ _____