Банк «Йошкар-Ола»
(публичное акционерное общество)

УТВЕРЖДЕНО
Правлением Банка
«Йошкар-Ола» (ПАО)
Протокол № 05
от «29» апреля 2015 г.

П О Л О Ж Е Н И Е

об обработке и защите персональных данных

в Банке «Йошкар-Ола» (ПАО)

(в редакции изменений от 29.01.2016 (Протокол № 01), от 19.02.2016 Решение Правления № 02/1902-01)

Настоящее Положение разработано в соответствии с Федеральным Законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными документами ФСТЭК и ФСБ России с целью обеспечения защиты прав и свобод граждан при обработке их персональных данных в информационных системах персональных данных.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящим Положением определяются цели и задачи при обработке персональных данных сотрудников и клиентов Банка, а так же обеспечение безопасности при обработке и хранении персональных данных.

В настоящем Положении используются следующие основные понятия:

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

Оператор ПДн – Банк «Йошкар-Ола» (ПАО), самостоятельно или совместно с другими юридическими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемых с персональными данными.

Информационная система персональных данных (далее ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, 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, применяемые в информационных системах.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа к информационным системам персональных данных – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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.

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

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

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

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.

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

Конфиденциальность персональных данных – Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

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

Несанкционированный доступ (несанкционированные действия) к информационным системам персональных данных – доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

Защита информации – комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным, при этом предусматривается:

- разграничение полномочий доступа к данным;
- авторизация, контроль и учет действий с данными (регистрация событий);
- контроль копирования, печати, обмена данными по каналам связи;
- межсетевое экранирование и защита от вирусов;
- учет внешних носителей данных;
- резервное копирование / восстановление данных;
- раздельное хранение носителей данных с резервными копиями;
- контроль доступа в помещения и к компьютерам;
- применение устройств идентификации пользователей для доступа.

Ресурс ПДн — совокупность ПДн, обрабатываемых в организации банковской системы РФ (далее БС РФ) с использованием или без использования средств автоматизации и АБС, в том числе ИСПДн, объединенных общими целями обработки.

2. ЦЕЛИ И ЗАДАЧИ

Целью обработки сведений, составляющих персональные данные, является оказание услуг в банковской сфере, осуществление уставной деятельности, ведение кадрового и бухгалтерского учета сотрудников, обеспечение защиты прав и свободы гражданина при обработке его персональных данных.

Задачей обеспечения безопасности информации в ИСПДн является защита интересов субъектов информационных отношений. Это достигается посредством постоянного поддержания следующих свойств информации в процессе ее обработки, хранения и передачи:

- целостности информации;
- доступности обрабатываемой информации для зарегистрированных пользователей;
- конфиденциальности информации.

3. ПРИНЦИПЫ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ

В Банке должна быть установлена необходимость осуществления уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн и организована деятельность по своевременному направлению указанного уведомления в соответствии с требованиями Федерального закона “О персональных данных” в случае наличия такой необходимости.

3.1. Под обработкой ПДн понимается получение, хранение, комбинирование, передача или любое другое использование.

Разделяют два вида информации с ПДн: на бумажных носителях и в электронном виде. Обработка ПДн осуществляется смешанным путем:

- неавтоматизированный способ (личные дела, трудовые книжки, другие документы, имеющиеся в банке, в которых содержатся ПДн).

- автоматизированный способ с использованием средств вычислительной техники, с возможностью дальнейшей передачи ПДн по сети интернет.

Исходя из этого применяют, соответственно, различные способы обработки и защиты ПДн.

При неавтоматизированном способе обработке ПДн в качестве мер защиты применяют:

- ограничение на доступ лиц в помещение, где обрабатываются ПДн;
- металлические шкафы (сейфы);
- охранно-пожарную сигнализацию.

При автоматизированном способе в качестве мер защиты используются:

- парольный доступ в ИСПДн;
- средства криптографической защиты информации при передаче ее по компьютерным сетям;
- антивирусная защита.

3.2. В целях обеспечения прав субъектов ПДн при их обработке должны соблюдаться следующие общие требования:

3.2.1. Обработка ПДн может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

3.2.2. При определении объема и содержания обрабатываемых ПДн оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

3.2.3. Получение персональных данных может осуществляться как путем представления их самим субъектом ПДн, так и путем получения их из иных источников.

3.3. К обработке, передаче и хранению персональных данных сотрудника в зависимости от способа обработки и вида ИСПДн могут иметь различные подразделения оператора. Список лиц имеющих доступ к персональным данным определяется правами доступа к соответствующей ИСПДн.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.5. Передача персональных данных сотрудника возможна только с согласия сотрудника или в случаях, прямо предусмотренных законодательством.

3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъектов распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4. СУБЪЕКТЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

4.1 Субъектами информационных отношений являются:

- Сотрудники (субъекты) – физические лица, состоящие в трудовых и иных гражданско-правовых отношениях с Банком-оператором;
- Клиенты (субъекты персональных данных) – физические лица, вступившие в договорные и иные гражданско-правовые отношения с Банком-оператором, предусмотренные Уставом.
- Оператор ПДн – Банк «Йошкар-Ола» (ПАО), другие операторы ПДн в случае необходимости передачи ПДн для их дальнейшей обработки.
- Физические лица, обращающиеся с заявлениями, жалобами, предложениями и другие посетители Банка «Йошкар-Ола» (ПАО).
- Аффилированные лица (учредители, акционеры) Банка «Йошкар-Ола» (ПАО).
- Кандидаты на работу в Банк «Йошкар-Ола» (ПАО).

4.2 Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности (сохранения в тайне) информации в соответствии с требованиями российского законодательства;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты информации от незаконного ее тиражирования (защиты персональных данных, защиты авторских прав, прав собственника информации).

5. ОСНОВНЫЕ ВИДЫ УГРОЗ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общая классификация угроз.

1. Угрозы конфиденциальности данных и программ. Данные угрозы реализуются при несанкционированном доступе к программам, данным, каналам связи, при перехвате электромагнитных излучений, при анализе трафика.
2. Угрозы целостности данных, программ, аппаратуры. Данные угрозы реализуются при несанкционированном уничтожении, модификации данных, порождении фальсифицированных данных, задержке и нарушении маршрутизации данных в каналах связи.
3. Угрозы доступности данных. Данные угрозы реализуются при создании условий, когда законный пользователь или процесс не получает своевременного доступа к данным или ресурсам системы, каналам связи.

Частная модель угроз безопасности персональных данных разрабатывается в отдельном документе и утверждается правлением Банка.

6. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, В РАМКАХ БАНКОВСКИХ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

6.1. Для обеспечения выполнения требований к защите персональных данных рекомендуется обеспечивать соответствующие уровни защищенности ПДн при их обработке в ИСПДн, установленных Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”.

6.2. В соответствии со стандартом Банка России СТО БР ИББС-1.0-2014 об информационной безопасности и с учетом специфики обработки и обеспечения безопасности ПДн в Банке, угрозы утечки персональных данных по техническим каналам, а также угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн, рекомендуется признавать неактуальными для Банка.

6.3. Результатом оценки рисков нарушения безопасности персональных данных должен быть документ «Частная модель угроз безопасности персональных данных», содержащий актуальные для Банка угрозы безопасности персональных данных, на основе которого вырабатываются требования, учитывающие особенности обработки персональных данных в Банке.

6.4. В Банке должны быть реализованы защита периметров сегментов вычислительной сети, в которых расположены ИСПДн, и контроль информационного взаимодействия между сегментами вычислительных сетей. В Банке должны быть определены и контролироваться правила информационного взаимодействия различных ИСПДн между собой так и иными АБС.

6.5. Для программных компонентов АБС, реализующих банковский платежный технологический процесс и предназначенных для обработки ПДн или иной информации, в отношении которой законодательством РФ или решением Банка установлено требование об обеспечении безопасности, рекомендуется перед проведением предварительных испытаний осуществлять контроль исходного кода с целью выявления типовых ошибок программирования и иных дефектов, приводящих к возникновению уязвимостей.

6.6. Использование в ИСПДн сертифицированных по требованиям безопасности информации средств защиты информации осуществляется в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 “Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных”.

7. ОБЩИЕ ТРЕБОВАНИЯ ПРИ ПРОВЕДЕНИИ РАБОТ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Обработка персональных данных осуществляется в зависимости от вида информации с ПДн.

7.2. Для ресурсов ПДн, обрабатываемых в АБС Банка, в том числе ИСПДн, порядок обработки ПДн может являться частью эксплуатационной документации на АБС.

7.3. Для ресурсов ПДн, обрабатываемых в неавтоматизированном режиме АБС порядок обработки ПДн определяется соблюдением порядка, предусмотренного Постановлением Правительства от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

7.4. В Банке должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета ресурсов ПДн, в том числе учета ИСПДн.

7.5. Для каждого ресурса ПДн должно быть обеспечено:

— установление цели обработки ПДн;

— установление и соблюдение сроков хранения ПДн и условий прекращения их обработки;

— определение перечня и категорий обрабатываемых ПДн (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн);

— выполнение ограничения обработки ПДн достижением цели обработки ПДн;

— соответствие содержания и объема обрабатываемых ПДн установленным целям обработки;

— точность, достаточность и актуальность ПДн, в том числе по отношению к целям обработки ПДн;

— выполнение установленных процедур получения согласия субъектов ПДн (их законных представителей) на обработку их ПДн, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона “О персональных данных”;

— выполнение установленных процедур получения согласия субъектов ПДн на передачу обработки их ПДн третьим лицам, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона “О персональных данных”;

— прекращение обработки ПДн и уничтожение либо обезличивание ПДн по достижении целей обработки, по требованию субъекта ПДн в случаях, предусмотренных Федеральным законом “О персональных данных”, в том числе при отзыве субъектом ПДн согласия на обработку его ПДн.

7.6. В Банке должны быть определены, выполняться, регистрироваться и контролироваться процедуры прекращения обработки ПДн и их уничтожения с составлением акта (*приложение 1*) либо обезличивания в сроки, установленные Федеральным законом “О персональных данных”, в следующих случаях:

— по достижении цели обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между организацией БС РФ и субъектом ПДн);

— отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между организацией БС РФ и субъектом ПДн);

— если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

— выявления неправомерной обработки ПДн, осуществляемой Банком или оператором, действующим по его поручению, если обеспечить правомерность обработки ПДн невозможно;

— выявления неправомерной обработки ПДн без согласия субъекта ПДн.

7.7. Банк должен опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, а также к сведениям о реализуемых требованиях по обеспечению безопасности персональных данных.

7.8. При работе с материальными носителями ПДн должно быть обеспечено:

— установление, выполнение и контроль выполнения порядка хранения (архивации), в том числе машинных носителей ПДн и доступа к ним;

— назначение работников, ответственных за организацию хранения материальных носителей ПДн;

— установление и выполнение порядка уничтожения (стирания) информации с машинных носителей ПДн с составлением акта (*приложение 1*).

Хранение (архивация) ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной выгодоприобретателем или поручителем по которому является субъект ПДн.

7.9. Поручение обработки ПДн третьему лицу (далее — обработчик) должно осуществляться на основании договора. В указанном договоре должны быть определены перечень действий (операций) с ПДн, которые будут совершаться обработчиком, и цели обработки, должна быть установлена обязанность обработчика обеспечивать безопасность ПДн (в том числе соблюдать конфиденциальность ПДн) при их обработке, не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом, а также должны быть указаны требования по обеспечению безопасности ПДн. При поручении обработки персональных данных оператору Банк должен получить согласие субъекта ПДн, если иное не предусмотрено законодательством РФ.

8. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ

8.1. Защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральными законами, и представляет собой жестко регламентированный и динамически-технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Банка.

8.2. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

8.3. Для обеспечении защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только президенту Банка, сотрудникам общего отдела и в исключительных случаях, по письменному разрешению президента Банка, - руководителю структурного подразделения (например, при подготовке материалов для аттестации сотрудника).

8.4. Посторонние лица (под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Банка, посетители, сотрудники других организационных структур) не должны знать распределение функций, рабочие процессы, технологию составления,

оформления, ведения и хранения документов, дел и рабочих материалов в общем отделе.

8.5. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

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

8.6. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных сотрудников. (*приложение 2)*

9. ПЕРСОНАЛЬНЫЕ ДАННЫЕ КЛИЕНТОВ

9.1. Получение персональных данных осуществляется преимущественно путем представления их самим клиентом, на основании его письменного согласия, за исключением случаев прямо предусмотренных действующим законодательством РФ.

9.2. Информация персонального характера клиента обрабатывается с соблюдением требований действующего Российского законодательства о защите персональных данных.

9.3. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона № 152 «О персональных данных».

9.4. Передача персональных данных клиентов третьим лицам осуществляется оператором только с письменного согласия клиента, с подтверждающей визой президента Банка, за исключением случаев, если:

1) передача необходима для защиты жизни и здоровья клиента, либо других лиц, и получение его согласия невозможно;

2) по запросу органов дознания, следствия, прокуратуры и суда в связи с проведением расследования или судебным разбирательством, в соответствии с Законом об оперативно-розыскной деятельности;

3) при наличии оснований, позволяющих полагать, что права и интересы клиента могут быть нарушены противоправными действиями других лиц;

4) в иных случаях, прямо предусмотренных Федеральным законодательством.

9.5. Персональные данные клиентов, содержащиеся на материальных носителях, уничтожаются по Акту об уничтожении персональных данных (*приложение 1*).

10. ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Персональные данные субъектов могут быть получены как на бумажных носителях, так и в электронном виде и проходить дальнейшую обработку и передаваться на хранение.

10.2. При получении персональных данных не от субъекта информационных отношений (за исключением случаев, если персональные данные являются общедоступными) оператор до начала обработки таких персональных данных обязан предоставить субъекту следующую информацию:

- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных.

10.3. При передаче персональных данных сотрудника оператор должен соблюдать следующие требования:

10.3.1. Не сообщать персональные данные сотрудника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья сотрудника, а также в случаях, установленных федеральным законом.

10.3.2. Не сообщать персональные данные сотрудника в коммерческих целях без его письменного согласия. Обработка персональных данных сотрудника в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

10.3.3. Передавать персональные данные сотрудника его законным, полномочным представителям в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции.

10.3.4. Предупредить лиц, получивших персональные данные сотрудника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные сотрудника, обязаны соблюдать режим секретности (конфиденциальности).

10.4. Разрешать доступ к персональным данным сотрудника только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

10.5. Не запрашивать информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

10.6. Персональные данные сотрудников на бумажных носителях обрабатываются и хранятся в общем отделе и УБУиО, на электронных носителях в соответствующей ИПДн.

11. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Закрепление прав сотрудника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

11.2. Сотрудники и их представители должны быть ознакомлены под роспись с документами Банка, устанавливающими порядок обработки персональных данных сотрудников, а также об их правах и обязанностях в этой области.

11.3. В целях защиты персональных данных, хранящихся у работодателя, сотрудник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

11.4. Сотрудник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.
- своевременно сообщать работодателю об изменении своих персональных данных.

11.5. Сотрудники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, данные об образовании, профессии, специальности, присвоении нового разряда и других данных, что получает отражение в трудовой книжке на основании представленных документов.

11.6. В целях защиты частной жизни, личной и семейной тайны сотрудники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

11.7. Клиент имеет право на получение информации, касающейся обработки его персональных данных

11.8. Сведения должны быть предоставлены субъекту ПДн оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

11.9. Для своевременной и полной реализации своих прав, клиент обязан предоставить оператору достоверные персональные данные.

12. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ.

12.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

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

12.3. Руководитель, разрешающий доступ сотруднику к конфиденциальному документу с персональными данными, несет персональную ответственность за данное разрешение.

12.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ с персональными данными, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

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

12.5.1. За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению настоящего положения по работе с персональными данными работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

12.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

12.5.3. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на сотрудников.

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

Президент Банка «Йошкар-Ола» (ПАО) Кулалаева О. Г.

Приложение 1

УТВЕРЖДАЮ
Президент
Банка «Йошкар-Ола» (ПАО)
_____
«___»_____20__ г.

Акт об уничтожении персональных данных

Комиссия, созданная в соответствии с требованием федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации, информация, записанная на них в процессе эксплуатации, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего подлежит уничтожению носителей: _____.
(цифрами и прописью)

После утверждения акта, перечисленные носители сверены с записями в акте и на указанных носителях персональные данные уничтожены путем: _____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

После утверждения акта, перечисленные носители сверены с записями в акте и уничтожены путем:
_____.
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Уничтоженные носители с книг и журналов учета списаны.

Председатель комиссии: _____/_____

Члены комиссии: _____/_____

_____/_____

Примечание:

1. Акт составляется раздельно на каждый способ уничтожения носителей.

2. Все листы Акта, а так же все произведенные исправления и дополнения в Акте заверяются подписями всех членов комиссии

Приложение 2

СОГЛАСИЕ
работника на обработку персональных данных

Я, нижеподписавшийся _____
(Ф.И.О. полностью)
зарегистрированный по адресу: _____
_____,
проживающий по адресу: _____,
документ, удостоверяющий личность _____ серия _____ номер _____,
выдан _____
(дата и название выдавшего органа)
своей волей и в своем интересе подтверждаю свое согласие на обработку Банком Йошкар-Ола (ПАО), расположенным по адресу: 424006, Республика Марий Эл, г. Йошкар-Ола, ул. Панфилова, 39Г, моих персональных данных.

Цель обработки персональных данных: в соответствии с требованиями ст.ст. 23, 24 Конституции РФ, статьи 9 Федерального закона от 27.07.06 г. № 152-ФЗ «О персональных данных», на основании ст. 86-90 Трудового Кодекса Российской Федерации, в целях обеспечения соблюдения законодательства Российской Федерации в области персональных данных и иных нормативных правовых актов с учетом положений Федерального закона № 152-ФЗ «О персональных данных», в целях предоставления доступа к сети Интернет, оформления трудовых отношений, расчета и выдачи заработной платы или других доходов, налоговых и пенсионных отчислений, предоставления сведений в рамках договоров медицинского обслуживания, содействия работникам в трудоустройстве, обучении, повышении квалификации и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества работодателя.

Перечень персональных данных, на обработку которых дано настоящее согласие:
- Фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- Число, месяц, год рождения;
- Место рождения;
- Пол;
- Информация о гражданстве (в том числе предыдущие гражданства, причина изменения, иные гражданства);
- реквизиты документа, удостоверяющего личность: серия (при наличии) и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (при наличии), фотография;
- СНИЛС;
- Идентификационный номер налогоплательщика;
- Адрес места жительства (адрес регистрации, фактического проживания);
- Номер контактного телефона или сведения о других способах связи;
- Реквизиты свидетельства государственной регистрации актов гражданского состояния;
- Семейное положение, состав семьи и сведения о близких родственниках;
- Сведения о трудовой деятельности, стаж работы;
- Сведения, содержащиеся в трудовой книжке;
- Сведения о трудовом договоре;
- Сведения о водительском удостоверении;
- Сведения о воинском учете и реквизиты документов воинского учета, воинское звание;
- Информация об участии в воинах (боевых действиях), ликвидация аварий, катастроф, и стихийных действий;
- Информация о социальных льготах, на которые сотрудник имеет право в соответствии с законодательством;

- Сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании, профессия);
- Сведения об ученой степени, ученом звании (когда присвоено, номера дипломов, аттестатов);
- Информация о владении иностранными языками, степень владения;
- Информация, содержащаяся в трудовом договоре;
- Сведения о профессиональной переподготовке и (или) повышении квалификации;
- Информация о наградах (поощрениях), почетных званиях;
- Информация о прохождении аттестации;
- Информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
- Сведения о заработной плате;
- Номер расчетного счета;
- Номер банковской карты;
- Должность субъекта персональных данных;
-Информация о состоянии здоровья;
- Биометрические персональные данные (документы (их копии), характеризующие физиологические и биологические особенности человека);
- Номера приказов и даты о приеме на работу (увольнении), о переводе, о предоставлении отпуска субъекта персональных данных;
- Иные персональные данные, необходимые для достижения целей, предусмотренных Федеральным законом от 27.07.06 г № 152-ФЗ «О персональных данных».

Перечень действий с персональными данными, на совершение которых дается согласие: обработка персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Если распространение (в том числе передача) информации о персональных данных производится в не предусмотренных Федеральным законодательством случаях обязательного предоставления субъектом персональных данных своих персональных данных, оператор обязан запросить письменное согласие клиента в каждом отдельном случае.

Способы обработки персональных данных: на бумажных носителях; в информационных системах персональных данных с использованием и без использования средств автоматизации, а также смешанным способом; при участии и при непосредственном участии человека.

Срок, в течение которого действует согласие: до достижения цели обработки персональных данных или до момента утраты необходимости в их достижении, если иное не предусмотрено Федеральным законодательством.

Настоящее согласие может быть отозвано мной путем подачи в Банк «Йошкар-Ола» (ПАО) письменного заявления об отзыве согласия.

Подтверждаю, что я ознакомлен с Положением об обработке и защите персональных данных в Банке «Йошкар-Ола» (ПАО), права и обязанности в области защиты персональных данных мне разъяснены.

«___» _____ 20___ г. _____ _____

(подпись) (расшифровка подписи работника)