УТВЕРЖДЕНО
Приказом АО «Яндекс Банк» от
30.12.2021 № 21–02/185

Положение о порядке и условиях обработки персональных данных в акционерном обществе «Яндекс Банк»

1. Термины, определения, сокращения

АРМ — автоматизированное рабочие место.

АС — автоматизированная система Банка.

БД — база данных.

Блокирование персональных данных — временное прекращение обработки персональных данных.

ИБ — информационная безопасность.

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

ИС — информационная система

НСД — несанкционированный доступ к информации.

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.

Обработка персональных данных с использованием средств автоматизации — обработка персональных данных с помощью средств вычислительной техники в границах информационной системы персональных данных.

Оператор, Банк — акционерное общество «Яндекс Банк»

ОС — операционная система.

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

Положение — настоящее Положение о порядке и условиях обработки персональных данных в Акционерном обществе «Яндекс Банк».

Правила локализации персональных данных — система принципов по определению мест, в которых может (должна) осуществляться обработка персональных данных в зависимости от их категории, состава, в зависимости от вида субъекта персональных данных или иных обстоятельств.

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

ПО — программное обеспечение.

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

РТД — рабочая техническая документация.

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

СУБД — система управления базами данных.

Сотрудник — лицо, состоящее с Банком в трудовых отношениях по определению действующего трудового законодательства РФ.

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных, обрабатываемых без использования средств автоматизации.

2. Общие положения

2.1 Настоящее Положение утверждено в соответствии со ст. 18.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», является основополагающим внутренним регулятивным документом Оператора, определяющим его политику в отношении обработки персональных данных, устанавливающим процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации при осуществлении такой обработки, а также устранение последствий таких нарушений, реализации требований законодательства в области обработки и защиты персональных данных, и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в Банке.

2.2 Положение распространяется на отношения по обработке персональных данных, возникшие в Банке как до, так и после утверждения Положения, за исключением случаев, когда по причинам правового, организационного и иного характера правила Положения не могут быть распространены на отношения по обработке персональных данных, возникшие до его утверждения.

2.3 Если в отношениях с Банком участвуют наследники (правопреемники) и (или) представители субъектов персональных данных, то Банк будет считать себя оператором персональных данных лиц, представляющих указанных субъектов.

2.4 Целью настоящего Положения является обеспечение выполнения Банком требований законодательства Российской Федерации в области обработки персональных данных и обеспечение организационной и правовой безопасности процессов в Банке, в рамках которых обрабатываются персональные данные.

2.5 Настоящее Положение издано в соответствии с:

- Конституцией РФ (принята всенародным голосованием 12 декабря 1993 г.);
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
- Постановлением Правительства РФ № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

— Постановлением Правительства РФ № 687 от 15.09.2008 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
— Приказом ФСТЭК России № 21 от 18.02.2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
— Положением о коммерческой тайне АО "Яндекс Банк" и Перечнем сведений, составляющих коммерческую тайну АО "Яндекс Банк".

3. Основания обработки ПДн. Состав ПДн, обрабатываемых банком. Категории субъектов персональных данных.

3.1 Банк осуществляет обработку следующих категорий ПДн следующих субъектов ПДн по следующим основаниям:

3.1.1 Обрабатываются персональные данные Сотрудников, бывших Сотрудников, их близких родственников в установленных нормативными актами случаях, физических лиц, выполняющих работы и (или) оказывающих услуги на основании гражданско-правового договора с Банком, обработка персональных данных которых осуществляется в целях обеспечения соблюдения требований трудового договора с Сотрудником, гражданско-правового договора с исполнителем, Трудового Кодекса РФ, Налогового Кодекса РФ, Гражданского кодекса РФ, ФЗ «О банках и банковской деятельности», ФЗ «О Центральном банке Российской Федерации (Банке России)», ФЗ «Об обязательном пенсионном страховании в Российской Федерации», ФЗ «Об основах обязательного социального страхования», ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний», ФЗ «О бухгалтерском учете», прочих федеральных законов и иных нормативных правовых актов Российской Федерации, действия которых распространяются на отношения Банка и таких лиц.

3.1.2 Обрабатываются персональные данные физических лиц - клиентов, их представителей, представителей, выгодоприобретателей, должностных лиц и единоличных органов юридических лиц – клиентов и контрагентов Банка, имеющих право совершения юридически значимых действий и (или) подписания документов, обработка персональных данных которых осуществляется в целях подготовки, заключения, исполнения договора между юридическим лицом и Банком, соблюдения требований Гражданского кодекса РФ, прочих федеральных законов и иных нормативных правовых актов, действия которых распространяются на отношения Банка и таких лиц.

3.1.3 Обрабатываются персональные данные работников и бывших работников аффилированных с Оператором организаций, обработка персональных данных которых осуществляется Оператором по поручению таких организаций на основании договоров и соглашений об оказании услуг по

ведению кадрового учета, предусмотренного трудовым законодательством, с согласия таких лиц, предоставленного указанным Банком или Оператору, в целях соблюдения требований договора между Оператором и такими Банками, соблюдения требований трудового договора между такими Банками и их работниками, требований Трудового Кодекса РФ, Налогового Кодекса РФ, ФЗ «Об обязательном пенсионном страховании в Российской Федерации», ФЗ «Об основах обязательного социального страхования», ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний», ФЗ «О бухгалтерском учете», Гражданского кодекса РФ, прочих федеральных законов и иных нормативных правовых актов, действия которых распространяются на указанные отношения.

3.1.4 Обрабатываются персональные данные разовых посетителей офисов Банка (гости Банка, посетители мероприятий Банка, участники переговоров, соискатели статуса Сотрудника и иные), обработка персональных данных которых осуществляется в целях Банка допуска указанных лиц на территории и в помещения Банка, открытые для доступа таких лиц, обеспечения возможности осуществления встреч, переговоров, мероприятий при участии таких лиц, обеспечения контрольно-пропускного режима Банка и защиты территорий и помещений Банка от проникновения посторонних лиц без права доступа, соблюдения требований федеральных законов и иных нормативных правовых актов, действия которых распространяются на отношения Банка и таких лиц.

3.1.5 Обрабатываются персональные данные пользователей интернет-сервисов и программ, предоставляемых Банком, обработка персональных данных которых осуществляется в целях исполнения соглашений (Пользовательского соглашения, Условий использования, Лицензионного соглашения, Правил использования, Политик, либо иных соглашений, в том числе постоянно размещенных в сети Интернет по адресу https://yandex.ru/legal/), заключенных с пользователем, в целях соблюдения требований Гражданского Кодекса РФ, ФЗ «Об информации, информационных технологиях и защите информации», прочих федеральных законов и иных нормативных правовых актов, действия которых распространяются на отношения Банка и таких лиц.

4. Принципы обработки персональных данных

4.1 Обработка персональных данных в Банке осуществляется на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

— достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
— недопустимости объединения информационных систем персональных данных, созданных для несовместимых между собой целей обработки ПДн;
— информированности Сотрудников о недопустимости нарушения режима ПДн в Банке, в том числе о содержании и требованиях настоящего Положения и иных локальных актов Банка и законодательства РФ о персональных данных;
— информированности субъектов персональных данных, а в случаях, предусмотренных законодательством – их представителей или правопреемников, о политике Оператора в отношении обработки персональных данных, о реализуемых требованиях к защите персональных данных;
— обеспечения контроля и надзора за соблюдением законодательства о персональных данных и локальных актов Банка со стороны лица, ответственного за организацию обработки персональных данных в АО "Яндекс Банк", назначаемого и сменяемого приказом руководителя Банка, а в случаях, предусмотренных настоящим Положением – со стороны такого лица и соответствующих комиссий.
— соблюдения Правил локализации персональных данных и обеспечения режима трансграничной передачи персональных данных.

4.2 Соблюдение указанных принципов осуществляется посредством обеспечения условий обработки персональных данных, установленных настоящим Положением с учетом нормативных правовых актов, регулирующих порядок и условия обработки персональных данных, а также требований к их защите.

5. Метод организации обработки ПДн

5.1 В Банке обработка ПДн организуется методом обеспечения законности и безопасности (защищенности) любого действия (операции) или совокупности 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.

5.2 В Банке обработка ПДн организуется как с использованием средств автоматизации путем использования раздельных (технологически отделенных друг от друга, независимых по оборудованию и не связанных локальными или глобальными сетями) ИСПДн, разделение которых осуществляется по критерию цели обработки ПДн, так и без использования средств автоматизации.

5.3 Для обеспечения законности и безопасности (защищенности) обработки ПДн Банк реализует следующие меры:

— руководитель Банка назначает лицо, ответственное за организацию обработки ПДн в Банке;
— руководителем Банка определяется перечень лиц, доступ которых к персональным данным, обрабатываемым в конкретной информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
— руководителем Банка определяется Перечень мест обработки персональных данных, обрабатываемых в Банке;
— утверждаются внутренние регулятивные документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;
— Банк принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных нормативными правовыми актами, для защиты ПДн от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;
— осуществляется внутренний контроль соответствия обработки ПДн нормативным правовым актам, требованиям к защите ПДн, Положению и иным внутренним регулятивным документам Банка;
— проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения правил законодательства РФ и Положения, определяется соотношение указанного вреда и принимаемых мер, направленных на обеспечение исполнения обязанностей Оператора, актуализируется Модель угроз ИСПДн;
— предоставление доступа к любым персональным данным, в том числе доступа к ИСПДн, либо доступа к материальным носителям ПДн, возможно только после ознакомления допускаемого лица с требованиями нормативных правовых актов, перечисленных в п. 2.5. Положения, ознакомления с настоящим Положением, а также с Положением о порядке обработки и защиты персональных данных сотрудников Банка, и подписи допускаемым лицом Обязательства о неразглашении персональных данных;
— реализована система контроля и управления доступом, ограничивающая доступ посетителей в помещения Банка, а для помещений (мест), в которых разрешена обработка ПДн реализован такой режим обеспечения безопасности помещений, который препятствует возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

5.4 Обеспечение безопасности ПДн при их обработке с использованием средств автоматизации дополнительно достигается следующими способами:

— при обработке персональных данных с использованием средств автоматизации используются ИСПДн, для которых обеспечиваются соответствующие уровни защищенности с учетом типов угроз и состава ПДн, обрабатываемых в ИСПДн; на стадии ввода в эксплуатацию конкретной ИСПДн выполняются настройки средств и механизмов обеспечения безопасности, не допускающие несанкционированного

изменения пользователем предоставленных ему полномочий, на стадии эксплуатации ИСПДн такие настройки контролируются и актуализируются;
- разделение ИСПДн основывается на принципе недопустимости объединения информационных систем персональных данных, созданных для несовместимых между собой целей обработки ПДн. ИСПДн в целях их идентификации имеют условные обозначения;
- каждая эксплуатируемая ИСПДн должна быть обозначена, описана и классифицирована (по уровню защищенности персональных данных, который необходимо обеспечить при их обработке в ИСПДн) в Заключении Комиссии по классификации информационных систем персональных данных АО "Яндекс Банк" и оценке соответствия выполнения требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», которое не реже чем раз в два года предоставляется руководителю Банка лицом, которое назначено ответственным за Банк обработки персональных данных в АО "Яндекс Банк" приказом руководителя Банка. Состав Комиссии также определяется и изменяется приказом по Банку;
- для каждой эксплуатируемой ИСПДн осуществляется утверждение руководителем Оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- для ИСПДн, в которых должен быть обеспечен 3-ий уровень защищенности, назначается должностное лицо (Сотрудник), ответственный за обеспечение безопасности персональных данных в информационной системе (администратор информационной безопасности);
- обеспечивается выполнение нормативных требований к журналированию ИСПДн;
- производится актуализация и аудит угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных исходя из уровня защищенности;
- применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации (в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз);
- производится оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- ведется учет машинных носителей персональных данных и обеспечена сохранность носителей персональных данных;
- установлен контроль информационной безопасности для обнаружения фактов несанкционированного доступа к персональным данным и принятия мер;
- реализовано резервное копирование и восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; установлены правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечены регистрация и учет действий,

совершаемых с персональными данными в информационной системе персональных данных;
— установлен контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

5.5 Полный состав и содержание конкретных организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных определяются уполномоченным лицом или органом Банка.

5.6 Обеспечение защиты ПДн при их обработке, осуществляемой без использования средств автоматизации, дополнительно достигается следующими способами:

— Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных в специальных разделах этих носителей (далее - материальные носители).
— При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных используется отдельный материальный носитель.
— Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, обрезка, вымарывание, переформатирование).
— Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется таким образом, что в отношении каждой категории персональных данных можно определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
— Классификация документов по уровню конфиденциальности производится на основании сведений, содержащихся в документах. Документы, содержащие персональные данные, относятся к конфиденциальным.
— Печать, фотокопирование (ксерокопирование, иные виды механического копирования) указанных документов должны производиться Сотрудниками, непосредственно осуществляющими обработку соответствующего документа и имеющими доступ к соответствующим персональным данным.
— Порядок нанесения и использования на документах специальных грифов и иных отметок, свидетельствующих о том, что данная информация относится к конфиденциальной, порядок работы с такими документами и их безопасного хранения, изложен в «Положении о коммерческой тайне АО "Яндекс Банк".

6. Сбор персональных данных

6.1 Сбор персональных данных осуществляется Банком следующими способами:

- непосредственно от субъекта персональных данных при условии наличия возможности определенно установить, что согласие субъекта ПДн на обработку его персональных данных исходит непосредственно от субъекта ПДн;
- путем получения персональных данных субъектов от лиц, уполномоченных субъектами персональных данных на передачу персональных данных Банка при условии наличия возможности определенно установить, что согласие на обработку персональных данных было получено уполномоченным лицом и исходило непосредственно от субъекта ПДн;
- в электронной или документарной форме;
- с использованием информационно-телекоммуникационной сети «Интернет» или без такого использования.

6.2 Согласие субъекта персональных данных должно быть получено по правилам, установленным действующим законодательством. Законодательство РФ может предусматривать случаи, в которых согласие субъекта персональных данных на обработку его персональных данных не требуется.

6.3 Не допускается сбор специальных категорий персональных данных, то есть ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением сведений о состоянии здоровья Сотрудников, обработка которых необходима для исполнения трудового договора, требований трудового законодательства РФ, Налогового Кодекса РФ, ФЗ «Об обязательном пенсионном страховании в Российской Федерации», ФЗ «Об основах обязательного социального страхования», ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний», ФЗ «О бухгалтерском учете», прочих федеральных законов и иных нормативных правовых актов.

6.4 Если Банк не вправе осуществлять сбор (получение) данных, то субъекту ПДн предоставляется отказ от сбора данных, а в случае передачи таких данных субъектом ПДн без ведома Банка (в направленном субъектом ПДн письме, заявлении, форме, ином документе, направленном в одностороннем порядке) Банк немедленно уничтожает такие данные и сообщает лицу о невозможности осуществлять их обработку в какой-либо форме.

6.5 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, а также обеспечивает соблюдение иных Правил локализации персональных данных, установленных законодательством о ПДн и настоящим Положением.

6.6 Основаниями предполагать российское гражданство субъекта ПДн для Банка являются:

— сведения о гражданстве, поступившие от самого субъекта ПДн или его представителя (данные документов, заявлений, заполненных электронных форм, обращений и пр.);
— сведения о гражданстве субъекта ПДн, полученные от органов государственной власти, местного самоуправления, включая правоохранительные и судебные органы, а также Уполномоченный орган по защите прав субъектов ПДн.

7. Хранение персональных данных и доступ к персональным данным

7.1 Доступ к персональным данным Сотрудников, бывших Сотрудников, физических лиц, выполняющих работы и (или) оказывающих услуги на основании гражданско-правового договора с Банком, доступ к персональным данным работников и бывших работников аффилированных с Оператором организаций, обработка персональных данных которых осуществляется Оператором по поручению таких организаций на основании договоров и соглашений об оказании услуг по ведению кадрового учета, предусмотренного трудовым законодательством, с согласия такого работника, в рамках своих должностных обязанностей имеют:

— уполномоченные лица в структурном подразделении Банка, ответственном за ведение кадрового делопроизводства и управление персоналом;
— уполномоченные лица в структурном подразделении Банка, ответственном за обеспечение отчетности, планирования и контроля;
— уполномоченные лица в структурном подразделении Банка, ответственном за обеспечение юридического сопровождения деятельности Банка;
— уполномоченные лица в структурном подразделении Банка, ответственном за обеспечение информационной безопасности.

7.2 Доступ к персональным данным представителей, должностных лиц и единоличных органов юридических лиц – контрагентов Банка, имеющих право совершения юридических действий и (или) подписания документов, в рамках своих должностных обязанностей имеют:

— уполномоченные лица в структурном подразделении Банка, ответственном за развитие бизнеса;
— уполномоченные лица в структурном подразделении Банка, ответственном за обеспечение юридического сопровождения деятельности Банка;
— уполномоченные лица финансового подразделения Банка;
— уполномоченные лица коммерческого подразделения Банка;
— уполномоченные лица в структурном подразделении Банка, ответственном за обеспечение информационной безопасности.

7.3 Доступ к персональным данным разовых посетителей офисов Банка (гости Банка, посетители мероприятий Банка, участники переговоров,

соискатели статуса Сотрудника и иные) в рамках своих должностных обязанностей имеют:

- уполномоченные лица в структурном подразделении Банка, ответственном за ведение кадрового делопроизводства и управление персоналом;
- уполномоченные лица в структурном подразделении Банка, ответственном за развитие бизнеса;
- уполномоченные лица в структурном подразделении Банка, ответственном за обеспечение информационной безопасности.

7.4 Доступ к персональным данным пользователей интернет-сервисов и программ, предоставляемых Банком, в рамках своих должностных обязанностей имеют:

- уполномоченные лица в структурном подразделении Банка, ответственном за обеспечение технической поддержки пользователей;
- уполномоченные лица в структурном подразделении Банка, ответственном за обеспечение администрирования сервисов, программ и оборудования, обеспечивающего их работу;
- уполномоченные лица в структурном подразделении Банка, ответственном за обеспечение юридического сопровождения деятельности Банка;
- уполномоченные лица в структурном подразделении Банка, ответственном за обеспечение информационной безопасности.

7.5 Сотрудники, имеющие доступ к любым персональным данным, обязаны принимать и соблюдать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, и других неправомерных действий в отношении данной информации. Предоставление доступа к любым персональным данным, в том числе доступа к ИСПДн, либо доступа к материальным носителям ПДн, возможно только после ознакомления допускаемого лица с настоящим Положением, а также с Положением о порядке обработки и защиты персональных данных сотрудников АО «Яндес Банк», и подписи допускаемым лицом Обязательства о неразглашении персональных данных.

7.6 Лица, осуществляющие обработку персональных данных, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

7.7 Доступ уполномоченных лиц к персональным данным, хранящимся в информационных системах, может осуществляться только локально (с АРМ конкретного Сотрудника).

7.8 Работа по обеспечению безопасности персональных данных при их обработке в информационных системах Банка являются неотъемлемой частью работ по созданию и эксплуатации ИСПДн.

7.9 Доступ к электронным носителям, содержащим персональные данные, обеспечивается за счет использования механизма разграничения прав доступа

в информационной системе, либо за счет использования механизма сейфового хранения.

7.10 Каждый носитель электронной информации, используемый в Банка для хранения персональных данных, должен иметь уникальный идентификационный номер.

7.11 Использование неучтенных носителей электронной информации для хранения персональных данных в Банка запрещается.

7.12 Сотрудники, использующие в работе зарегистрированные носители электронной информации, обязаны по требованию предъявлять их для проверки в структурное подразделение Банка, ответственное за обеспечение информационной безопасности.

7.13 Передача материальных носителей с персональным данными должна осуществляться строго по акту, который подписывается передающим лицом и получателем.

8. Трансграничная передача персональных данных

8.1 Банк вправе осуществлять трансграничную передачу персональных данных в установленных законодательством случаях.

8.2 Трансграничная передача ПДн осуществляется с обязательным учетом Правил локализации ПДн.

8.3 При осуществлении трансграничной передачи ПДн Сотрудники руководствуются в том числе:

- Законодательством РФ о персональных данных;
- Конвенцией Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбург 28 января 1981 года);
- Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных» от 15.03.2013 №274 (Зарегистрировано в Минюсте России 19.04.2013 №28212).

8.4 Сотрудник 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.

9. Представление и распространение персональных данных

9.1 Сотрудники, ответственные за работу с персональными данными, должны четко знать случаи, при которых они могут передавать персональные данные и процедуры (формы) такого предоставления.

9.2 Предоставление персональных данных третьим по отношению к Банку и к субъекту персональных данных (его представителю) лицам по общему правилу допускается только с осознанного, явного и информированного согласия субъекта персональных данных (его представителя), с учетом ограничений, установленных законодательством о персональных данных. Такое согласие может быть получено как на осуществление одной конкретной операции предоставления, так и на осуществление совокупности операций предоставления в определенных Оператором в полученном согласии случаях. Законодательством РФ могут устанавливаться случаи, когда такое согласие не требуется.

9.3 Распространение персональных данных (раскрытие персональных данных неопределенному или неизвестному лицу, либо неопределенному или неизвестному кругу лиц) запрещено.

10. Траспортировка носителей информации, содержащих персональные данные

10.1 Под носителями информации, содержащей персональные данные, понимаются документы в бумажной форме, любые электронные и иные носители информации, содержащие персональные данные.

10.2 При транспортировке носителей информации, содержащей персональные данные, исключается возможность случайного или намеренного ознакомления с перевозимой информацией неуполномоченных лиц.

10.3 Все транспортируемые носители информации, содержащей персональные данные, перед выносом за пределы охраняемого периметра Банка должны быть запечатаны в специальные конверты, позволяющие определять факт вскрытия, или защищены пломбированием или аналогичным образом.

10.4 Передача транспортируемых носителей информации, содержащей персональные данные, производится под роспись принимающего лица. При этом принимающее лицо должно проверить целостность конвертов или иных защитных маркеров, о чём сделать соответствующую отметку.

10.5 Допускается транспортировка носителей информации, содержащей персональные данные с использованием почтовых и курьерских служб. При этом принимающее лицо должно проверить целостность конвертов или иных защитных маркеров, не использовать полученные носители в случае выявления

повреждений защитных маркеров и немедленно уведомить о данном факте отправителя и почтовую/курьерскую службу.

11. Учет и уничтожение персональных данных

11.1 ПДн подлежат уничтожению при достижении цели их сбора и обработки, при невозможности достижения цели их сбора и обработки, по законному требованию субъекта ПДн, его представителя, органа, уполномоченного осуществлять контроль и надзор в сфере персональных данных, в иных случаях, предусмотренных действующим законодательством.

11.2 Банк вправе предоставить субъекту ПДн право и техническую возможность внести, дополнить, уточнить (изменить) или удалить (уничтожить) данные самостоятельно. В остальных случаях данные уничтожаются уполномоченными Сотрудниками по правилам настоящего раздела Положения.

11.3 В Банке определяется и документально фиксируется порядок постановки на учет и снятия с учета электронных носителей, предназначенных для размещения персональных данных.

11.4 Персональные данные уничтожаются следующим способом:

— уничтожение ПДн в составе ИСПДн осуществляется путем удаления информации без возможности восстановления с электронных носителей, на которых размещены персональные данные, средствами гарантированного стирания информации, при невозможности стирания - по акту путем безвозвратного уничтожения носителей. Уничтожение электронных носителей информации должно производиться как минимум двумя лицами, одно из которых – Сотрудник структурного подразделения Банка, ответственного за обеспечение информационной безопасности. При этом в журнале учета делается соответствующая запись за подписями Сотрудников, производивших уничтожение;
— уничтожение ПДн, обрабатываемых без применения средств автоматизации, производится путем уничтожения носителя с применением кросс-шредера или путем сжигания.

11.5 Изложенные в настоящем Положении принципы и процедуры уничтожения ПДн могут быть ограничены в соответствии с требованиями законодательства РФ. В частности, такие ограничения могут предусматривать обязанность Банка сохранить информацию, в том числе содержащую ПДн, на срок, установленный законодательством, и передать такую информацию в соответствии с законодательно установленной процедурой государственному органу.

12. Лицо, ответственное за организацию обработки персональных данных в банке

12.1 Лицо, ответственное за организацию обработки персональных данных в Банке, обязано:

- осуществлять внутренний контроль за соблюдением Оператором и его Сотрудниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных и к соблюдению прав и законных интересов субъектов ПДн;
- доводить до сведения Сотрудников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных с целью соблюдения Сотрудниками прав и законных интересов субъектов ПДн, либо обеспечивать такое доведение силами уполномоченных лиц в структурном подразделении Банка, ответственном за ведение кадрового делопроизводства и управление персоналом;
- осуществлять общий контроль за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей, которые возложены на уполномоченных Сотрудников подразделения, обеспечивающего юридическое сопровождение деятельности Банка;
- обеспечивать работу Комиссии по классификации информационных систем персональных данных АО "Яндес Банк" и оценке соответствия выполнения требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- издавать за личной подписью документы, издание которых возложено на лицо настоящим Положением;
- исполнять иные обязанности, возложенные на лицо руководителем Банка путем их закрепления в настоящем Положении и должностной инструкции.

12.2 Лицо, ответственное за организацию обработки персональных данных в Банке, подотчетно исключительно руководителю Банка и должно быть Сотрудником.

13. Исполнение банком обязанностей по информированию и работа с обращениями по вопросам ПНд

13.1 Банк, являясь оператором, осуществляющим сбор персональных данных, в том числе с использованием информационно-телекоммуникационной сети «Интернет», публикует в соответствующей информационно-телекоммуникационной сети документ, определяющий политику Банка в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечивает возможность постоянного доступа неограниченного круга лиц к указанному документу на странице сети «Интернет» по сетевому адресу

https://yandex.ru/legal/confidential/ с использованием средств соответствующей информационно-телекоммуникационной сети.

13.2 Банк принимает обращения, заявления и требования субъектов ПДн, а в предусмотренных законодательством РФ случаях – их представителей (правопреемников), а также органа, уполномоченного в области защиты прав и законных интересов субъектов ПДн, в электронной и бумажной формах.

13.3 Исполнение обязанностей, возложенных на Банк в части обращений и запросов субъектов персональных данных, их представителей, органа, уполномоченного в области защиты прав и законных интересов субъектов ПДн, возложено на уполномоченных Сотрудников подразделения, обеспечивающего юридическое сопровождение деятельности Банка, и регламентировано документами данного подразделения.

13.4 Лицо, ответственное за организацию обработки ПДн в Банке, осуществляет общий контроль за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей, органа, уполномоченного в области защиты прав и законных интересов субъектов ПДн, за правильностью ведения Журнала обращений субъектов ПДн.

14. Порядок внесения изменений в документы банка. Прочие положения.

14.1 РТД Банка ведется в электронном виде (базы данных, электронные таблицы). Формат РТД по различным АС Банка выбирается Сотрудниками, ответственными за ведение РТД, и согласовывается Сотрудниками структурного подразделения Банка, ответственного за обеспечение информационной безопасности. Один экземпляр РТД на АС должен храниться у администратора АС на бумажном носителе с соблюдением требований защиты от НСД.

14.2 Нормативные документы Банка, касающиеся обработки персональных данных, ведутся в бумажном виде. Такие документы подлежат периодическому пересмотру в соответствии со сроками, установленными законодательством РФ, при его отсутствии – со сроками, указанными в этих документах. Если срок пересмотра документа никак не регламентирован, пересмотр должен производиться один раз в два года.

14.3 Настоящее Положение подлежит пересмотру не реже одного раза в два года на основании анализа произошедших или планируемых изменений в законодательстве РФ, изменений в документах Банка, анализа текущего уровня науки и техники, в том числе в области технологий защиты информации, анализа достигнутых результатов обработки и защиты ПДн за период действия Положения.

14.4 Внеплановый пересмотр нормативных документов Банка может производиться по инициативе лица, ответственного за организацию обработки персональных данных, по инициативе Сотрудников структурного

подразделения Банка, ответственного за обеспечение информационной безопасности, по инициативе Сотрудников подразделения, обеспечивающего юридическое сопровождение деятельности Банка, в случаях:

- выявления изменений в законодательстве РФ, основополагающих внутренних документах Банка;
- изменения видов деятельности Банка, существенного изменения технологических и производственных процессов;
- выявления несоответствий законодательству РФ, основополагающим внутренним документам Банка, иным применимым требованиям;
- появления сведений о новых угрозах информационной безопасности, новой информации по результатам расследования инцидентов.