

УТВЕРЖДАЮ
Председатель Правления
ПАО «Бест Эффортс Банк»
И. Б. Ионова
«30» июня 2017 г.

**ПОЛИТИКА
О ПОРЯДКЕ ОБРАБОТКИ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
(ВКЛЮЧАЮЩАЯ СВЕДЕНИЯ О РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К
ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ)**

Москва 2017

Оглавление

1. Общие положения	3
2. Список терминов и определений.....	3
3. Субъекты персональных данных.....	4
4. Цели обработки персональных данных.....	5
5. Условия обработки персональных данных	5
6. Сведения о реализуемых требованиях к защите персональных данных.....	6
7. Ответственность за разглашение персональных данных	8
8. Заключительные положения	9

1. Общие положения

Настоящая Политика разработана на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" и других нормативно-правовых актов Российской Федерации.

Настоящая Политика устанавливает порядок приема, получения, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, учета документов, содержащих сведения, отнесенные к персональным данным субъектов персональных данных ПАО «Бест Эффортс Банк» (далее Банк) с использованием средств автоматизации или без использования таких средств.

Целью настоящей Политики является защита персональных данных субъектов персональных данных Банка от несанкционированного доступа и разглашения, неправомерного их использования или утраты. Персональные данные являются конфиденциальной, строго охраняемой информацией.

Настоящая Политика распространяется на все подразделения Банка.

2. Список терминов и определений

Банк - Публичное акционерное общество «Бест Эффортс Банк».

Персональные данные - 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.

Субъект персональных данных - физическое лицо, которое прямо или косвенно определено или определяется с помощью персональных данных.

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не

допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

3. Субъекты персональных данных

3.1 Банком осуществляется обработка персональных данных следующих категорий субъектов персональных данных:

- клиенты Банка: физические лица, включая индивидуальных предпринимателей, их представители, выгодоприобретатели (физические лица) и бенефициарные владельцы;
- учредители/участники/акционеры (физические лица), представители, бенефициарные владельцы и выгодоприобретатели (физические лица) клиентов Банка - юридических лиц;
- физические лица, с которыми Банк состоит или состоял в трудовых отношениях;
- физические лица, с которыми Банк состоит или состоял в гражданско-правовых отношениях; физические лица, входящие в органы управления Банка;
- представители Банка - физические лица, представляющие интересы Банка во всех регионах Российской Федерации на основании доверенности;
- физические лица, являющиеся кандидатами на работу;
- акционеры Банка - физические лица, владельцы обыкновенных и привилегированных акций Банка;
- физические лица, предоставившие персональные данные посредством информационно-телекоммуникационной сети "Интернет" для проведения упрощенной идентификации.

- физические лица, осуществлявшие проход на территорию Банка, на которой осуществляется пропускной режим;
- иные физические лица, выразившие согласие на обработку Банком их персональных данных или физические лица, обработка ПД которых необходима Банку для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей.

4. Цели обработки персональных данных

4.1 Обработка персональных данных клиентов Банка осуществляется с целью:

- выполнения предусмотренных Уставом Банка и лицензией Банка России банковских операций;
- выполнения предусмотренных Уставом Банка и лицензиями Банка России на осуществление брокерской, дилерской и депозитарной деятельности;
- осуществления Банком Административно-хозяйственной деятельности;
- подбора персонала, содействия работникам в трудоустройстве, обучения и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- поручения физическим лицам представлять интересы Банка на основании доверенности во всех регионах Российской Федерации;
- ведения реестра акционеров во исполнение статьи 44 Федерального закона от 26.12.1995г. № 208-ФЗ «Об акционерных обществах»;
- проведения Банком упрощенной идентификации клиентов Банка или клиентов иных лиц, предоставивших персональные данные в соответствии с требованиями Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» при заключении договора о брокерском обслуживании, договора доверительного управления ценными бумагами, и/или депозитарного договора.

5. Условия обработки персональных данных

5.1 Обработка персональных данных осуществляется с согласия субъектов персональных данных.

5.2 При обработке персональных данных обеспечена их конфиденциальность, т.е. созданы условия, не допускающие их распространения без согласия субъекта персональных данных, за исключением случаев, когда персональные данные относятся к обезличенным или общедоступным.

5.3 В случае если Банк на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

5.4 В соответствии с Указом Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», персональные данные относятся к конфиденциальной информации. Банком осуществляется документальное оформление перечня сведений конфиденциального характера. Перечень сведений конфиденциального характера утвержден соответствующим внутренним приказом Председателя Правления Банка.

5.5 Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их

обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не предусмотрено законодательством Российской Федерации.

5.6 Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только при условии предварительного согласия субъекта персональных данных.

5.7 Трансграничная передача персональных данных (передача через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства) осуществляется только при наличии письменного согласия субъекта персональных данных.

5.8 Создание общедоступных источников персональных данных Банком не осуществляется.

6. Сведения о реализуемых требованиях к защите персональных данных.

6.1 Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности Банка.

6.2 Организация работ по обеспечению безопасности персональных данных осуществляется руководством Банка.

6.3 Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах Банка, приказом Председателя Правления назначается должностное лицо, ответственное за обеспечение безопасности персональных данных.

6.4 Для выбора и реализации методов и способов защиты информации может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

6.5 Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе управленческой и производственной деятельности Банка.

6.6 Банк при обработке персональных данных принимает необходимые организационные и технические меры, в том числе использует шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий в соответствии с требованиями к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, установленными Правительством Российской Федерации.

6.7 Использование и хранение биометрических персональных данных вне информационных систем персональных данных осуществляются только на таких материальных носителях информации и с применением технологий хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

6.8 Мероприятия по защите персональных данных делятся на внутреннюю и внешнюю защиту.

«Внутренняя защита» включает организационно-технические мероприятия, регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководством и специалистами Банка.

Для «Внешней защиты» конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

6.9 Для защиты персональных данных в Банке применяются следующие принципы и правила:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключается бесконтрольное использование защищаемой информации;
- знание сотрудниками требований нормативно-методических документов по защите персональных данных;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится соответствующая вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа сотрудниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- защита паролями доступа персональных компьютеров, на которых содержатся персональные данные.

6.10 Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

6.11 Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Банка, посетители, сотрудники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в управлении кадрами, управлении бухгалтерского учета, финансов и прогнозирования, других подразделений, использующих персональные данные.

6.12 Для защиты персональных данных соблюдается ряд мер организационно-технического характера:

- порядок приема, учета и контроля деятельности посетителей;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

6.13 При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", Банк обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Федеральном законе «О персональных данных».

7. Ответственность за разглашение персональных данных

7.1 Персональная ответственность является одним из главных требований к организации функционирования системы защиты персональных данных и обязательным условием обеспечения эффективности функционирования данной системы.

7.2 Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3 Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5 Каждый сотрудник Банка, получающий для работы конфиденциальный документ, несет личную ответственность за сохранность носителя и конфиденциальность полученной информации.

7.6 Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому субъекту персональных данных, возможность ознакомления с документами и материалами, если иное не предусмотрено законом.

7.7 Неправомерный отказ в предоставлении собранных в установленном порядке персональных данных, либо несвоевременное их предоставление в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного наказания в порядке установленном Кодексом Российской Федерации об административных правонарушениях.

7.8 В соответствии с Гражданским кодексом РФ лица, незаконными методами получившие информацию, составляющую персональные данные, обязаны возместить причиненные убытки; такая же обязанность возлагается и на работников, не обладающих правом доступа к персональным данным.

7.9 Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное соби́рание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения влечет наложение наказания в порядке, предусмотренном Уголовным кодексом РФ.

7.10 Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

8. Заключительные положения

8.1. Иные права и обязанности Банка как оператора персональных данных определяются законодательством Российской Федерации в области персональных данных.

8.2. Настоящая Политика подлежит обязательному опубликованию на официальном сайте Банка в соответствии с федеральным законом «О персональных данных».