Приложение № 1
к приказу АО «ОТП Банк»
от « » _____ 2019 г №

ПОЛОЖЕНИЕ
о персональных данных
АО «ОТП Банк»

Версия 1.3

МОСКВА
2019

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

1.1. **Термины**

Банк – АО «ОТП Банк»

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

Внутриобъектовый режим - порядок действий работников и посетителей в помещениях офиса АО «ОТП Банк», направленный на обеспечение безопасности, сохранности имущества и документов.

Доступ к информации - возможность получения информации и ее использования.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

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

Кандидат – физическое лицо, претендующее на вакантную должность в Банке, персональные данные которого приняты Банком.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Лицо, ответственное за организацию обработки персональных данных – Сотрудник ответственный за обработку персональных данных, назначается приказом по Банку.

Материальный носитель персональных данных (далее материальный носитель) - материальный объект, используемый для закрепления и хранения информации. В целях настоящего Положения под материальным носителем понимается бумажный документ, диск, дискета, флэш-карта и т.п.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

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.

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.

Оператор персональных данных - 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.

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

Пользователь - работник Банка, работающий по трудовому договору, специалисты, оказывающие услуги (выполняющие работы) для Банка на основании гражданско-правового договора, а также представители юридических лиц, имеющих с Банком договорные отношения, (подрядчики, аудиторы и т.п.).

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

Режимные помещения - помещения, допуск в которые разрешен ограниченному кругу работников Банка.

Субъект персональных данных - любое физическое лицо, обработка персональных данных которого производится Банком.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

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

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.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Цель обработки персональных данных – конкретный конечный результат действий, совершенных с персональными данными, вытекающий из требований законодательства и направленный, в том числе на создание необходимых правовых условий для достижения оптимального согласования интересов сторон**.**

1.2. **Сокращения**

ПДн	Персональные данные
РФ	Российская Федерация
ФЗ	Федеральный закон
АО	Акционерное общество
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ФСБ	Федеральная служба безопасности

2. ВВЕДЕНИЕ

2.1. Важнейшим условием реализации целей деятельности Банка является обеспечение необходимого и достаточного уровня информационной безопасности активов, к которым в том числе относятся ПДн и банковские технологические процессы, в рамках которых они обрабатываются.

2.2. Настоящее Положение о персональных данных (далее - Положение) разработано в соответствии с требованиями законодательства РФ, в том числе Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), требованиями (рекомендациями) Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор), ФСБ России, ФСТЭК России, а так же комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

2.3. Настоящее Положение разработано с целью определения принципов, порядка и условий обработки ПДн работников Банка и иных лиц, чьи ПДн обрабатываются в Банке, обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн.

2.4. ПДн всегда являются конфиденциальной, строго охраняемой информацией и на них распространяются все требования, установленные внутренними нормативными документами Банка к защите конфиденциальной информации.

2.5. Настоящее Положение подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке ПДн.

2.6. Настоящее Положение является внутренним нормативным документом Банка, регламентирующим деятельность в сфере обработки и защиты ПДн.

2.7. Требования настоящего Положения обязательны для выполнения всеми пользователями, допущенными к работе с ПДн в Банке, а также обеспечивающими защиту ПДн.

3. ПОНЯТИЕ И СОСТАВ ПДН

3.1. Перечень ПДн, подлежащих защите в Банке, формируется в соответствии с Федеральным законом РФ от 27 июля 2006 № 152-ФЗ «О персональных данных».

3.2. Сведениями, составляющими ПДн, является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

4. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Целью обработки ПДн является:

- осуществление банковских операций и иной деятельности (осуществление возложенных на Банк функций), предусмотренной (ых) действующим законодательством РФ, в частности Федеральными законами от 2 декабря 1990 № 395-1 «О банках и банковской деятельности», от 30 декабря 2004 № 218-ФЗ «О кредитных историях», от 7 августа 2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», от 10 декабря 2003 № 173-ФЗ «О валютном регулировании и валютном контроле», от 22 апреля 1996 № 39-ФЗ «О рынке ценных бумаг», от 23 декабря 2003 № 177-ФЗ «О страховании вкладов физических лиц в банках РФ», от 1 апреля 1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», от 03 июля 2016 № 230-ФЗ «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», от 27 июля 2006 № 152-ФЗ «О персональных данных», нормативными актами Банка России, а также уставом, лицензиями и нормативными актами Банка;

- заключение, исполнение и прекращение гражданско-правовых договоров с физическими, юридическими и иными лицами в случаях, предусмотренных действующим законодательством и уставом Банка; проверка добросовестности контрагента до заключения договора;

- ведение кадровой работы и организации учета работников Банка: организация кадрового учета Банка, для обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам; ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, а также уставом и нормативными актами Банка;

- привлечение и отбор Кандидатов на работу в Банке;

- в целях продвижения на рынке товаров и(или) услуг Банка и(или) третьих лиц и формирования индивидуального предложения для клиентов Банка;

- однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

- проведение маркетинговых акций, оценка качества обслуживания клиентов;

- оптимизация Банком своих веб-ресурсов и рассылок.

5. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Сроки обработки указанных выше ПДн определяются в соответствие со сроком действия согласия Субъекта ПДн на обработку персональных данных, договора с субъектом ПДн, Приказом Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», Постановлением ФКЦБ РФ от 16.07.2003 № 03-33/пс «Об утверждении Положения о порядке и сроках хранения документов акционерных обществ», сроком исковой давности, а также иными требованиями законодательства РФ и нормативными документами Банка России.

6. ОСНОВНЫЕ ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Принципы обработки персональных данных.

6.1.1. Обработка ПДн в Банке должна осуществляться на основе принципов:

- законности;
- справедливости;
- ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- недопустимости обработки персональных данных, несовместимых с целями сбора персональных данных;
- недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- соответствия обработки персональных данных целям их обработки;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;
- недопустимости обработки избыточных по отношению к заявленным целям их обработки персональных данных;
- обеспечения точности обрабатываемых персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных;
- хранения персональных данных в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
- уничтожения либо обезличивания обрабатываемых персональных данных по достижении целей обработки или в случае утраты необходимости в их достижении.

6.2. Порядок сбора персональных данных.

6.2.1. Обработка ПДн осуществляется с согласия субъекта ПДн, кроме случаев, определенных в п. 6.2.5 настоящего Положения. В случаях, предусмотренных законодательством РФ, обработка ПДн осуществляется только с согласия в письменной форме. В рамках отдельных продуктов Банка могут утверждаться свои формы согласия на обработку ПДн. В случаях, если обязанность предоставления ПДн установлена законодательством РФ, оператор обязан также разъяснить субъекту ПДн юридические последствия отказа предоставить свои персональные данные.

6.2.2. Субъект ПДн принимает решение о предоставлении своих ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на

обработку ПДн может быть отозвано субъектом ПДн.

6.2.3. Если ПДн субъекта возможно получить только у третьей стороны, до начала обработки ПДн субъект ПДН должен быть уведомлен (Приложение 3 к настоящему Положению) об этом заранее и от него должно быть получено письменное согласие, в котором указываются: цель, предполагаемые источники и способы получения ПДн, а также сведения о характере подлежащих получению ПДн и последствиях отказа дать письменное согласие на получение ПДн.

Если ПДн были получены не от субъекта ПДн, оператор до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию: наименование и адрес оператора или его представителя; цель обработки ПДн и ее правовое основание, предполагаемые пользователи ПДн, установленные законодательством РФ права субъекта ПДн, источник получения ПДн.

Оператор освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные абзацем вторым настоящего пункта, в случаях, если:

- субъект ПДн уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- персональные данные сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;
- предоставление субъекту ПДн сведений, предусмотренных абзацем вторым настоящего пункта, нарушает права и законные интересы третьих лиц.

6.2.4. Третье лицо, предоставляющее ПДн субъекта, должно обладать согласием субъекта на передачу ПДн (за исключением случаев, предусмотренных законодательством РФ). Банк обязан получить подтверждение от третьего лица, передающего ПДн субъекта ПДн о том, что ПДн передаются с согласия субъекта. Банк обязан при взаимодействии с третьими лицами заключить с ними соглашение о конфиденциальности информации, касающейся ПДн субъектов в соответствии с п. 8.11 настоящего Положения.

6.2.5. В случае отсутствия согласия или отзыва согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта ПДн при наличии следующих оснований:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- 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 предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от

27 июля 2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

- 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 защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров (работ, услуг) на рынке и целей политической агитации, при условии обязательного обезличивания персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

- в иных случаях, предусмотренных законодательством РФ.

6.2.6. За исключением случаев, предусмотренных законодательством РФ Банк не имеет права получать и обрабатывать ПДн субъекта о:

- его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни;

- членстве субъекта ПДн в общественных объединениях или его профсоюзной деятельности.

6.3. Порядок сбора персональных данных работников Банка.

6.3.1. На основании Трудового кодекса РФ, а также исходя из положений ч. 2 ст. 6 Закона о персональных данных, обработка ПДн осуществляется в Банке без письменного согласия работника, за исключением случаев, предусмотренных законодательством РФ.

6.3.2. Работник обязан предоставлять работодателю достоверные сведения о себе и своевременно сообщать ему об изменении своих ПДн. Банк имеет право проверять достоверность сведений, предоставленных работником, сверяя данные, предоставленные работником, с имеющимися у работника документами.

6.3.3. Предоставление работником подложных документов при поступлении на работу может являться основанием для расторжения трудового договора.

6.3.4. При заключении трудового договора работник предоставляет в Банк в соответствии со ст. 65 Трудового кодекса РФ сведения о себе:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки.

6.3.5. В отдельных случаях, с учетом положений Трудового кодекса РФ и иных нормативно-правовых актов РФ может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

6.3.6. Работники должны быть ознакомлены под роспись с документами Банка, устанавливающими порядок обработки их ПДн, а также об их правах и обязанностях в этой области.7.3.7 Форма согласия на обработку персональных данных работников Банка приведена в Приложении № 1 к настоящему Положению.

6.3.7. Для обработки ПДн потенциальных соискателей требуется письменное согласие на обработку от таких соискателей на период принятия решение о приеме либо отказе в приеме на работу. Исключение составляют случаи, когда от имени соискателя действует кадровое агентство, с которым соискатель заключил ответствующий договор, а также при самостоятельном размещением соискателем своего резюме в сети Интернет, доступного неограниченному кругу лиц. В случае отказа в приеме на работу сведения, предоставленные соискателем, должны быть уничтожены в течение 30 дней.

6.4. Порядок сбора персональных данных клиентов Банка.

6.4.1. Обработка ПДн клиентов осуществляется в целях обеспечения осуществления комплекса кредитных, финансовых, расчетных, кассовых и других банковских операций и иных сделок субъекта ПДн (а также в иных целях, определяемых в соответствии с договором с Субъектом ПДН и/или согласием Субъекта ПДн) и соблюдения законов и иных нормативных правовых актов.

6.4.2. Клиент предоставляет в Банк ПДн, объем и содержание которых соответствует целям обработки ПДн в Банке, в соответствии с внутренними документами Банка, регламентирующими правила предоставления услуг.

6.4.3. При определении объема и содержания обрабатываемых ПДн Банк должен руководствоваться требованиями законодательства РФ, Банка России, ФСБ России, ФСТЭК России и иных органов государственной власти.

6.4.4. Объем и содержание ПДн, необходимых для осуществления банковских операций и иных сделок с участием субъекта ПДн, определяется подразделением, ответственным за осуществление предоставляемых услуг по согласованию с соответствующими подразделениями Банка.

6.5. Обработка персональных данных.

6.5.1. В целях информационного обеспечения в Банке могут создаваться внутренние источники ПДн (в том числе справочники, адресные книги). Во внутренние

источники ПДн с письменного согласия субъекта ПДн (Приложение 2 к настоящему Положению) могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн, предоставленные субъектом ПДн.

6.5.2. Сведения о субъекте ПДн должны быть исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

6.5.3. Банк обязан безвозмездно предоставить субъекту возможность ознакомления с его ПДн по его просьбе (письменному запросу), информацию, касающуюся обработки его ПДн в течение тридцати дней со дня получения запроса субъекта ПДн или его представителя.

6.5.4. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте ПДн или персональных данных субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение соответствующего нормативного правового акта, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

6.5.5. В случае выявления неправомерной обработки персональных данных при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту ПДн, с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту ПДн, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта ПДн или третьих лиц.

В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

В случае выявления неправомерной обработки персональных данных, осуществляемой оператором, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.5.6. В случае отзыва субъектом ПДн согласия на обработку его персональных

данных оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации.

При получении запроса на отзыв согласия, об уничтожении ПДн Банк обязан уведомить Субъекта ПДн (Приложение 9 к настоящему Положению).

6.5.7. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с Законом о персональных данных и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

6.5.8. Возможность трансграничной передачи ПДн и надлежащая регламентация указанного процесса устанавливается работником, ответственным за обеспечение безопасности ПДн в мотивированном заключении, в котором излагаются:

- цель передачи ПДн;
- перечень планируемых к передаче ПДн, их категорию;
- сведения о принимающей стороне;
- обоснование необходимости и целесообразности передачи ПДн, оценка последствий такой передачи для обеспечения защиты прав и интересов субъектов ПДн;
- предполагаемые последствия в случае невыполнения принимающей стороной адекватной защиты ПДн.

6.5.9. При определении степени адекватности защиты прав субъектов ПДн, должны учитываться следующие критерии:

- развитость иностранного законодательства, регламентирующего вопросы обеспечения безопасности ПДн;
- соответствие иностранного законодательства нормам законодательства РФ;
- соблюдение иностранным государством международных стандартов;
- уровень развития информационных технологий в иностранном государстве;
- участие иностранного государства в международных организациях и договорах, предусматривающих и реализующих меры защиты прав субъектов персональных данных;
- наличие межгосударственных соглашении с РФ;
- соответствие принимающей стороны требованиям Банка к обработке ПДн.

6.5.10. При определении степени адекватности защиты прав субъектов ПДн

необходимо руководствоваться законодательством иностранного государства (наличие нормативно-правовых актов в области защиты ПДн и уполномоченного органа государственной власти по защите прав субъектов ПДн), на территорию которого осуществляется передача ПДн, законодательством РФ в области защиты прав субъектов ПДн, а также международными нормативными актами, в том числе Конвенцией Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. ETS № 108 с учетом перечня стран, подписавших и ратифицировавших данную Конвенцию.

6.5.11. Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта ПДн на трансграничную передачу его персональных данных;
- предусмотренных международными договорами РФ;
- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;
- исполнения договора, стороной которого является субъект ПДн;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта ПДн.

6.5.12. В случае необходимости трансграничной передачи ПДн Банк обязан удостовериться в том, что на территории иностранного государства будет адекватная защита прав субъектов ПДн., т.е. условия обработки ПДн, соответствующие по своему характеру и содержанию установленным законодательством РФ.

7. ПРАВА И ОБЯЗАННОСТИ

7.1. Права и обязанности Банка:

- отстаивать свои интересы в суде;
- предоставлять ПДн субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.), договором с субъектом ПДн, согласием субъекта ПДн;
- отказывать в предоставлении ПДн в случаях, предусмотренных законодательством;
- использовать ПДн субъекта без его согласия, в случаях предусмотренных законодательством;
- в случаях и в порядке, предусмотренных законодательством Российской Федерации, предоставлять субъекту ПДн информацию, касающуюся обработки его ПДн;
- принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами;
- если иное не предусмотрено Законом о персональных данных или другими

федеральными законами - самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами;

- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику Банка в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

Иные права и обязанности Банка определяются законодательством Российской Федерации.

7.2. Права и обязанности субъекта персональных данных.

7.2.1. Субъект ПДн имеет право:

- требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

- требовать перечень своих ПДн, обрабатываемых в Банке и источник их получения;

- получать информацию о сроках обработки своих ПДн, в том числе о сроках их хранения;

- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжаловать в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке неправомерные действия или бездействия при обработке его ПДн.

Иные права и обязанности Субъекта ПДн определяются законодательством Российской Федерации.

8. НОРМАТИВНЫЕ ДОКУМЕНТЫ

8.1. **Внутренние:**

- Устав АО «ОТП Банк»;

- Порядок отнесения информационных систем к информационным системам персональных данных и их классификации АО «ОТП Банк, утвержденный приказом № 588 от 23.10.2017 с последующими изменениями и дополнениями;

- Положение по защите данных и информационной безопасности, утвержденное приказом № 141 от 03.04.2018 с последующими изменениями и дополнениями;

- Инструкции по организации пропускного и внутриобъектового режима на объектах АО "ОТП Банк" «Клара Цеткин» и «Метрополис», утвержденный приказом № 77 от 17.02.2015 с последующими изменениями и дополнениями.

8.2. **Внешние:**

- Закон Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Федеральный закон от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц

и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;

- Федеральный закон от 03.07.2016 №230-ФЗ «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях»;

- «Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014»;

- «Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.2-2014»;

- «Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации»

- Приказ Минэкономразвития России от 30.04.2009 № 141 «О реализации положений Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;

- Приказ Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»;

- Постановление ФКЦБ РФ от 16.07.2003 № 03-33/пс «Об утверждении Положения о порядке и сроках хранения документов акционерных обществ»;

- Постановление Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

- Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных";

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная 15.02.2008 г. Заместителем директора ФСТЭК России;

- Состав и содержание 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, утвержденным Приказом ФСБ России от 10.07.2014 №378 - при использовании средств криптографической защиты информации для защиты ПДн;

- Указание Банка России от 10.12.2015 № 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных;

- Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по

обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

- Федеральный закон от 02.12.1990 N 395-1 "О банках и банковской деятельности";
- Федеральный закон от 30.12.2004 N 218-ФЗ "О кредитных историях";
- Федеральный закон от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма";
- Федеральный закон от 10.12.2003 N 173-ФЗ "О валютном регулировании и валютном контроле";
- Федеральный закон от 22.04.1996 N 39 "О рынке ценных бумаг";
- Федеральный закон от 26.10.2002 N 127-ФЗ "О несостоятельности (банкротстве)";
- Федеральный закон от 23.12.2003 N 177-ФЗ "О страховании вкладов в банках Российской Федерации";
- Федеральный закон от 01.04.1996 N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования".