Приложение №6
УТВЕРЖДЕНО
Правлением ООО «Земский банк»
(Протокол №33/19 от 26 сентября 2019 года)

Председатель Правления
ООО «Земский банк»
_____ С.Ю.Зудин

ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ООО «ЗЕМСКИЙ БАНК»

(введена в действие с 01 октября 2019г.)

г. Сызрань, Самарской области
2019г.

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

Автоматизированная банковская система – автоматизированная система, реализующая технологию выполнения функций Банка.

Автоматизированная обработка персональных данных (ПДн) – обработка персональных данных с помощью средств вычислительной техники.

Автоматизированная система[1] **–** система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную поддержку выполнения установленных функций.

Акт определения требуемого уровня защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) – ввнутрибанковский документ, в котором фиксируется результат определения требуемого уровня защищенности персональных данных при их обработке в ИСПДн Банка.

Административно-хозяйственная деятельность – внутрибанковские процессы, направленные на текущее обеспечение деятельности Банка товарно-материальными ценностями (осуществление закупок канцтоваров, офисного оборудования, расходных материалов, хозяйственных товаров, услуг связи и т.п.); на организацию документооборота (ведение архива, библиотек, баз данных); на организацию эксплуатации зданий, помещений, территорий (содержание, уборка, оформление и ремонт помещений); на организацию рабочего процесса.

Банк – Общество с ограниченной ответственность «Земский банк», ООО «Земский банк».

Банковский информационный технологический процесс – часть банковского технологического процесса, реализующая операции по изменению и (или) определению состояния информационных активов, необходимых для функционирования Банка и не являющихся платежной информацией.

Банковский платежный технологический процесс – часть банковского технологического процесса, реализующая банковские операции с информационными активами Банка, связанные с перемещением денежных средств с одного счета на другой и (или) контролем этих операций.

Банковский технологический процесс – технологический процесс, осуществляющий операции по изменению и (или) определению состояния активов Банка, используемых при его функционировании или необходимых для реализации банковских услуг.

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

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

Близкие родственники - являются родственники по прямой восходящей и нисходящей линии (родители и дети, дедушки, бабушки и внуки), полнородные и неполнородные (имеющие общих отца или мать) братья и сестры.

Владелец ИСПДн – владелец информационной системы персональных данных, выполняющий действия в данной системе.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Банка, находящаяся в распоряжении Банка и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Информационная система персональных данных – совокупность содержащихся в

[1] Согласно стандарту Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014), утвержденному распоряжением Банка России от 17.05.2014 № Р-399.

базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств[2]. К информационным системам персональных данных относятся автоматизированные банковские системы, целью создания и использования которых является обработка персональных данных.

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

Клиент – термин, используемый при совместном упоминании Корпоративного клиента и Розничного клиента.

Корпоративный клиент – юридическое лицо, индивидуальный предприниматель, а также физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, заключившее или намеревающееся заключить с Банком договор на оказание услуг.

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) Банка 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 (Предоставление, доступ), Обезличивание, Блокирование, удаление и Уничтожение персональных данных. В рамках Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» установлены следующие определения:

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

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

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

–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.

Оператор – 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.

Определение требуемого уровня защищённости персональных данных при их обработке в ИСПДн - определение одного из четырёх уровней защищённости персональных данных, в соответствии с критериями, установленными постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», которые требуется обеспечить при обработке персональных данных в ИСПДн Банка.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[3].

Примечание. *К ПДн субъекта относятся в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, биометрические характеристики (индивидуальные биометрические характеристики лица, слепок голоса).*

[2] Согласно п. 10 ст. 3 главы 1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».
[3] Согласно п. 1 ст.3 главы 1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Пользователь сайта – лицо, предоставляющее Банку для обработки свои персональные данные с использованием средств web-сайта Банка.

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

Представитель Корпоративного клиента – физическое лицо, персональные данные которого переданы Банку и

–входящее в органы управления Корпоративного Клиента;

–являющееся владельцем/учредителем/акционером/участником Корпоративного клиента;

–действующее от имени Корпоративного клиента на основании доверенности/указанное в карточке с образцами подписей и оттиска печати Корпоративного клиента.

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

Роскомнадзор – уполномоченный орган по защите прав субъектов ПДн.

Розничный клиент – физическое лицо, которое заключило с Банком договор на оказание услуг, включая получение услуг путем присоединения к условиям публичного договора, и персональные данные которого переданы Банку.

Система обеспечения безопасности персональных данных – система правовых, организационных, технических и иных мер по обеспечению доступности, целостности и конфиденциальности персональных данных.

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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

БР ИББС – Банк России – информационная безопасность банковской системы.

ИСПДн – информационная система персональных данных.

ИБ – информационная безопасность.

ПДн – персональные данные.

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1. Настоящая Политика обработки персональных данных ООО «Земский банк» (далее – Политика) регулирует отношения, связанные с обработкой ПДн, осуществляемой Банком с использованием средств автоматизации, в том числе в информационных системах, или без использования таких средств, если обработка ПДн без использования таких средств соответствует характеру действий (операций), совершаемых с ПДн с использованием средств автоматизации, а также вопросы обеспечения безопасности ПДн.

2.2. Политика разработана в целях реализации требований законодательства в области обработки и обеспечения безопасности персональных данных и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в Банке.

2.3. Политика разработана в соответствии с положениями действующих нормативно-правовых актов Российской Федерации, в том числе:

–Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

–Постановления Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

–Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ с учетом изменений и дополнений.

–Постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

–Приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

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

2.4. Действие Политики распространяется на все процессы Банка, связанные с обработкой и защитой ПДн, и ее требования обязательны для применения всеми работниками Банка.

2.5. Положения настоящей Политики являются основой для организации работы по обработке персональных данных в Банке, в том числе, для разработки внутренних нормативных документов 2-го и 3-го уровня (регламентов, методик, технологических схем и пр.), регламентирующих процесс обработки персональных данных в Банке.

2.6. На основании приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Банк включен в реестр операторов, осуществляющих обработку ПДн.

2.7. Политика является общедоступной и подлежит размещению на официальном сайте Банка или иным образом обеспечивается неограниченный доступ к настоящему документу.

2.8. Настоящая Политика размещается на общедоступном ресурсе Банка для общего пользования Работниками Банка.

2.9. В случае изменения законодательства Российской Федерации и принятых в соответствии с ним нормативных правовых актов, изменения или введения в действие стандартов, нормативно-методических рекомендаций, требований уполномоченных органов настоящая Политика применяется в части, не противоречащей вновь принятым нормативным правовым документам.

3. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Банк осуществляет обработку персональных данных на основе общих принципов:

–законности заранее определенных конкретных целей и способов обработки персональных данных;

–обеспечения надлежащей защиты персональных данных;

–соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;

–соответствия объема, характера и 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 баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

–хранения персональных данных в форме, позволяющей определить Субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

–уничтожения или обезличивания персональных данных по достижении целей их обработки, если срок хранения персональных данных не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект персональных данных;

–обеспечения конфиденциальности и безопасности обрабатываемых персональных данных.

3.2. В рамках обработки персональных данных для Субъекта персональных данных и Банка определены следующие права:

3.2.1. Субъект персональных данных имеет право:

−получать информацию, касающуюся обработки его персональных данных, в порядке, форме и сроки, установленные Законодательством о персональных данных;

−требовать уточнения своих персональных данных, их Блокирования или Уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными, не являются необходимыми для заявленной цели обработки или используются в целях, не заявленных ранее при предоставлении Субъектом персональных данных согласия на обработку персональных данных;

−принимать предусмотренные законом меры по защите своих прав;

−отозвать свое согласие на обработку персональных данных.

3.2.2. Банк имеет право:

−обрабатывать персональные данные Субъекта персональных данных в соответствии с заявленной целью;

−требовать от Субъекта персональных данных предоставления достоверных персональных данных, необходимых для исполнения договора, оказания услуги, идентификации Субъекта персональных данных, а также в иных случаях, предусмотренных Законодательством о персональных данных;

−ограничить доступ Субъекта персональных данных к его персональным данным в случае, если Обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, доступ Субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц, а также в иных случаях, предусмотренных законодательством Российской Федерации;

−обрабатывать общедоступные персональные данные физических лиц;

−осуществлять обработку персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации;

−поручить обработку персональных данных другому лицу с согласия Субъекта персональных данных.

4. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Целями обработки ПДн являются:

−выполнение работ, услуг, функций, полномочий и обязанностей, определенных Уставом, лицензиями и внутренними документами Банка, договорных обязательств Банка перед клиентами, предоставления возможности работникам контрагентов Банка выполнения обязанностей, предусмотренных договорами между Банком и его контрагентами;

−осуществление возложенных на Банк законодательством Российской Федерации функций (в том числе по передаче сведений третьим лицам) в соответствии с законодательством Российской Федерации об исполнительном производстве, Налоговым кодексом Российской Федерации, федеральными законами, в том числе: «Об организации предоставления государственных и муниципальных услуг», «О банках и банковской деятельности», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О несостоятельности (банкротстве)», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О кредитных историях», «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»;

−организация учета работников Банка для обеспечения соблюдения законов Российской Федерации и иных нормативных правовых актов, содействие субъектам ПДн в трудоустройстве, обучении, продвижении по службе, очередности предоставления отпусков, расчета размера заработной платы, использования различных форм страхования,

обеспечения пропускного режима Банка, обеспечения личной безопасности работников и сохранности имущества, контроля количества и качества выполняемой работы, пользовании различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, заключенными с субъектами ПДн договорами, а также Уставом и внутренними документами Банка.

5. КЛАССИФИКАЦИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. К персональным данным относится любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (Субъекту персональных данных), обрабатываемая Банком для достижения заранее определенных целей.

5.2. Банк не осуществляет обработку специальных категорий персональных данных, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, интимной жизни физических лиц, если иное не установлено законодательством Российской Федерации.

5.3. Банк вправе осуществлять обработку специальной категории персональных данных, касающейся состояния здоровья Субъекта персональных данных (застрахованных лиц и иных лиц, в случаях предусмотренных действующим законодательством).

5.4. Банк не осуществляет обработку данных о судимостях субъектов, за исключением физических лиц – членов Правления и акционеров, а так же случаев принятия субъекта персональных данных на должность главного бухгалтера и его заместителей, руководителя подразделения Банка, осуществляющего профессиональную деятельность.

5.5. Банк вправе осуществлять обработку биометрических персональных данных с целью идентификации клиентов и работников Банка, при оказании банковских услуг.

5.6. Банк осуществляет обработку персональных данных следующих категорий Субъектов персональных данных:

–физические лица, являющиеся Кандидатами на трудоустройство;

–физические лица, являющиеся Работниками Банка и их близких родственников;

–физические лица, осуществляющие выполнение работ по оказанию услуг и заключившие с Банком договор гражданско-правового характера;

–физические лица, входящие в состав Правления и Совет директоров Банка;

–физические лица, являющиеся Розничными клиентами Банка;

–физические лица, представляющие интересы Корпоративного клиента Банка (Представители Корпоративного клиента);

–физические лица, приобретшие или намеревающиеся приобрести услуги Банка, услуги третьих лиц при посредничестве Банка или не имеющие с Банком договорных отношений при условии, что их персональные данные включены в автоматизированные системы Банка и обрабатываются в соответствии с Законодательством о персональных данных;

–физические лица, не относящиеся к Клиентам Банка, заключившие или намеревающиеся заключить с Банком договорные отношения в связи с осуществлением Банком Административно-хозяйственной деятельности при условии, что их персональные данные включены в автоматизированные системы Банка и обрабатываются в соответствии с Законодательством о персональных данных;

–физические лица, персональные данные которых сделаны ими общедоступными, а их обработка не нарушает их прав и соответствует требованиям, установленным Законодательством о персональных данных;

–иные физические лица, выразившие согласие на обработку Банком их персональных данных или физические лица, обработка персональных данных которых необходима Банку для достижения целей, предусмотренных законодательством Российской Федерации, для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей.

5.7. В процессе своей деятельности Банк осуществляет обработку следующих ПДн:

–фамилия, имя, отчество (в том числе прежние);

–пол;

–дата и место рождения;

–паспортные данные, данные других документов, удостоверяющих личность (серия, номер, дата выдачи, код подразделения, наименование органа, выдавшего документ);

–гражданство;

–статус резидента;

–семейное положение;

–места жительства (адрес регистрации, адрес проживания);

–электронный адрес (e-mail) (при наличии);

–номера контактных телефонов;

–место работы и должность;

–идентификационный номер налогоплательщика;

–номер пенсионного удостоверения;

–информация о счетах, включая информацию об остатках и операциях по ним;

–номера договоров;

–номера кредитных карт;

–сведения о посетителях сайта, cookie – файлы;

–IP-адрес в сети Интернет, используемый Субъектом для взаимодействия с Банком, в том числе для подключения к системе дистанционного банковского обслуживания (Интернет-банк, мобильный банк), а также время осуществления взаимодействия;

–иная информация необходимая Банку для осуществления услуг, согласно заключенному договору.

5.8. Для лиц, изъявивших желание воспользоваться кредитными продуктами, Банк дополнительно осуществляет обработку следующих ПДн:

–образование и профессия;

–уровень платежеспособности (уровень дохода);

–данные, содержащиеся в трудовой книжке;

–контактная информация о текущем и предыдущих местах работы;

–информация о составе семьи;

–информация о финансовом состоянии;

–информация об имущественных правах;

–имевшиеся судебные процессы, решения суда об ограничении дееспособности;

–алиментные обязательства.

5.9. Для лиц, являющихся работниками Банка или проходящих процедуры оформления на работу с целью заключения трудового договора, Банк дополнительно осуществляет обработку следующих ПДн:

–образование и профессия;

–сведения о воинском учете;

–данные, содержащиеся в трудовой книжке;

–контактная информация о текущем и предыдущих местах работы;

–информация о составе семьи;

–фамилии, имена и отчества, даты и места рождения родственников;

–знание иностранных языков (каких и степень знания);

–другая информация, представленная соискателем в резюме (анкете).

6. ОРГАНИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ ПРОЦЕССОМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных Субъекта персональных данных осуществляется с его согласия на обработку персональных данных, а также без такового, если 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 или в иных случаях, предусмотренных Законодательством о персональных данных.

6.2. Обработка специальной категории персональных данных, касающейся состояния здоровья Субъекта персональных данных осуществляется с согласия Субъекта персональных данных на обработку своих персональных данных в письменной форме, а также без такового, если персональные данные сделаны общедоступными Субъектом персональных данных.

6.3. Банк вправе поручить обработку персональных данных другому лицу с согласия Субъекта персональных данных, если иное не предусмотрено федеральным законом. Такая Обработка персональных данных осуществляется только на основании договора, заключенного между Банком и третьим лицом, в котором должны быть определены:

–перечень действий (операций) с персональными данными, которые будут совершаться третьим лицом, осуществляющим обработку персональных данных;

–цели обработки персональных данных;

–обязанности третьего лица соблюдать конфиденциальность персональных данных и обеспечивать их безопасность при обработке, а также требования к защите обрабатываемых персональных данных.

6.4. Банк осуществляет передачу персональных данных государственным органам в рамках их полномочий в соответствии с законодательством Российской Федерации.

6.5. Банк несет ответственность перед Субъектом персональных данных за действия лиц, которым Банк поручает обработку персональных данных Субъекта персональных данных.

6.6. Доступ к обрабатываемым персональным данным предоставляется только тем Работникам Банка, которым он необходим в связи с исполнением ими своих должностных обязанностей и с соблюдением принципов персональной ответственности.

6.7. Обработка персональных данных прекращается при достижении целей такой обработки, а также по истечении срока, предусмотренного законом, договором, или согласием Субъекта персональных данных на обработку его персональных данных. При отзыве Субъектом персональных данных согласия на обработку его персональных данных, Банк вправе продолжить обработку персональных данных без согласия Субъекта персональных данных, если такая обработка предусмотрена договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект персональных данных, иным соглашением между Банком и Субъектом персональных данных, либо если Банк вправе осуществлять обработку персональных данных без согласия Субъекта персональных данных на основаниях, предусмотренных или другими федеральными законами.

6.8. Обработка персональных данных осуществляется с соблюдением конфиденциальности, под которой понимается обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия Субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

6.9. Банк обеспечивает конфиденциальность персональных данных Субъекта персональных данных со своей стороны, со стороны своих Работников, имеющих доступ к персональным данным физических лиц, а также обеспечивает использование персональных данных вышеуказанными лицами исключительно в целях, соответствующих закону, договору или иному соглашению, заключенному с Субъектом персональных данных.

6.10. Обеспечение безопасности обрабатываемых персональных данных осуществляется Банком в рамках единой комплексной системы организационно-технических и правовых мероприятий по защите информации, составляющей банковскую и коммерческую тайну, с учетом требований Законодательства о персональных данных, принятых в соответствии с ним нормативных правовых актов. Система информационной

безопасности Банка непрерывно развивается и совершенствуется на базе требований международных и национальных стандартов информационной безопасности, а также лучших мировых практик.

6.11. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

6.12. Факт подтверждения согласия путем установки соответствующих флагов/переключателей/нажатия кнопок на экранных веб-формах, подтверждающих согласие субъекта с условиями обработки ПДн при заполнении анкет на официальном сайте Банка в целях получения услуг, предоставляемых Банком, расценивается Банком как согласие на обработку ПДн субъектом, даваемое субъектом в письменном виде.

6.13. Согласие на обработку ПДн может быть отозвано субъектом ПДн путем направления в Банк письменного заявления в свободной форме. В этом случае Банк обязуется прекратить обработку, а также уничтожить все имеющиеся в Банке ПДн в сроки, установленные ФЗ «О персональных данных». Банк вправе обрабатывать ПДн без согласия субъекта ПДн (или при отзыве субъектом ПДн указанного согласия) при наличии оснований в соответствии с законодательством Россий Федерации.

6.14. Обработка ПДн Банком осуществляется путем их сбора, записи, систематизации, накопления, хранения, уточнения (обновление, изменение), извлечения, использования, передачи (распространение, предоставление, доступ), обезличивания, блокирования, удаления, уничтожения.

6.14.1. Банк осуществляет обработку ПДн следующими способами:

−автоматизированная обработка (производится при помощи средств вычислительной техники);

−неавтоматизированная обработка (производителя без участия средств вычислительной техники);

−смешанная обработка (производится как при помощи средств вычислительной техники, так и без них).

6.15. Запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных законодательством Российской Федерации.

6.15.1. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.

6.16. В случае необходимости осуществления трансграничной передачи ПДн Банк, перед совершением такой передачи, обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн, а также отсутствии установленных законодательством Российской Федерации запретов или ограничений на передачу ПДн на территорию данного иностранного государства.

6.16.1. Трансграничная передача ПДн на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, может осуществляться Банком в случаях:

−наличия согласия в письменной форме субъекта ПДн;

−исполнения договора, стороной которого является субъект ПДн;

−в иных случаях, установленных законодательством Российской Федерации.

6.17. Обработка персональных данных, осуществляемая без использования средств автоматизации, выполняется таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных

(материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

6.17.1. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Банком без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

6.17.2. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки, которых заведомо несовместимы. Для обработки каждой категории ПДн используется отдельный бумажный носитель.

6.18. Уточнение ПДн, обрабатываемых в Банке осуществляется по запросам субъектов ПДн, их законных представителей или в случае обращения уполномоченного органа по защите прав субъектов ПДн.

6.18.1. Основанием для уничтожения ПДн, обрабатываемых в Банке, является:

−достижение цели обработки ПДн;

−прекращение необходимости в достижении цели обработки ПДн;

−отзыв субъектом ПДн согласия на обработку своих ПДн, за исключением случаев, когда обработка указанных ПДн является обязательной в соответствии с законодательством Российской Федерации или договором, либо обработка может осуществляться без согласия субъекта ПДн;

−выявление неправомерных действий с ПДн и невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты такого выявления;

−истечение срока хранения ПДн, установленного законодательством Российской Федерации и нормативными документами Банка;

−предписание уполномоченного органа по защите прав субъектов ПДн или иного уполномоченного органа.

6.18.2. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае прекращения необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.18.3. Обезличивание ПДн должно осуществляться следующими методами:

−введения идентификаторов, путем замены части сведений идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным;

−изменения состава или семантики данных путем их замены результатами статистической обработки, преобразования, обобщения или удаления части сведений;

−декомпозиции, путем разделения множества (массива) данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;

−перемешивания, путем перестановки отдельных значений или групп значений атрибутов данных в массиве данных.

6.19. При обработке ПДн в ИСПДн с целью обеспечения безопасности ПДн при наличии технической возможности Банк стремится:

−исключать фиксацию на одном материальном носителе ПДн и иных видов информации, а также ПДн, цели, обработки которых заведомо несовместимы;

−для каждой категории ПДн использовать отдельный материальный носитель.

6.20. Сроки обработки ПДн Банком определяются в соответствии со сроком действия договора с субъектом ПДн, сроком исковой давности, Приказом Министерства культуры Российской Федерации 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», а также иными требованиями законодательства Российской Федерации.

6.20.1. Обработка ПДн начинается – с момента их поступления в Банк и прекращается:

−в случае выявления неправомерной обработки ПДн Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты такого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Банка. В случае

невозможности устранения допущенных нарушений Банк в срок, не превышающий десять рабочих дней с даты выявления неправомерности действий с ПДн, уничтожает ПДн или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Банк уведомляет субъекта ПДн или его представителя, а в случае, если обращение или запрос были направлены Роскомнадзором - также этот орган;

–в случае достижения цели обработки ПДн Банк незамедлительно прекращает обработку ПДн и уничтожает соответствующие ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн либо если Банк не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации;

–в случае отзыва субъектом ПДн согласия на обработку своих ПДн Банк прекращает обработку ПДн и уничтожает (за исключением ПДн, которые хранятся в соответствии с действующим законодательством) ПДн в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва. Об уничтожении ПДн Банк уведомляет субъекта ПДн.

6.20.2. Уничтожение ПДн производится в случаях и в сроки, указанные выше, за исключением ПДн бухгалтерского и кадрового учета, которые хранятся в соответствии с действующим законодательством Российской Федерации.

6.20.3. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в п.6.14.1 настоящей Политики, Банк осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7. ОСНОВНЫЕ УЧАСТНИКИ СИСТЕМЫ УПРАВЛЕНИЯ ПРОЦЕССОМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В целях осуществления эффективного управления процессом обработки персональных данных определены основные его участники.

7.1.1. Правление Банка:

–определяет, рассматривает и утверждает политику Банка в отношении обработки персональных данных, а так же внутренние нормативные документы Банка в части обеспечения защиты персональных данных;

–принимает решения по реализации действий Банка, связанных с использованием персональных данных, подверженных риску;

–назначает лиц (-о), ответственных (-ое) за организацию обработки персональных данных и определяет подразделение (-я), ответственное (-ые) за управление процессом обработки персональных данных.

7.2. Лицо, ответственное за организацию обработки и защиту персональных данных, назначается приказом Председателя Правления Банка и выполняет следующие функции:

–разрабатывает, организует и контролирует процесс обработки персональных данных (осуществляемый с использованием средств автоматизации или без использования таких средств, в том числе на бумажных носителях) в соответствии с Законодательством о персональных данных, настоящей Политикой, внутренними нормативными документами Банка;

–осуществляет управление и постоянное совершенствование процесса обработки персональных данных по единым правилам, стандартизацию и тиражирование процесса;

–разрабатывает и представляет для утверждения Председателю Правления Банка внутренние нормативные документы, касающиеся вопросов обработки персональных данных, требований к защите персональных данных;

–организует доведение и (или) доводит до сведения работников Банка положений Законодательства о персональных данных, настоящей Политики, внутренних нормативных

документов Банка по вопросам обработки персональных данных, требований к защите персональных данных;

−осуществляет анализ, оценку и прогноз рисков, связанных с обработкой персональных данных в Банке, выработку мер по снижению рисков;

−осуществляет оценку влияния процессов на права и свободы субъектов персональных данных;

−осуществляет анализ автоматизированных систем и процессов обработки персональных данных на предмет соответствия установленным обязательным требованиям в области обработки и защиты персональных данных;

−осуществляет ведение учета процедур и средств обработки персональных данных;

−осуществляет разработку и организацию применения правовых, организационных и технических мер защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также иных неправомерных действий в отношении персональных данных;

−осуществляет определение угроз безопасности персональных данных при их обработке;

−осуществляет организацию и контроль уровня защищенности информационных систем персональных данных;

−разрабатывает внутренние процедуры, направленные на обеспечение безопасности и защиты персональных данных;

−организует и осуществляет внутренний контроль за соблюдением оператором и его работниками законодательства о персональных данных, настоящей Политики, внутренних нормативных документов Банка, требований к защите персональных данных;

−осуществляет методологическую помощь структурным подразделениям Банка по вопросам взаимодействия с органами государственной власти и надзорными органами по вопросам обработки персональных данных;

−осуществляет взаимодействие с органами государственной власти по вопросам защиты персональных данных;

−осуществляет уведомление надзорного органа в соответствии с применимыми требованиями о фактах утечки персональных данных;

−организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов;

−организует оповещение субъектов персональных данных о фактах утечки их персональных данных;

−делегирует иные функции, предусмотренные для лица, ответственного за организацию обработки персональных данных и защиту персональных данных, законодательством о персональных данных, в профильные подразделения Банка.

7.3. Служба внутреннего аудита:

−в рамках проводимых контрольных процедур оценивает эффективность системы внутреннего контроля Банка по обеспечению соблюдения требований настоящей Политики, а также утвержденных нормативных документов Банка в отношении персональных данных.

7.4. Управление правового обеспечения:

−осуществляет мониторинг законодательства и доведение до сведения заинтересованных подразделений информации об изменении правовых норм;

−осуществляет контроль наличия и полноты содержания договоров поручения на обработку персональных данных, договоров на передачу персональных данных;

−обеспечивает правовую защиту интересов Банка в судах и государственных органах по спорам, связанным с обработкой персональных данных, а также при рассмотрении административных дел, связанных с нарушением законодательства в указанной сфере.

7.5. Комиссия по оценке эффективности принимаемых мер по обеспечения безопасности персональных данных проводит:

–анализ структуры ИСПДн и технологического процесса обработки информации;

–оценка достаточности разработанных внутренних нормативных документов и соответствия их содержания требованиям по обеспечению безопасности информации;

–оценка правильности выбора уровней защищенности ПДн и мер защиты;

–оценка соответствия состава и структуры программно-технических средств ИСПДн представленной документации;

–оценка состояния организации работ и выполнения организационно-технических требований по защите информации;

–оценка достаточности мер физической охраны технических средств информационной системы.

8. ОСНОВНЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. В Банке принимаются следующие меры по обеспечению выполнения обязанностей в отношении ПДн, предусмотренных ФЗ «О персональных данных»:

–назначение ответственного за организацию обработки и защиты ПДн;

–издание документов, определяющих политику Банка в отношении обработки ПДн, локальных актов по вопросам обработки и защиты ПДн;

–применение правовых, организационных и технических мер по обеспечению безопасности ПДн;

–осуществление внутреннего контроля и аудита соответствия обработки ПДн требованиям законодательства Российской Федерации, настоящей Политике, иным локальным актам Банка;

–оценка возможного вреда субъектам ПДн, причиненного в случае нарушения ФЗ «О персональных данных», соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных»;

–ознакомление работников, непосредственно осуществляющих обработку ПДн с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите ПДн, настоящей Политикой и иными локальными актами Банка по вопросам обработки ПДн и (или) обучение указанных работников;

–обеспечение обработки ПДн граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в ФЗ «О персональных данных».

8.2. Обеспечение безопасности ПДн в Банке достигается:

–определением угроз безопасности ПДн при их обработке в ИСПДн;

–применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн;

–применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

–оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

–обеспечением учета и сохранности носителей ПДн;

–обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

–восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

–установлением правил доступа к ПДн, обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

–контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

8.3. Меры по обеспечению безопасности ПДн принимаются для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн и направлены на нейтрализацию актуальных угроз безопасности ПДн.

8.4. Состав и содержание организационных и технических мер безопасности ПДн устанавливается в соответствии с внутренними нормативными документами Банка.

9. ОТВЕТСТВЕННОСТЬ

9.1. Банк, а также его должностные лица и Работники несут гражданско-правовую, административную и иную ответственность за несоблюдение принципов и условий обработки персональных данных физических лиц, а также за разглашение или незаконное использование персональных данных в соответствии с законодательством Российской Федерации.