



УТВЕРЖДЕНО:

Решением Совета директоров

КБ «Новый век» (ООО)

от «31» января 2018 г. № 6

Председатель Совета директоров

_____ **Н.М. Артемов**

М.П.

ПОЛИТИКА

Коммерческого Банка «Новый век» (Общество с Ограниченной Ответственностью)

в отношении обработки персональных данных

Москва

2018г.

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее-Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ « О персональных данных», а также иных нормативно - правовых актов Российской Федерации в области защиты персональных данных (далее - ПДн), которые Коммерческий банк «Новый век» (Общество с Ограниченной Ответственностью) (далее - Банк) может получить от субъекта ПДн, являющегося стороной по договору на оказание банковских услуг, иному гражданско - правовому договору, а также субъекта ПДн, состоящего с Банком в отношениях, регулируемых трудовым законодательством (далее-Работника).

1.2. Положения настоящей Политики являются основой для организации работы по обработке ПДн Банком, в том числе, для разработки внутренних нормативных документов и локальных актов Банка, регламентирующих процесс обработки ПДн.

1.3. Действующая редакция Политики на бумажном носителе хранится по адресу:
115093, г. Москва, ул. Щипок, д. 4, стр. 1

Электронная версия действующей редакции Политики общедоступна на сайте Банка в сети Интернет: www.newbank.ru

1.4. Банк до начала обработки ПДн, согласно статьи 22 Федерального Закона №152-ФЗ осуществил уведомление Уполномоченного органа по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн. Банк добросовестно и в соответствующий срок осуществляет актуализацию сведений, указанных в уведомлении.

2. Основные понятия и определения

2.1. Для целей настоящей Политики используются следующие понятия и определения:

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн (для целей настоящей Политики Банк является Оператором);

Обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

Клиент - физическое лицо, индивидуальный предприниматель, а также физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, заключившее или намеревающееся заключить с Банком договор на оказание услуг или которое заключило с Банком договор на оказание услуг, включая получение услуг путем присоединения к условиям публичного договора, и ПДн которого переданы Банку;

Конклюдентное действия — согласие лица, выражающее его волю установить правоотношение (например, совершить сделку), но не в форме устного или письменного волеизъявления, а поведением, по которому можно сделать заключение о таком намерении.

Распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц;

Работник - физическое лицо, заключившее с Банком трудовой договор;

Автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники;

Предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

Блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн (далее - ИСПДн) и (или) в результате которых уничтожаются материальные носители ПДн;

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

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

Трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, физическому или юридическому лицу.

3. Правовые основания обработки ПДн

3.1. Политика Банка в области обработки ПДн определяется в соответствии со следующими нормативно-правовыми актами РФ:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Налоговым кодексом Российской Федерации;
- Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 02.12. 1990г. №395-1 «О банках и банковской деятельности»;
- Федеральным законом от 30.12.2004г. №218-ФЗ «О кредитных историях»;
- Федеральным законом от 07.08.2001 N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федеральным законом от 27.06.2011г. №161-ФЗ «О национальной платежной системе»;
- Постановлением Правительства России от 01.11.2012года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Банка России от 24. 08. 2016г. №552-П «О требованиях к защите информации в платежной системе Банка России»;
- Стандартом Банка России СТО БР ИББС-1.0-2014г. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»;
- Положением Банка России от 09.06.2012г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля над соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»;
- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Федеральной службы безопасности России от 10.07.2014г. № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

4. Принципы и условия обработки ПДн

4.1. Обработка ПДн осуществляется Банком в соответствии с требованиями Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятых в соответствии с ним иных нормативных правовых актов, регулирующих вопросы обработки и защиты ПДн. При обработке ПДн Оператор придерживается принципов, установленных законодательством РФ в области ПДн.

4.2. Банк осуществляет обработку ПДн после получения согласия субъекта на обработку его ПДн.

4.3. Субъект ПДн выражает согласие на обработку его ПДн в форме конклюдентного действия в случае предоставления данных документа, удостоверяющего личность, для прохода на территорию Банка.

4.4. Принципы обработки ПДн:

- обработка ПДн осуществляется на законной и справедливой основе;
- обработка ПДн ограничивается 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 соответствуют заявленным целям обработки и не являются избыточными по отношению к заявленным целям их обработки;
- при обработке ПДн обеспечивается их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки. Принимаются необходимые меры по удалению или уточнению неполных или неточных данных;
- хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки, если срок хранения ПДн не установлен федеральным законом. Обрабатываемые ПДн по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом, подлежат уничтожению либо обезличиванию.

4.5. Обработка ПДн Банком включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение ПДн.

5. Цели обработки ПДн

5.1. Банк осуществляет обработку ПДн в целях:

- соблюдения действующего законодательства Российской Федерации;
- идентификации лиц, обратившихся в Банк для получения банковских услуг;
- осуществления банковских операций и сделок в соответствии с Уставом Банка и выданными Банку лицензиями на совершение банковских и иных операций, а также выполнение иных договоров гражданско-правового характера;
- исполнения условий трудовых договоров, заключенных между Банком и работниками Банка, а также иными лицами;
- предоставления субъекту ПДн информации об оказываемых Банком услугах, о разработке новых продуктов и услуг;
- ведения бухгалтерского, налогового, управленческого, кадрового и воинского учета;
- формирования и предоставления в соответствующие органы необходимой статистической, бухгалтерской, налоговой и иной отчетности по установленным формам;

— ведения документооборота, информационного взаимодействия с органами государственной власти.

5.2. Для достижения перечисленных целей Банк прибегает к обработке ПДн следующих субъектов:

- работников, состоящих в трудовых отношениях с Банком;
- физических лиц, являющихся кандидатами на вакантные должности;
- физических лиц, являющихся родственниками работников Банка;
- физических лиц, обратившихся для получения услуг Банка;
- физических лиц с целью прохода на территорию Банка;
- физических лиц, состоящих в договорных и иных гражданско-правовых отношениях с Банком;
- физических лиц, входящих в органы управления Банка;
- физических лиц, представляющих интересы клиентов Банка;
- физических лиц, являющихся пользователями сайта Банка и услуг, предоставляемых на нем;
- физические лица, приобретшие или намеревающиеся приобрести услуги Банка, услуги третьих лиц при посредничестве Банка или не имеющие с Банком договорных отношений при условии, что их ПДн включены в автоматизированные системы Банка в связи с оказанием Банком услуг своим клиентам, и обрабатываются в соответствии с законодательством РФ о ПДн;

— иные физические лица, выразившие согласие на обработку Банком их ПДн или физические лица, обработка ПДн которых необходима Банку для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на Банк функций, полномочий и обязанностей.

5.3. Для указанных категорий субъектов могут обрабатываться: фамилия, имя, отчество; год, месяц, дата рождения; место рождения, адрес; семейное положение; социальное положение; имущественное положение; образование; профессия; доходы; ИНН, СНИЛС, контактная информация (телефон, адрес электронной почты), или сведения, предусмотренные типовыми формами и установленным порядком обработки.

5.4. Обработка и хранение ПДн осуществляются не дольше, чем этого требуют цели обработки ПДн, если отсутствуют законные основания для дальнейшей обработки, например, если федеральным законом или договором с субъектом ПДн не установлен соответствующий срок хранения. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию при наступлении следующих условий:

5.4.1. Достижение целей обработки ПДн или максимальных сроков хранения - в течение 30 дней.

5.4.2. Утрата необходимости в достижении целей обработки ПДн - в течение 30 дней с даты наступления такого события.

5.4.3. Предоставление субъектом ПДн или его законным представителем сведений, подтверждающих, что ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки - в течении 7 рабочих дней.

5.4.4. Невозможность обеспечения правомерности обработки ПДн - в течение 10 рабочих дней.

5.4.5. Отзыв субъектом ПДн согласия на их обработку, если сохранение ПДн более не требуется для целей обработки - в течение 30 дней.

5.4.6. Истечение сроков исковой давности для правоотношений, в рамках которых осуществляется либо осуществлялась обработка ПДн.

5.4.7 В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в пп.5.4.1-5.4.5, Банк осуществляет их блокирование и обеспечивает их уничтожение в срок не более чем шесть месяцев, если иной срок не установлен федеральным законом.

5.5. Банк не выполняет обработку специальных категорий ПДн, определенных ст.10 Федерального Закона № 152-ФЗ.

5.6. В ходе своей деятельности Банк может осуществлять Трансграничную передачу ПДн в соответствии с требованиями Федерального закона «О персональных данных», с предварительным направлением в уполномоченный орган соответствующего уведомления (в случае осуществления такой трансграничной передачи).

6. Меры обеспечения безопасности при обработке ПДн

6.1. В соответствии с требованиями нормативных документов Банком создана система защиты ПДн, состоящая из подсистем правовой, организационной и технической защиты.

Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование системы защиты ПДн.

Подсистема организационной защиты включает в себя организацию структуры управления, разрешительной системы, защиты информации при работе.

Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

Банк осуществляет обработку ПДн, как с использованием средств вычислительной техники (в том числе, в информационных системах), так и без использования технических средств (автоматизированная и неавтоматизированная обработка персональных данных).

В целях предотвращения нарушений законодательства Российской Федерации в сфере ПДн Банком обеспечивается надлежащее документальное сопровождение процессов обработки ПДн:

- анализ правовых оснований обработки ПДн;
- документальное закрепление целей обработки;
- установление сроков обработки ПДн;
- регламентация процессов обработки ПДн (в том числе процесса допуска к ПДн, процесса прекращения их обработки);
- определение круга лиц, осуществляющих обработку ПДн и (или) имеющих доступ к ПДн;
- выявление и классификация информационных систем ПДн;
- распределение и закрепление обязанностей и ответственности работников Банка в сфере обработки и обеспечения безопасности ПДн.

6.2. Основными мерами защиты ПДн, используемыми Банком являются:

6.2.1 Разработка Политики в отношении обработки ПДн.

6.2.2. Определение актуальных угроз безопасности ПДн при их обработке в информационных системах, и разработка мер и мероприятий по защите ПДн.

6.2.3. Установление правил доступа к ПДн, обрабатываемых в информационных системах, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн.

6.2.4. Установление индивидуальных паролей доступа работников в информационную систему в соответствии с их трудовыми обязанностями.

6.2.5. Применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации, в том числе сертифицированного антивирусного программного обеспечения с регулярно обновляемыми базами, сертифицированного межсетевое экрана, сертифицированного программного средства защиты информации от несанкционированного доступа, а также организация иных мер по защите баз данных от несанкционированного доступа.

6.2.6. Назначение лица, ответственного за организацию работ по сохранности ПДн и по обеспечению порядка их обработки, а также за выявление инцидентов и реагирование на них.

6.2.7. Применение средств криптографической защиты информации для обеспечения безопасности ПДн при передаче по открытым каналам связи и хранении на машинных носителях информации;

6.2.8. Учет машинных носителей ПДн;

6.2.9. Резервное копирование информации;

6.2.10. Обучение работников, использующих средства защиты информации, применяемые в информационных системах ПДн, правилам работы с ними;

6.2.11. Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационных систем обработки ПДн, обнаружение фактов несанкционированного доступа к ПДн и принятие мер;

6.2.12. Контроль за принимаемыми мерами по обеспечению безопасности ПДн;

6.2.13. Размещение технических средств обработки ПДн в пределах границ охраняемой территории;

6.2.14. Обеспечение пропускного режима на территорию Банка.

Банком реализованы меры физической защиты помещений от несанкционированного проникновения, где размещены технические средства, обрабатывающие ПДн, и хранятся материальные носители ПДн.

Все работники Банка, допущенные к обработке ПДн, ознакомлены под роспись с положениями законодательства РФ о ПДн, в том числе требованиями к защите ПДн, локальными актами Банка по вопросам обработки и защиты ПДн, в части, их касающейся.

7. Права субъекта ПДн

7.1. В соответствии с положениями Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» субъект ПДн имеет следующие права в отношении своих ПДн:

а) получать информацию, касающуюся обработки его ПДн, в порядке, форме и сроки, установленные законодательством РФ;

б) требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными, не являются необходимыми для заявленной цели обработки или используются в целях, не заявленных ранее при предоставлении субъектом ПДн согласия на их обработку;

в) принимать предусмотренные законом меры по защите своих прав;

г) отозвать свое согласие на обработку ПДн.

7.2. Если субъект ПДн считает, что Банк осуществляет обработку его ПДн с нарушением требований Федерального закона РФ от 27.07.2006г. № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Банка в Уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

7.3. Право субъекта ПДн на доступ к своим ПДн может быть ограничено в соответствии с законодательством, в том числе если:

а) обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма или иными законодательными актами;

б) доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

8. Обязанности и права Банка при обработке ПДн

8.1. Банк обязан:

а) при сборе ПДн предоставить информацию об обработке ПДн;

б) в случаях, если ПДн были получены не от субъекта ПДн, уведомить субъекта;

в) при отказе в предоставлении ПДн разъяснить субъекту последствия такого отказа;

г) опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющим его Политику в отношении обработки ПДн;

д) принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

е) давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.

8.2. Банк имеет право:

а) обрабатывать ПДн субъектов ПДн в соответствии с заявленной целью;

б) требовать от субъекта ПДн предоставления достоверных ПДн, необходимых для исполнения договора, оказания услуги, идентификации субъекта ПДн, а также в иных случаях, предусмотренных законодательством о ПДн;

в) обрабатывать общедоступные ПДн физических лиц;

г) осуществлять обработку ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации;

д) поручить обработку ПДн другому лицу с согласия субъекта ПДн.

9. Ответственность за нарушение норм, регулирующих обработку и защиту ПДн

9.1. Лица, виновные в нарушении норм, регулирующих Обработку Персональных данных и защиту обрабатываемых в Банке Персональных данных, несут предусмотренную законодательством Российской Федерации ответственность