УТВЕРЖДЕНО
приказом Генерального директора
КИТ Финанс Инвестиционный банк (ОАО)

от «24» июня 2013г. № 166

КИТ Финанс Инвестиционный банк
(Открытое акционерное общество)

Положение
об обработке персональных данных

КОД ДОКУМЕНТА № 1 – 2013

Санкт-Петербург

2013 год

Содержание

1. Сокращения и определения

В тексте настоящего Положения используются следующие сокращения и определения:

ИСПДн – информационная система персональных данных
ПДн – персональные данные

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Актуальные угрозы безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Банк – КИТ Финанс Инвестиционный банк (Открытое акционерное общество).

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Оператором для установления личности субъекта персональных данных.

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

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

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

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.

Оператор персональных данных/Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Ответственный работник – работник Банка, ответственный за организацию работы по обеспечению безопасности персональных данных в Банке, назначаемый приказом Генерального директора.

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

Положение – настоящее Положение об обработке персональных данных.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Специальные категории персональных данных - категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Субъект персональных данных – физическое лицо **–** клиент Банка, работник Банка.

Третьи лица – партнеры Банка, осуществляющие по поручению Банка обработку персональных данных субъектов персональных данных, содействующие в реализации трудовых отношений с работником Банка (обеспечивающие повышение квалификации, предоставляющие билеты, обеспечивающие бронирование гостиниц, предоставляющие визы), государственные уполномоченные органы, имеющие право доступа к персональным данным в силу характера осуществляемой ими деятельности и предоставленных законодательством Российской Федерации полномочий и т.п.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Уполномоченные органы по надзору выполнения требований законодательства – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и его территориальные органы в субъектах Российской Федерации, ФСТЭК России, ФСБ России.

Уполномоченный орган по защите прав субъектов персональных данных – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и его территориальные органы в субъектах Российской Федерации.

Уровень защищенности персональных данных - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Если иное прямо не указано, все сокращения и определения, указанные с заглавной буквы, имеют то же значение, что и сокращения и определения, написанные строчными буквами и наоборот.

2. Нормативные ссылки

Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных» (Федеральный закон «О персональных данных»);
- Указом Президента Российской Федерации от 06.03.1997г. №188 «Об утверждении перечня сведений конфиденциального характера»;
- Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены Постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119);
- Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждено Постановлением Правительства Российской Федерации от 15.09.2008г. № 687);
- Рекомендациями по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных (утверждены Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 19.08.2011 г. № 706);
- Иными нормативными правовыми актами, определяющими принципы и условия обработки персональных данных, а также требования к обеспечению безопасности персональных данных при их обработке.

3. Цели и область действия Положения

Настоящее Положение устанавливает принципы и условия обработки персональных данных, а также требования к обеспечению безопасности персональных данных при обработке с использованием средств автоматизации или без использования таких средств.

Действие Положения распространяется на все подразделения/работников Банка, осуществляющих обработку и обеспечивающих безопасность персональных данных.

Настоящее Положение должно быть доведено до каждого работника Банка, осуществляющего обработку персональных данных, под подпись в листе ознакомления. Личной подписью в листе ознакомления с настоящим Положением работник подтверждает, что он проинформирован о факте осуществления им обработки персональных данных, а также ознакомлен со всей совокупностью требований по обработке и обеспечению безопасности персональных данных, указанных в настоящем Положении.

Вновь принятый работник Банка, в должностные обязанности которого входит обработка персональных данных, при приме на работу должен быть проинформирован работниками Службы по работе с персоналом о факте осуществления им обработки персональных данных и требованиях по обработке и обеспечению безопасности персональных данных, указанных в настоящем Положении под подпись, а также ознакомлен при проведении первичного инструктажа работниками Управления информационной безопасности и контроля с применяемыми мерами по защите персональных данных.

Настоящее Положение определяет политику Банка в области обработки и обеспечения безопасности персональных данных и подлежит опубликованию доступными для Банка средствами.

Владельцем настоящего Положения является Департамент информационной безопасности и охраны, который несет ответственность за полноту и содержание документа, его соответствие действующей практике работы Банка, своевременную актуализацию, организацию и сопровождение процедуры согласования документа.

4. Принципы обработки персональных данных

Обработка персональных данных должна осуществляться на основе следующих принципов:

- обработка персональных данных должна осуществляться на законной основе;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей, не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- 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;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

5. Условия обработки персональных данных

Обработка персональных данных должна осуществляться с соблюдением принципов, указанных в п.2.1, и допускается в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных, форма такого согласия определяется внутренними нормативными документами Банка;

- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для осуществления прав и законных интересов Банка или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

6. Категории субъектов и категории персональных данных

Банк осуществляет обработку персональных данных следующих категорий субъектов:
- физических лиц, заключивших или намеревающихся заключить договор с Банком;
- работников Банка;
- работников\представителей юридических лиц, заключивших или намеревающихся заключить договор с Банком.

В информационных системах Банка обрабатываются категории персональных данных работников Банка необходимые для обеспечения трудовых отношений и иных непосредственно связанных с ними отношений в соответствии с трудовым законодательством и иными нормативными правовыми актами, содержащими нормы трудового права, персональные данные физических лиц (работников\представителей юридических лиц), заключивших или намеревающихся заключить договор с Банком, необходимые для исполнения договоров, осуществления банковских операций, формирования и предоставления информации, входящей в состав кредитных историй, противодействия легализации доходов, полученных преступным путем, и финансированию терроризма, выполнения требований законодательства Российской Федерации.

При наличии письменного согласия субъекта персональных данных или в установленных законодательством случаях, допускается обработка дополнительной следующей информации: фотографий, сканированных копий документов, а также сведений о судимости, обработка которых предусмотрена Указанием Центрального Банка РФ от 20 августа 2004 г. № 1492-У «О применении требований законодательства Российской Федерации о рынке ценных бумаг к руководителям и членам совета директоров кредитных организаций – профессиональных участников рынка ценных бумаг».

Форма Сообщения о согласии на обработку персональных данных приведена в Приложении № 11 Банковских правил для физических лиц.

7. Цели, действия, способы и сроки обработки персональных данных

Банк осуществляет обработку персональных данных с целью обеспечения трудовых отношений и иных непосредственно связанных с ними отношений в соответствии с трудовым законодательством и иными нормативными правовыми актами, содержащими нормы трудового права, исполнения договоров, заключенных с физическими лицами, осуществления банковских операций, формирования и предоставления информации, входящей в состав кредитных историй, противодействия легализации доходов, полученных преступным путем, и финансированию терроризма, выполнения требований законодательства Российской Федерации.

При обработке персональных данных Банк осуществляет следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

При обработке персональных данных Банк использует следующие способы обработки:
- с использованием средств автоматизации;
- без использования средств автоматизации.

Сроки обработки персональных данных должны определяться в соответствии со сроками:
- действия договоров с субъектами персональных данных;
- исполнения договорных обязательств субъектами персональных данных;
- исполнения постановлений судебных органов Российской Федерации;
- принятия решения Банком, либо контрагентом Банка о прекращении работы с задолженностью;
- прекращения деятельности (ликвидация) Банка как юридического лица, а также в случаях, предусмотренных Федеральным законом «О персональных данных».

8. Рассмотрение Банком обращений граждан (субъектов персональных данных) и уполномоченного органа по защите прав субъектов персональных данных

Требования и порядок обработки обращений граждан (субъектов персональных данных) и уполномоченного органа по защите прав субъектов персональных данных и иных уполномоченных органов федерального государственного надзора определены в Положении о реагировании на обращения субъектов персональных данных и Регламенте реагирования на обращения граждан (субъектов персональных данных) о выполнении их законных прав при обработке персональных данных.

9. Уведомление об обработке персональных данных

Порядок уведомления уполномоченного органа по защите прав субъектов персональных данных определен в Положении о реагировании на обращения субъектов персональных данных.

10. Обеспечение конфиденциальности персональных данных

В соответствии с Указом Президента Российской Федерации от 06.03.1997 г. №188 «Об утверждении перечня сведений конфиденциального характера», персональные данные относятся к сведениям конфиденциального характера.

Перечень должностей работников Банка, уполномоченных обрабатывать персональные данные утверждается приказом Генерального директора.

Работники Банка, уполномоченные обрабатывать персональные данные, обеспечивать безопасность персональных данных, а также иные лица, получившие доступ к персональным данным, обязаны соблюдать конфиденциальность персональных данных, не предоставлять их третьим лицам без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Договоры в рамках, которых осуществляется обработка, в том числе передача персональных данных третьим лицам должны содержать условия по обеспечению конфиденциальности персональных данных.

Передача персональных данных третьим лицам, должна осуществляться при условии обеспечения конфиденциальности и предотвращения несанкционированного доступа к персональным данным.

Проекты договоров, документов, типовых форм, технологических процессов обработки информации и т.п. в рамках, которых будет осуществляться обработка персональных данных должны быть согласованы с Ответственным работником за организацию работы по обеспечению безопасности персональных данных.

11. Обеспечение безопасности персональных данных

Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения безопасности персональных данных, а также Ответственного работника за организацию обработки персональных данных.

При обработке персональных данных Банк обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

11.1. Обеспечение безопасности персональных данных при автоматизированной обработке персональных данных

Для каждой информационной системы персональных данных исходя из актуальных угроз безопасности персональных данных, категорий персональных данных и количества субъектов, чьи персональные данные обрабатываются в информационных системах, должен быть определен уровень защищенности персональных данных и в соответствии с уровнем защищенности выполнены требования по защите персональных данных при их обработке в информационной системе.

Актуальные угрозы безопасности персональных данных при их обработке в информационных системах должны быть определены руководствуясь нормативными правовыми актами Федеральных органов исполнительной власти и Банка России, осуществляющих функции по выработке государственной политики и нормативно-правовому регулированию в области обеспечения безопасности персональных данных.

11.2. Обеспечение безопасности персональных данных, обрабатываемых без использования средств автоматизации

Обработка персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень работников Банка, осуществляющих обработку персональных данных либо имеющих к ним доступ. Фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы, не допускается.

Хранение материальных носителей должно осуществляться на условиях, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом (удаления, вымарывания), исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе. Уничтожение носителей, содержащих персональные данные, должно осуществляться посредством специализированного оборудования, исключающего восстановление уничтоженной информации.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации 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 персональные данные изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию Банка, или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена внутренними нормативными документами Банка, содержащими сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способах фиксации и составе информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию Банка, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию Банка.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) полученная в результате такого копирования копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

12. Контроль выполнения требований по обеспечению безопасности персональных данных

Контроль выполнения настоящих требований должен обеспечиваться Банком самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Контроль проводится не реже 1 раза в 3 года в сроки, определяемые Банком (ответственным работником за организацию работы по обеспечению безопасности персональных данных в Банке).

13. Ответственность

Работники Банка, получающие доступ к обрабатываемым персональным данным, несут персональную ответственность за обеспечение конфиденциальность полученной информации.

Лица, виновные в нарушении требований настоящего Положения, несут ответственность, предусмотренную законодательством Российской Федерации.