Приложение № 1

УТВЕРЖДЕНО

Приказом Председателя Правления ПАО «БИНБАНК»
№ 75 от « 28 »ноября 2016 г.

П О Л И Т И К А

Защиты персональных данных ПАО «БИНБАНК»

Москва, 2016

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

1.1. С целью поддержания деловой репутации и обеспечения выполнения норм федерального законодательства, согласно требованиям Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Банк определяет важнейшими задачами: обеспечение законности обработки персональных данных в бизнес-процессах Банка и обеспечение надлежащего уровня безопасности обрабатываемых в Банке персональных данных.

1.2. Настоящий документ «Политика защиты персональных данных ПАО «БИНБАНК»» (далее - Политика) направлен на определение общих принципов и условий Публичного Акционерного Общества «БИНБАНК» (далее - Банк) в области обработки персональных данных (далее - ПДн), формулировки целей и задач в данной области, определения отношений, связанных с обработкой ПДн, осуществляемых Банком, распределения основных ролей и ответственности, и формализацию процесса управления защитой персональных данных в Банке в рамках обеспечения соблюдения законодательства Российской Федерации. Настоящая Политика является документом второго уровня по отношению к Политике информационной безопасности ПАО «БИНБАНК». Политика разработана в соответствии с законодательством РФ о ПДн и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн, в том числе при их обработке в информационных системах ПДн (далее - ИСПДн).

1.3. Областью действия документа являются действия, относящиеся к процессу управления защитой ПДн для всех процессов и информационных систем, относящихся к ИСПДн и все действия, связанные с обработкой (сбором, хранением, передачей, уничтожением и т.д.) ПДн. Настоящая Политика распространяется на всех работников Банка, осуществляющих обработку ПДн и обеспечивающих безопасность ПДн, а также является обязательным документом для исполнения всеми работниками Банка

1.4. Процесс управления защитой ПДн направлен на противодействие угрозам и уязвимостям, связанным с реализацией несанкционированного доступа с целью нарушения конфиденциальности или целостности ПДн, а также нарушения законных прав субъекта ПДн.

1.5. Требования настоящей Политики могут детализироваться, при необходимости, иными внутренними нормативными документами Банка.

1.6. Настоящая Политика подлежит опубликованию на сайте Банка www.binbank.ru с предоставлением неограниченного доступа к ней, как документ, определяющий политику Банка в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн.

2. ОПРЕДЕЛЕНИЯ ДОКУМЕНТА

2.1. Основные понятия, приведенные в настоящей Политике, полностью соответствуют понятиям, указанным в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее - ФЗ «О персональных данных»), а также в «Политики информационной безопасности ПАО «БИНБАНК»». Термины и определения, специфические для данной Политики, указаны в разделе 2.2.

2.2. Термины, определения и сокращения

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Персональные данные, сделанные общедоступными субъектом персональных данных – обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием

электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Банк – Публичное Акционерное Общество «БИНБАНК» (ПАО «БИНБАНК»)

ИСПДн – информационная система, обрабатывающая персональные данные

ПДн – персональные данные

РФ – Российская Федерация

ФЗ – Федеральный закон

ФЗ «О персональных данных» – Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»

3. ЦЕЛИ И ЗАДАЧИ

3.1. Основная цель разработки настоящего документа – определение политики Банка в отношении обработки ПДн и обеспечения безопасности ПДн.

3.2. Основной задачей Политики является определение высокоуровневых правил и требований к деятельности в области обработки и обеспечения безопасности ПДн.

4. РОЛИ И ОТВЕТСТВЕННОСТЬ

4.1. В рамках процесса обеспечения безопасности ПДн выделяются следующие роли:

– Субъект ПДн – физическое лицо, чьи ПДн обрабатываются Банком и ПДн которого необходимо защищать.

– Работник Банка, участвующий (допущенный) в обработке ПДн – работник Банка, которому в рамках выполнения своих должностных обязанностей стали известны ПДн, обрабатывающиеся в Банке, и который обеспечивает их конфиденциальность и безопасность.

– Администратор ИСПДн – работник Банка, который в рамках выполнения своих должностных обязанностей обслуживает, поддерживает и управляет требуемым составом технических средств, обеспечивающих обработку ПДн.

– Куратор, ответственный за обеспечение безопасности ПДн – руководитель службы безопасности, который в рамках выполнения своих должностных обязанностей осуществляет контроль за обеспечением выполнения требований в области обработки ПДн.

– Ответственный за организацию обработки и обеспечение безопасности ПДн – руководитель, ответственный за организацию процессов обработки и защиты ПДн, назначается Приказом Президента Банка.

4.2. В должностных инструкциях работников Банка и соглашениях с третьими сторонами должны быть определены права и обязанности в соответствии с требованиями ФЗ «О персональных данных», для каждого участвующего в процессе обработки ПДн (Банка, как оператора ПДн, работников, участвующих в обработке ПДн, субъекта ПДн).

4.3. Банк разрабатывает и поддерживает в актуальном состоянии порядок (регламент) обработки обращений субъектов ПДн, определяющий обязанности Банка при обращении к нему субъекта ПДн либо при получении запроса субъекта ПДн или его представителя, а также уполномоченного органа по защите прав субъектов ПДн, а также действия в случае получения таких запросов.

4.4. В случае нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Банку, клиентам, работникам и посетителям материального или иного ущерба виновные лица несут ответственность в соответствии с законодательством РФ:

– дисциплинарную, вплоть до расторжения трудового договора (ст. 81, 192 ТК РФ);
– административную (ст. 5.39, 13.11, 13.14 КоАП РФ);
– уголовную, при наличии состава преступления (ст. 137, 272 УК РФ).

5. ОСНОВНЫЕ ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Принципы обработки персональных данных

5.1.1. Обработка ПДн в Банке осуществляется на основе следующих принципов:

– Банк осуществляет обработку ПДн с соблюдением принципов, правил и в случаях, предусмотренных ФЗ «О персональных данных», с учетом защиты интересов сторон процесса обработки;

– обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;

– не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только ПДн, которые отвечают целям их обработки;

– содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки;

– при обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Банк принимает необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

– хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;

– обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

– обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, в целях осуществления банковской деятельности не допускается.

5.2. Категории, состав и цели обработки персональных данных

5.2.1. В целях выполнения основной деятельности Банк обрабатывает ПДн субъектов, включая, но не ограничиваясь:

– физические лица, состоящие в договорных отношениях с Банком или планирующие заключить договорные отношения (клиенты, работники, кандидаты на замещение вакантных должностей);

– аффилированные лица Банка (участники, члены Совета директоров Банка);

– физические лица, являющиеся представителями или работниками юридических лиц, состоящие в договорных отношениях или планирующие заключить договорные отношения с Банком;

– выгодоприобретатели;

– посетители зданий и сооружений Банка и не являющиеся клиентами Банка.

5.2.2. Цели и правовое основание обработки ПДн, состав и содержание ПДн, а также категории субъектов ПДн, чьи данные обрабатываются в Банке, зафиксированы во внутренних документах Банка, и подлежат обновлению в случае их изменения.

5.2.3. Состав ПДн должен соответствовать принципу их достаточности для достижения целей обработки. ПДн не должны быть избыточными по отношению к целям обработки.

5.3. Условия обработки персональных данных

5.3.1. Банк самостоятельно определяет состав, и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей по обработке ПДн, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено федеральными законами.

5.3.2. Банк осуществляет обработку ПДн, как без использования средств автоматизации, так и автоматизированную обработку ПДн, с передачей и без передачи по внутренней сети Банка, с передачей и без передачи в сети общего пользования Интернет.

5.3.3. Банк в ходе своей деятельности на основании договора предоставляет и (или) поручает обработку ПДн третьим лицам с согласия субъекта ПДн, если иное не предусмотрено федеральным законом. При этом, условием такого предоставления и (или) поручения является обязанность третьего лица, осуществляющего обработку ПДн по поручению Банка, соблюдать принципы и правила обработки ПДн, конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке.

5.3.4. Банк в ходе своей деятельности имеет право осуществлять трансграничную передачу ПДн на территорию иностранных государств органам власти иностранного государства, иностранным физическим или юридическим лицам. При этом вопросы обеспечения адекватной защиты прав субъектов ПДн и обеспечения безопасности их ПДн при трансграничной передаче являются наивысшим приоритетом для Банка, решение которых реализуется в соответствии с законодательством РФ по вопросам обработки ПДн.

5.3.5. Банк осуществляет аудит соответствия обработки ПДн ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, настоящей Политике и другим внутренним документам Банка в отношении обработки и защите ПДн

5.3.6. Обработка ПДн Банком осуществляется при наличии согласия в письменной форме субъекта ПДн в следующих случаях:

– для информационного обеспечения, создания общедоступных источников ПДн (справочники, адресные книги);

– для установления личности субъекта ПДн – при обработке сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн);

– для осуществления трансграничной передачи ПДн на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн;

– для принятия решений на основании исключительно автоматизированной обработки ПДн.

5.3.7. Письменная форма согласия должна оформляться в соответствии с требованиями, предъявляемыми к ней ФЗ «О персональных данных».

5.3.8. Сроки обработки ПДн (сроки хранения) должны быть определены в соответствие с целями обработки ПДн и зафиксированы для каждой категории субъектов ПДн.

5.3.9. Хранение ПДн должно осуществляться Банком в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн. Сроки хранения также могут устанавливаться договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, «Перечнем типовых управленческих документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», исковой давностью и иными требованиями законодательства и нормативными документами Банка России.

5.4. Обеспечение безопасности ПДн

5.4.1. ПДн, обрабатываемые в Банке, должны обладать уровнем конфиденциальности не ниже данных, отнесенных к Банковской тайне, а также к ним могут применяться я и другие характеристики безопасности. В частности, к таким характеристикам относятся: целостность, доступность, неотказуемость, учетность (подконтрольность), аутентичность (достоверность), адекватность

5.4.2. Банк реализует кадровую политику (тщательный подбор персонала и мотивация), позволяющую исключить или минимизировать возможность нарушения безопасности ПДн своими работниками.

5.4.3. ПДн могут иметь различные формы представления (бумажная, электронные файлы/документы, записи и поля записей баз данных, электромагнитные волны и поля, излучения и т.д.), каждая из которых связана с различными ресурсами ИСПДн.

5.4.4. Обработка ПДн в любой форме представления должна обеспечивать безопасность ПДн и определять информацию о методах и средствах обеспечения этой безопасности.

5.4.5. Предлагаемые меры по обеспечению безопасности ПДн (в том числе, для ИСПДн) должны быть спланированы так, чтобы был результат их применения, мог быть измеряем и оценен.

5.4.6. Неотъемлемой частью работ по защите ПДн должна являться оценка эффективности системы защиты ПДн.

5.4.7. С целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн должны быть определены требования, мероприятия по обеспечению безопасности и процедуры для постоянного контроля использования систем обработки и защиты ПДн (в том числе в ИСПДн), а результаты контроля должны регулярно анализироваться.

6. ЗАКЛЮЧЕНИЕ

6.1 Документ разработан на основе:

– ФЗ «О персональных данных» и соответствующих нормативных актах РФ;

– Политики информационной безопасности ПАО «БИНБАНК».

6.2 Контроль над реализацией настоящей частной политики лежит на Ответственном за организацию обработки и обеспечение безопасности ПДн.

6.3 Ответственность за реализацию настоящей частной политики лежит на Кураторе, ответственном за обеспечение безопасности ПДн.

6.4 Настоящая документ будет регулярно пересматриваться – не реже 1 раза в 2 года либо при возникновении условий, оказывающих влияния на положения документа (по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения безопасности персональных данных, по результатам проведения внутренних аудитов и других контрольных мероприятий).