Политика обработки и обеспечения безопасности персональных данных в АО КИБ «ЕВРОАЛЬЯНС»

г. Иваново

2018 год

Оглавление

Принятые обозначения

Банк – АО КИБ «ЕВРОАЛЬЯНС».

ИБ – информационная безопасность.

ПДн – персональные данные.

ИСПДн – информационная система персональных данных.

Информационная система (ИС) – совокупность содержащейся в базе данных информации и обеспечивающих ее обработку информационных технологий и технических средств, принадлежащих Банку или эксплуатирующихся в его интересах.

СИБ – служба информационной безопасности Банка.

СКЗИ – средства криптографической защиты информации.

1. Назначение документа

1.1. Настоящая Политика обработки и обеспечения безопасности персональных данных в АО КИБ «ЕВРОАЛЬЯНС» (далее - Политика) определяет:

- категории субъектов персональных данных,
- цели обработки персональных данных в Банке,
- перечень персональных данных, обрабатываемых в Банке,
- общие принципы обработки персональных данных в Банке,
- права субъекта персональных данных и права Банка как оператора персональных данных,
- условия и порядок обработки персональных данных в Банке,
- защиту персональных данных физических лиц при их обработке, осуществляемой Банком,
- требования к обеспечению безопасности персональных данных в ИСПДн при их обработке,
- обучение сотрудников Банка по вопросам обеспечения безопасной обработки персональных данных,
- управление инцидентами в области защиты персональных данных,
- распределение ответственности сотрудников Банка в части обработки персональных данных.

1.2. Действие Политики распространяется на все структурные подразделения Банка.

2. Общие положения

2.1. Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2.2. Политика обязательна для ознакомления и исполнения всеми сотрудниками Банка.

2.3. Политика пересматривается по мере необходимости.

2.4. Сотрудники информируются обо всех изменениях в Политике и имеют доступ к наиболее актуальной версии документа.

2.5. Политика размещается на сайте Банка в свободном доступе.

3. Основные понятия

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

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;

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

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

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

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

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

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

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

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

4. Категории субъектов персональных данных. Цели обработки персональных данных. Перечень персональных данных, обрабатываемых в Банке

4.1. Банк осуществляетобработку персональных данных следующих категорий субъектов персональных данных:

- кандидатов на работу,
- сотрудников Банка,
- физических лиц, входящих в органы управления Банка,
- клиентов-физических лиц (владелец счета, открытого в Банке, заемщик, вкладчик, выгодоприобретатель и иные лица, пользующиеся финансовыми услугами Банка), в т.ч. потенциальных клиентов, представителей клиентов, уполномоченных представлять интересы клиентов,
- руководителей и главных бухгалтеров юридических лиц, являющихся клиентами Банка (владелец счета, открытого в Банке, заемщик),
- бенефициарных владельцев клиентов Банка,
- поручителей,
- залогодателей,
- физических лиц, заключивших с Банком гражданско-правовые договоры на оказание услуг Банку,
- работников партнеров, субподрядчиков, поставщиков и других юридических лиц, имеющих договорные отношения с Банком,
- посетителей Банка,
- контрагентов клиентов-физических лиц,

- иных физических лиц, выразивших согласие на обработку Банком их персональных данных,
- физических лиц, обработка персональных данных которых необходима Банку для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей.

4.2. В информационных системах Банка не осуществляется обработка персональных данных, относящихся к специальным категориям персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости. Обработка специальных категорий персональных данных может осуществляться только в установленных законодательством случаях и по согласованию со службой информационной безопасности Банка.

4.3. Обработка персональных данных Банком проводится в целях:

- осуществления банковских операций и сделок в соответствии с Уставом Банка и выданными Банку лицензиями на совершение банковских и иных операций,
- заключения с субъектами персональных данных любых договоров и их дальнейшего исполнения,
- предоставления субъекту персональных данных информации об оказываемых Банком услугах, для разработки новых услуг, информирования клиентов о предложениях Банка,
- ведения кадрового учета сотрудников Банка и кадрового делопроизводства, привлечения и отбора кандидатов на работу в Банк, регулирования трудовых и иных, непосредственно связанных с ними, отношений,
- формирования статистической и прочей отчетности, в том числе для предоставления в Банк России,
- осуществления Банком административно-хозяйственной деятельности (деятельности, направленной на текущее обеспечение деятельности Банка

товарно-материальными ценностями, организацию документооборота, эксплуатацию зданий, помещений, территорий, организацию рабочего процесса и т.п.),

- проведения Банком акций, опросов, исследований,
- выявления случаев мошенничества, хищения средств со счетов, иных противоправных действий, предотвращения таких противоправных действий в дальнейшем и локализации таких действий,
- осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей,
- в иных целях, указанных в согласии субъекта персональных данных на обработку его персональных данных.

4.4. Перечень персональных данных, в том числе специальных категорий персональных данных, обрабатываемых в Банке, определяется в соответствии с законодательством Российской Федерации и внутренними документами Банка с учетом целей обработки персональных данных, указанных выше, в соответствии с уведомлением об обработке персональных данных, направленных Банком в Роскомнадзор, и согласием клиента на обработку персональных данных.

4.5. Сроки обработки персональных данных определяются в соответствии со сроками действия договоров с субъектами персональных данных, согласиями на обработку персональных данных, а также иными требованиями законодательства и нормативными документами Банка России.

5. Принципы обработки персональных данных

5.1. Банк осуществляет обработку персональных данных на основе общих принципов:

- законности заранее определенных конкретных целей и способов обработки персональных данных,
- обеспечения надлежащей защиты персональных данных,

- соответствия целей обработки персональных данных целям, заявленным при сборе персональных данных,
- соответствия объема, характера и 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 баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой,
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки,
- уничтожения или обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом или договором,
- обеспечения конфиденциальности и безопасности обрабатываемых персональных данных,
- добросовестности Банка как оператора персональных данных.

6. Права субъекта персональных данных

6.1. Субъект персональных данных имеет право:

- получать информацию, касающуюся обработки его персональных данных, в порядке, форме и сроки, установленные законодательством о персональных данных,
- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными, не являются необходимыми для заявленной цели обработки или используются в целях, не заявленных ранее при предоставлении субъектом персональных данных согласия на обработку персональных данных,

- отозвать свое согласие на обработку персональных данных.

6.2. Право субъекта персональных данных на получение информации, касающейся обработки его персональных данных, может быть ограничено в случаях, установленных Федеральным законом «О персональных данных».

6.3. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Банк вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Федеральном законе «О персональных данных».

7. Права Банка как оператора персональных данных

7.1. Банк как оператор персональных данных имеет следующие права:

- обрабатывать персональные данные субъекта персональных данных в соответствии с заявленной целью,
- требовать от субъекта персональных данных предоставления достоверных персональных данных, необходимых для исполнения договора, оказания услуги, идентификации субъекта персональных данных, а также в иных случаях, предусмотренных законодательством,
- ограничить доступ субъекта персональных данных к его персональным данным в случае, если обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц, а также в иных случаях, предусмотренных законодательством Российской Федерации,
- поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством,
- обрабатывать общедоступные персональные данные физических лиц,

- осуществлять обработку персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации.

8. Обработка персональных данных Банком

8.1. Обработка персональных данных Банком осуществляется с согласия субъекта персональных данных на обработку его персональных данных, за исключением случаев, установленных законодательством.

8.2. Использование персональных данных Банком возможно только в соответствии с целями обработки персональных данных.

8.3. Обработка персональных данных в Банке производится как с применением средств автоматизации, так и без их применения.

8.4. При обработке персональных данных Банк обязуется обеспечить точность персональных данных, их достаточность и принять меры по удалению или уточнению неполных или неточных данных.

8.5. Банк вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, на основании заключаемого с этим лицом договора. В договоре определяются:

- перечень действий (операций) с персональными данными, которые будут совершаться третьим лицом, осуществляющим обработку персональных данных,
- цели обработки персональных данных,
- обязанность третьего лица соблюдать конфиденциальность персональных данных и обеспечивать их безопасность при обработке, а также требования к защите обрабатываемых персональных данных в соответствии с действующим законодательством.

8.6. Лицо, осуществляющее обработку персональных данных по поручению Банка – оператора персональных данных, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

8.7. В случае, если Банк поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Банк. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед Банком.

8.8. Банк осуществляет передачу персональных данных государственным органам в рамках их полномочий в соответствии с законодательством Российской Федерации.

8.9. Доступ к обрабатываемым персональным данным предоставляется только тем сотрудникам Банка, которым он необходим в связи с исполнением ими своих должностных обязанностей и с соблюдением принципов персональной ответственности.

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

8.11. Обработка персональных данных осуществляется с соблюдением конфиденциальности, под которой понимается обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством.

8.12. Банк обеспечивает конфиденциальность персональных данных субъекта персональных данных со своей стороны, со стороны своих аффилированных лиц, со стороны своих сотрудников, имеющих доступ к персональным данным физических лиц, а также обеспечивает использование персональных данных вышеуказанными лицами исключительно в целях, соответствующих закону, договору или соглашению, заключенному с субъектом персональных данных.

8.13. Банк может осуществлять трансграничную передачу персональных данных в ходе своей деятельности в соответствии с требованиями Федерального закона «О персональных данных».

9. Защита персональных данных

9.1. Защита персональных данных — это комплекс мер технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к субъекту персональных данных.

9.2. Защита ПДн является обязанностью Банка как оператора персональных данных. Банк обеспечиваетдолжный уровень защиты обрабатываемых им персональных данных, самостоятельно определяя состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и другими федеральными законами.

9.3. В Банке принимаются следующие меры по обеспечению выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», в области обработки персональных данных:

- в Банке назначается сотрудник, ответственный за организацию обработки персональных данных,
- издаются политики, положения и другие внутренние документы Банка по вопросам обработки персональных данных,
- применяютсяправовые, организационные и технические меры по обеспечению безопасности персональных данных,
- осуществляется внутренний контроль и аудит соответствия обработки персональных данных в Банке требованиям законодательства о персональных данных и внутренних документов,
- сотрудник, ответственный за организацию обработки персональных данных в Банке,проводит ознакомление и/или обучение сотрудников Банка, непосредственно осуществляющих обработку персональных данных, положениям законодательства о персональных данных и внутренним документам по вопросам обработки персональных данных.

9.4. Банк принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных, в частности:

- определяются угрозы безопасности персональных данных при их обработке в информационных системах,
- применяются организационные меры и технические средства по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, направленные на нейтрализацию актуальных угроз безопасности персональных данных,
- проводятся мероприятия по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер,
- обеспечивается возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним,
- устанавливаются правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, регистрация и учет действий, совершаемых с персональными данными в информационной системе персональных данных,
- осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

10. Требования к обеспечению безопасности персональных данных в информационных системах персональных данных

10.1. Безопасность персональных данных в ИСПДн в Банке обеспечивается комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации, подобранным в зависимости от уровня защищенности ИСПДн.

10.2. Комплекс мер по обеспечению безопасности персональных данных в ИСПДн Банка предусматривает, в том числе:

- защиту относящейся к персональным данным информации от искажения, фальсификации, переадресации, несанкционированного уничтожения;

- доступ сотрудника Банка только к тем ресурсам ИСПДн, которые необходимы ему для исполнения должностных обязанностей;
- контроль (мониторинг) обработки персональных данных;
- работу в ИСПДн только авторизованных пользователей;
- контроль, направленный на исключение возможности совершения злоумышленных действий;
- восстановление информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- управление конфигурацией информационной системы и системы защиты персональных данных;
- учет и защиту машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- обеспечение целостности информационной системы и персональных данных;
- контроль (анализ) защищенности персональных данных;
- выявление инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и(или) к возникновению угроз безопасности персональных данных, и реагирование на них.

10.3. Сотрудники Банка, в том числе администраторы автоматизированных систем и средств защиты информации, не обладают полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения информации в ИСПДн, а также проведения в них несанкционированных операций.

10.4. На всех сотрудников Банка, в том числе и сотрудников, осуществляющих обработку персональных данных в ИСПДн, наложено обязательство соблюдения документов Банка по информационной безопасности.

10.5. Передача персональных данных по телекоммуникационным каналам и линиям связи между подразделениями организации и внешними организациями осуществляется с использованием сертифицированныхСКЗИ или иных защитных механизмов.

10.6. Передача персональных данных между подразделениями Банка по телекоммуникационным каналам и линиям связи осуществляется только при обеспечении защиты персональных данных с помощью защитных мер, механизмов и средств.

10.7. В Банке определена система контроля доступа, позволяющая осуществлять контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации ИСПДн.

10.8. В Банке ведется логирование действий в ИСПДн.

11. Обучение сотрудников аспектам обеспечения безопасности персональных данных

11.1. Сотрудники Банка, допущенные к работе с персональными данными и в ИСПДн, в обязательном порядке проходят соответствующий инструктаж по обеспечению безопасности персональных данных и информационной безопасности, в целом.

12. Управление инцидентами

12.1. Сотрудники Банка обязаны уведомлять СИБ обо всех инцидентах, связанных с обработкой персональных данных.

12.2. Каждый выявленный инцидент рассматривается в отдельном порядке, при участии непосредственного руководителя сотрудника, сотрудника СИБ и, при необходимости, других уполномоченных сотрудников и руководства Банка в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

13. Распределение ответственности

13.1. Ответственность за организацию и контроль выполнения требований по обеспечению безопасности персональных данных возлагается на сотрудника, ответственного за организацию и контроль обеспечения защиты информации.

13.2. Ответственность за своевременное и корректное реагирование на запросы по персональным данным возлагается на руководителей подразделений,в которые поступил запрос.

13.3. Ответственность за выполнение сотрудниками Банка требований настоящей Политики возлагается непосредственно на сотрудников и руководителей функционального подразделения, в котором они работают. На основании Трудового кодекса РФ сотрудники, нарушающие требования настоящей Политики, могут быть подвергнуты дисциплинарным взысканиям.

13.4. Лица, виновные в нарушении норм, регулирующих обработку персональных данных и защиту обрабатываемых в Банке персональных данных, несут предусмотренную законодательством Российской Федерации гражданско-правовую, административную и иную ответственность.

13.5. Контроль исполнения данной Политики возлагается на сотрудника, ответственного за организацию обработки персональных данных.