УТВЕРЖДЕНА

Приказом по АО «Тольяттихимбанк»

№ 93 от 21 июля 2020 г.

ПОЛИТИКА

в отношении обработки персональных данных,
сведения о реализуемых требованиях к защите персональных данных
в АО «Тольяттихимбанк»

Тольятти
2020

Содержание

1. Используемые термины, определения и сокращения

Автоматизированная обработка Персональных данных – **Обработка Персональных данных** с помощью средств вычислительной техники.

База персональных данных – упорядоченный массив **Персональных данных**, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных).

Банк – АО «Тольяттихимбанк».

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**).

Дата-центр – специализированная организация, предоставляющая услуги по размещению серверного и сетевого оборудования, сдаче серверов (в том числе виртуальных) в аренду, а также по подключению к сети Интернет.

Доступ к **Персональным данным –** ознакомление определенных лиц (в том числе работников) с **Персональными данными Субъектов**, **Обрабатываемыми Банком**, при условии сохранения конфиденциальности этих сведений.

Законодательство – законодательство Российской Федерации.

Информационная система персональных данных – совокупность **Персональных данных** содержащихся в **Базах персональных данных** и обеспечивающих их **Обработку** информационных технологий и технических средств.

Контрагент – сторона договора с **Банком**, не являющаяся **Работником Банка**.

Конфиденциальность Персональных данных – обязанность лиц, получивших доступ к **Персональным данным**, не раскрывать их третьим лицам и не **Распространять Персональные данные** без согласия **Субъекта Персональных данных**, если иное не предусмотрено **Законодательством**.

Лицо, ответственное за обеспечение безопасности персональных данных в информационных системах персональных данных – работник **Банка**, в обязанности которого входит организация процессов обеспечения безопасности **Персональных данных** при их **Обработке в Информационных системах персональных данных Банка**.

Лицо, ответственное за организацию обработки персональных данных – работник **Банка**, в обязанности которого входит организация процессов **Обработки Персональных данных** в **Банке**.

Обработка Персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с **Персональными данными**, включая их сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Общедоступные Персональные данные – **Персональные данные**, доступ неограниченного круга лиц к которым предоставлен на основании **Законодательства Субъектом Персональных данных** либо по его просьбе, а также данные, которые подлежат обязательному раскрытию или опубликованию.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее **Обработку Персональных данных**, а также определяющее цели **Обработки Персональных данных**, состав **Персональных данных**, подлежащих **Обработке**, действия (операции), совершаемые с **Персональными данными**; в **Политике** под **Оператором** понимается **Банк**, если иное не указано специально.

Перечень должностей - перечень должностей работников **Банка**, замещение которых предусматривает осуществление **Обработки Персональных данных** либо осуществление **Доступа** к соответствующим **Персональным данным** для выполнения должностных (трудовых) обязанностей.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (**Субъекту Персональных данных**).

Политика – предоставляемый неограниченному кругу лиц и размещаемый на сайте **Банка** в сети Интернет настоящий документ «Политика в отношении обработки персональных данных, сведения о реализуемых требованиях к защите персональных данных».

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

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

Специальные категории Персональных данных – сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья.

Субъект Персональных данных – физическое лицо, к которому относятся **Персональные данные**.

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**.

2. Общие положения

2.1. **Политика** предназначена для доведения до неограниченного круга лиц, пользующихся или желающих воспользоваться продуктами и услугами **Банка** информации об общих принципах, порядке **Обработки Персональных данных** и

содержит описание мер, предпринимаемых **Банком** для обеспечения их безопасности.

2.2. Целью **Политики** является обеспечение защиты прав и свобод человека и гражданина при **Обработке** его **Персональных данных**, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, четкое и неукоснительное соблюдение требований **Законодательства** и международных договоров Российской Федерации в области персональных данных.

2.3. **Политика** разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», другими законодательными и нормативными правовыми актами, определяющими порядок работы с **Персональными данными** и требования к обеспечению их безопасности.

3. Статус банка и категории субъектов, персональные данные которых обрабатываются банком

3.1. В соответствии с определением Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» **Банк** является **Оператором Персональных данных**

3.2. На основании Приказа № 606 от 22.07.2011 Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций **Банк** включен в реестр операторов, осуществляющих **Обработку Персональных данных**. Номер записи в реестре 11-0213170.

3.3. Банк является **Оператором** в отношении **Персональных данных** следующих категорий физических лиц:

- работников **Банка**, с которыми **Банком** заключены или были заключены трудовые договоры, включая бывших работников, с которыми трудовые договоры прекращены (расторгнуты) (далее – **Работники**);
- близких родственников, супругов **Работников Банка** и лиц, находящихся на иждивении **Работников** (далее – **Члены семей работников**);
- соискателей вакантных должностей **Банка** (кандидатов для приема на работу **Банком**), представивших свои резюме или анкеты, содержащие **Персональные данные**, лично или через специализированные организации по подбору персонала (кадровые агентства), в том числе через специализированные сайты в сети Интернет (далее – **Соискатели**);
- клиентов **Банка** – физических лиц (в том числе индивидуальных предпринимателей), включая владельцев банковских счетов, вкладчиков, заемщиков, арендаторов сейфовых ячеек, клиентов по торговым операциям на рынке ценных бумаг, залогодателей и поручителей по кредитам, клиентов разовых услуг (потребителей услуг **Банка**, не требующих открытия счета: обмен валют, денежные переводы, платежи), плательщиков по счетам, лиц, от имени которых осуществляются платежи, держателей основных и дополнительных банковских карт, лиц, которым предоставлена банковская гарантия (далее – **Клиенты**);
- лиц, выразивших желание пройти первичную биометрическую идентификацию и не являющихся **Клиентами** (далее – **Идентифицируемые лица**);

- выгодоприобретателей по договорам, заключенным с **Банком** его **Клиентами** и **Банком** как страховым агентом, в том числе физических лиц, в пользу которых **Клиентом Банка** заключен договор вклада и застрахованных лиц (далее – **Выгодоприобретатели**);
- получателей платежей-физических лиц и их представителей (далее – **Получатели**);
- страхователей и застрахованных лиц по договорам страхования, заключаемым **Банком** как страховым агентом (далее – **Клиенты по страхованию**);
- контрагентов-физических лиц и представителей контрагентов **Банка**, являющихся юридическими лицами и индивидуальными предпринимателями, с которыми у **Банка** существуют договорные отношения, или с которыми он намерен вступить в договорные отношения, или которые намерены вступить в договорные отношения с **Банком**, а также иных лиц (работников, участников (акционеров), учредителей, бенефициаров, выгодоприобретателей, контрагентов, членов руководящих органов, не являющихся работниками, лиц, действующих в интересах контрагента на основании доверенностей и т.д.), **Персональные данные** которых могут передаваться **Банку** в целях заключения и исполнения договоров контрагентами, а также в целях проверки **Банком** контрагентов в качестве благонадежных для заключения с ними договоров и совершения иных сделок и в рамках противодействия легализации (отмыванию) доходов полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (далее – **Представители контрагентов**);
- представителей клиентов-физических лиц, в том числе распорядителей по счетам, наследников, представителей по доверенности, бенефициаров, финансовых и арбитражных управляющих физических лиц-банкротов и иных лиц, действующих от имени и в интересах **Клиентов**, или в пользу которых действуют **Клиенты** (далее – **Представители клиентов**);
- представителей **Субъектов Персональных данных**, не являющихся **Работниками Банка** и обращающихся в **Банк** по поручению и от имени **Субъектов Персональных данных** (далее – **Представители субъектов**);
- незарегистрированных посетителей сайтов **Банка** в сети Интернет (далее – **Посетители сайтов**);
- **Посетителей сайтов Банка** в сети Интернет, выразивших желание сообщить **Банку** свои контактные данные для заказа услуг и обратной связи (далее – **Пользователи сайтов**);
- **Клиентов, Представителей клиентов, Представителей контрагентов, Представителей субъектов** и иных **Субъектов Персональных данных,** выразивших желание использовать предоставляемые **Банком** системы Интернет-банкинга, в том числе мобильные приложения, прошедших для этого при необходимости процедуру предварительной регистрации в системе Интернет-банкинга и предоставивших с этой целью свои **Персональные данные Банку** (далее – **Зарегистрированные пользователи**);
- посетителей охраняемых помещений **Банка**, не имеющих права постоянного входа в эти помещения (далее – **Посетители**).

Субъекты Персональных данных одновременно могут относиться к нескольким категориям, указанным выше, например, являться **Клиентом, Представителем контрагентов, Зарегистрированным пользователем, Посетителем сайтов** и т.п.

3.4. **Банк** является лицом, осуществляющим передачу на регулярной основе **Персональных данных Субъектов** другим **Операторам**, к которым относятся (без ограничения):

- органы власти, местного самоуправления и государственные внебюджетные фонды, в которые перечисляются средства **Работников** или средства для зачисления на счета **Работников** (инспекции Федеральной налоговой службы, территориальные отделения Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования, Фонда социального страхования Российской Федерации и др.);
- Федеральная налоговая служба, которой предоставляется информация по открытым и закрытым счетам;
- регистраторы и номинальные держатели, которым по их запросам предоставляются сведения о владельцах ценных бумаг с целью раскрытия списка владельцев ценных бумаг;
- Банк России, Росфинмониторинг, Государственная корпорация «Агентство по страхованию вкладов», бюро кредитных историй в случаях, когда такая информация должна предоставляться в соответствии с **Законодательством**;
- ПАО «Московская биржа», которой предоставляются список инсайдеров **Банка** по запросу организатора торгов в соответствии с Указанием Банка России № 5129-У от 22.04.2019 и сведения о клиентах при открытии брокерских счетов и при заключении договоров доверительного управления;
- органы статистики, военные комиссариаты, операторы связи, которым такая информация должна предоставляться в соответствии с **Законодательством**.

3.5. Органам власти и государственным внебюджетным фондам, иным органам и организациям, указанным в пункте 3.4, **Персональные данные Предоставляются** (передаются) в объеме, определенном **Законодательством**, соответствующим органам власти, государственным внебюджетным фондом, Банку России в пределах их полномочий. Согласие **Субъектов** на такую передачу **Персональных данных** не требуется.

4. Принципы и цели обработки персональных данных

Обработка Персональных данных Банком осуществляется в соответствии со следующими принципами:

4.1. Законность и справедливая основа **Обработки Персональных данных**. **Банк** принимает все необходимые меры по выполнению требований **Законодательства**, не **Обрабатывает Персональные данные** в случаях, когда это не допускается **Законодательством** и не требуется для достижения определенных **Банком** целей, не использует **Персональные данные** во вред **Субъектам** таких данных.

4.2. Ограничение **Обработки Персональных данных** достижением конкретных, заранее определённых и законных целей. Целями **Обработки Персональных данных Банком** являются:

- в отношении **Работников** – исполнение заключенных трудовых договоров, в том числе содействие в обучении и продвижение по службе, обеспечение личной безопасности **Работников**, контроль количества и качества выполняемой работы; формирование обязательной и управленческой отчетности по персоналу, в том числе отчетов для учёта трудового стажа; обеспечение сохранности имущества; расчет и выплата заработной платы, иных вознаграждений, расчет и перечисление налогов и страховых взносов; предоставление **Работникам** дополнительных услуг за счет работодателя (перечисление доходов на банковские карты **Работников**, страхование за счет работодателя, обеспечение командировок, предоставление парковочного места и пр.), контроль за аффилированностью в случаях, установленных Банком России, выполнение требований нормативных правовых актов органов государственного статистического учета;
- в отношении **Членов семей работников** – предоставление **Работникам** льгот и гарантий, предусмотренных **Законодательством** для лиц, имеющих (усыновивших) детей, лиц с семейными обязанностями; выполнение требований трудового законодательства об информировании родственников о несчастных случаях; страхование **Членов семей работников** частично или полностью за счет **Банка**; выполнение требований нормативных правовых актов органов государственного статистического учета; предоставление в Фонд социального страхования информации для выплаты пособий при рождении ребенка, по уходу за ребенком;
- в отношении **Соискателей** – принятие решения о возможности замещения вакантных должностей **Соискателями**, наиболее полно соответствующими требованиям **Банка**;
- в отношении **Клиентов** – оказание банковских услуг в соответствии с условиями договоров с **Клиентами** и правилами **Банка**, выполнение требований **Законодательства**: об идентификации **Клиентов**, об осуществлении внутреннего контроля в рамках противодействия легализации (отмыванию) доходов полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения; предоставление информации о **Клиентах** лицам, установленным **Законодательством**, взыскание просроченной задолженности по кредиту (займу) в досудебном порядке; соблюдение законодательства Российской Федерации и США о налогообложении иностранных счетов (для клиентов, подпадающих под FATCA);
- в отношении **Идентифицируемых лиц** – предоставление возможности пройти первичную биометрическую идентификацию для включения персональных данных в Единую биометрическую систему;
- в отношении **Выгодоприобретателей** – выполнение условий договоров с **Клиентами** и **Клиентами по страхованию**, идентификация **Выгодоприобретателей** в установленных **Законодательством** случаях;
- в отношении **Получателей** – обеспечение возможности получения платежей **Получателями**;
- в отношении **Клиентов по страхованию** – заключение **Банком** договоров страхования как страховым агентом;

- в отношении **Представителей контрагентов** – заключение и исполнение договоров с контрагентами, проверка **Банком** контрагентов в качестве благонадежных для заключения с ними договоров и совершения иных сделок и в рамках противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения;
- в отношении **Представителей клиентов** – исполнение договоров между **Клиентами** и **Банком**; выполнение требований **Законодательства** об идентификации **Представителей клиентов**;
- в отношении **Представителей субъектов** – выполнение Банком действий по поручению Представителей субъектов персональных данных;
- в отношении **Посетителей сайтов** – информирование **Посетителей сайтов** о деятельности **Банка** и предоставляемых **Банком** услугах; раскрытие информации, в соответствии с требованиями **Законодательства**; профилирование **Посетителей сайтов** с целью повышения удобства навигации по сайту;
- в отношении **Пользователей сайтов** – получение услуг **Банка** и обеспечение обратной связи с **Посетителями сайтов Банка** в сети Интернет, добровольно сообщивших **Банку** свои контактные данные с использованием посещённого сайта;
- в отношении **Зарегистрированных пользователей** – предоставление возможности выполнить при необходимости предварительную регистрацию для использования систем Интернет-банкинга, включая мобильные приложения;
- в отношении **Посетителей** – обеспечение возможности прохода на охраняемую территорию **Банка**.

4.3. **Обработка** только тех **Персональных данных**, которые отвечают заранее объявленным целям их **Обработки**; соответствие содержания и объема **Обрабатываемых Персональных данных** заявленным целям **Обработки**; недопущение **Обработки Персональных данных**, не совместимой с целями сбора **Персональных данных**, а также избыточных по отношению к заявленным целям **Обработки Персональных данных**. **Банк** не собирает и не **Обрабатывает Персональные данные**, не требующиеся для достижения целей, указанных в пункте 4.2 **Политики**, не использует **Персональные данные Субъектов** в каких-либо целях, кроме указанных.

4.4. Недопущение объединения баз данных, содержащих **Персональные данные**, **Обработка** которых осуществляется в целях, не совместимых между собой.

4.5. Обеспечение точности, достаточности и актуальности **Персональных данных** по отношению к целям **Обработки Персональных данных**. **Банк** принимает все разумные меры по поддержке актуальности **Обрабатываемых Персональных данных**, включая (без ограничения) реализацию права каждого **Субъекта** получать для ознакомления свои **Персональные данные** и требовать от **Банка** их уточнения, **Блокирования** или **Уничтожения** в случае, если **Персональные данные** являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленных выше целей **Обработки**.

4.6. Хранение **Персональных данных** в форме, позволяющей определить **Субъекта Персональных данных**, не дольше, чем этого требуют цели **Обработки Персональных данных**, если срок хранения **Персональных данных** не установлен **Законодательством**, договором, стороной которого является **Субъект Персональных данных**, а также согласием **Субъекта Персональных данных** на **Обработку** данных.

4.7. **Уничтожение Персональных данных** по достижении заявленных целей их **Обработки** или в случае утраты необходимости в достижении этих целей, при невозможности устранения **Банком** допущенных нарушений установленного **Законодательством** порядка **Обработки Персональных данных**, отзыве согласия на **Обработку Субъектом Персональных данных**, истечении срока **Обработки Персональных данных**, установленных локальными актами **Банка**, согласием на **Обработку Персональных данных**, если иное не предусмотрено **Законодательством** или договорами с **Субъектами Персональных данных**.

5. Условия обработки персональных данных

5.1. **Обработка Персональных данных Банком** допускается в следующих случаях:

5.1.1. При наличии согласия **Субъекта Персональных данных** на **Обработку** его **Персональных данных**. Порядок получения **Банком** согласия **Субъекта Персональных данных** описан в разделе 8 **Политики**.

5.1.2. **Обработка Персональных данных** необходима для достижения целей, предусмотренных законом, а также для осуществления и выполнения возложенных **Законодательством** на **Банк** функций, полномочий и обязанностей.

5.1.3. Для заключения договора по инициативе **Субъекта Персональных данных** и исполнения договора, стороной которого, **Выгодоприобретателем** или поручителем по которому является **Субъект Персональных данных**. Такими договорами, без ограничения, являются, трудовые договоры с **Работниками**, договоры **Банка** с **Клиентами**.

До момента заключения указанных договоров **Банк** осуществляет **Обработку Персональных данных** на стадии преддоговорной работы при подборе персонала, когда согласие **Субъекта** на **Обработку** подтверждается собственноручно заполненной анкетой **Соискателя** или анкетой (резюме), переданных им **Банку** либо в специализированную организацию по подбору персонала, или размещенных **Соискателем** на специализированных сайтах в сети Интернет, или направленных **Соискателем Банку** по электронной почте, а также при подготовке договоров с **Клиентами**, выразившими намерение получить в **Банке** услуги , в том числе подавшими кредитное заявление.

5.1.4. **Обработка Персональных данных Банком** необходима для осуществления прав и законных интересов **Банка** и/или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы **Субъектов Персональных данных**.

5.1.5. **Обработка Персональных данных** осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания **Персональных данных**.

5.1.6. **Обработка Персональных данных**, доступ неограниченного круга лиц к которым предоставлен **Субъектом Персональных данных** либо по его просьбе.

5.1.7. **Персональные данные** подлежат опубликованию или обязательному раскрытию в соответствии с **Законодательством**.

5.2. **Банк** не раскрывает третьим лицам и не **Распространяет Персональные данные** без согласия **Субъекта Персональных данных**, если иное не предусмотрено **Законодательством**, договором с **Субъектом Персональных данных**, не указано в полученном от него согласии на **Обработку Персональных данных** или **Персональные данные** не сделаны **Субъектом Общедоступными** самостоятельно.

5.3. **Банк** не **Обрабатывает Персональные данные**, относящиеся к специальным категориям и касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, о членстве **Субъектов Персональных данных** в общественных объединениях или их профсоюзной деятельности, за исключением сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения **Работником** трудовой функции и необходимых для целей, определенных законодательством о государственной социальной помощи, законодательством об обязательных видах страхования, трудовым, пенсионным и страховым законодательством.

5.4. **Обработка Персональных данных** о судимости осуществляется **Банком** исключительно в случаях и в порядке, установленных **Законодательством**.

5.5. Во исполнение обязанностей, возложенных на **Банк** требованиями **Законодательства**, он осуществляет сбор регламентированных **Законодательством Биометрических Персональных данных** для их передачи в Единую биометрическую систему.

5.6. При сборе **Персональных данных Банк** обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение **Персональных данных** с использованием баз данных, находящихся на территории **Банка** и в **Дата-центрах** на территории Российской Федерации.

5.7. **Банк** осуществляет **Трансграничную передачу Персональных данных** в целях перевода денежных средств и платежей по счетам клиентов-физических и юридических лиц, индивидуальных предпринимателей в государства, указанные клиентами и/или их представителями, как обеспечивающие, так и не обеспечивающие адекватную защиту прав **Субъектов Персональных данных**.

5.8. **Банк** не принимает решения, порождающие юридические последствия в отношении **Субъектов Персональных данных** или иным образом затрагивающие их права и законные интересы, на основании исключительно **Автоматизированной обработки Персональных данных**. Данные, имеющие юридические последствия или затрагивающие права и законные интересы **Субъекта**, такие как размер начисленных доходов, налогов и иных отчислений и другие, подлежат перед их использованием проверке со стороны уполномоченного работника **Банка**.

6. Способы обработки персональных данных

6.1. **Банк** осуществляет **Обработку Персональных данных** с использованием средств автоматизации, а также без использования таких средств.

6.2. **Политика** распространяется в полном объеме на **Обработку Персональных данных** с использованием средств автоматизации, а при **Обработке Персональных данных** без использования средств автоматизации – на те случаи, когда такая **Обработка** соответствует характеру действий (операций), совершаемых с **Персональными данными** с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск **Персональных данных**, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях **Персональных данных**, и (или) **Доступ** к таким **Персональным данным**.

7. Конфиденциальность персональных данных

7.1. Работниками **Банка**, получившими **Доступ** к **Персональным данным**, должна обеспечивается конфиденциальность таких данных.

Обеспечение конфиденциальности не требуется в отношении **Общедоступных Персональных данных** и данных, прошедших процедуру обезличивания.

7.2. **Банк** вправе с согласия **Субъекта** поручить **Обработку Персональных данных** другому лицу, если иное не предусмотрено **Законодательством**, на основании заключаемого с этим лицом договора поручения на **Обработку Персональных данных**, предусматривающего в качестве существенного условия обязанность лица, осуществляющего **Обработку Персональных данных** по поручению **Банка**, соблюдать принципы и правила **Обработки Персональных данных**, предусмотренные **Законодательством**. Объем передаваемых другому лицу для **Обработки Персональных данных**, действия, выполняемые с **Персональными данными** этим лицом, должны быть минимально необходимыми для выполнения им своих обязанностей перед **Банком**.

В поручении **Банка** должны быть определены перечень действий (операций) с **Персональными данными**, которые будут совершаться лицом, осуществляющим **Обработку Персональных данных**, и цели **Обработки**, должна быть установлена обязанность такого лица соблюдать конфиденциальность **Персональных данных** и обеспечивать безопасность **Персональных данных** при их **Обработке**, а также должны быть указаны требования к защите **Обрабатываемых Персональных данных** в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

При выполнении поручения **Банка** на **Обработку Персональных данных** лицо, которому такая **Обработка** поручена, вправе использовать для **Обработки Персональных данных** свои информационные системы, соответствующие требованиям безопасности, установленным **Законодательством**, что отражается в заключаемом договоре поручения на **Обработку Персональных данных**.

7.3. В случае, если **Банк** поручает **Обработку Персональных данных** другому лицу, ответственность перед **Субъектом Персональных данных** за действия указанного лица несет **Банк**. Лицо, осуществляющее **Обработку Персональных данных** по поручению **Банка**, несет ответственность перед **Банком**.

7.4. **Банк** вправе разместить свои **Информационные системы персональных данных** в **Дата-центре** (облачной вычислительной инфраструктуре), у другого **Оператора**. В этом случае в договор с **Дата-центром** (провайдером облачных услуг, другим **Оператором**) в качестве существенного условия может включаться

требование о запрете доступа персонала **Дата-центра** (провайдера облачных услуг, другого **Оператора**) к **Информационным системам персональных данных Банка**, размещаемых в **Дата-центре** (облачной инфраструктуре, у другого **Оператора**), и тогда такое размещение не рассматривается **Банком** как поручение **Обработки Персональных данных Дата-центру** (провайдеру облачных услуг, другому **Оператору**) и не требует согласия **Субъектов Персональных данных** на такое размещение.

8. Согласие субъекта персональных данных на обработку своих персональных данных

8.1. **Субъект Персональных данных** принимает решение о предоставлении своих **Персональных данных Банку** и дает согласие на их **Обработку** свободно, своей волей и в своем интересе. Согласие на **Обработку Персональных данных** должно быть конкретным, информированным и сознательным и может предоставляться **Субъектом** в любой позволяющей подтвердить факт его получения форме, если иное не установлено **Законодательством**.

8.2. В случае получения **Банком Персональных данных** от контрагента или клиента на основании и в целях заключения и/или исполнения заключенного с ним договора, ответственность за правомерность и достоверность **Персональных данных**, а также за получение согласия **Представителей контрагентов** и **Представителей клиентов** на передачу их **Персональных данных Банку** несет контрагент или **Клиент**, передающий **Персональные данные**, что закрепляется в тексте договора с контрагентом или **Клиентом**.

8.3. **Банк**, получивший **Персональные данные** от контрагента, не принимает на себя обязательства по информированию **Субъектов** (их представителей), **Персональные данные** которых ему переданы, о начале **Обработки Персональных данных**, поскольку обязанность осуществить соответствующее информирование при заключении договора с **Субъектом Персональных данных** и/или при получении согласия на такую передачу несет передавший **Персональные данные** контрагент. Данная обязанность контрагента включается в договор, заключаемый с ним **Банком**.

8.4. Специально выраженного согласия **Работника** на **Обработку** его **Персональных данных** не требуется, так как **Обработка** необходима для исполнения трудового договора, стороной которого является **Работник - Субъект Персональных данных**, за исключением случаев, когда необходимо получение согласия **Работника** в письменной форме для конкретных случаев **Обработки Персональных данных**. К случаям, требующим согласия **Работника** в письменной форме, относятся (без ограничения):

8.4.1. Размещение **Персональных данных Работников** в общедоступных источниках, в том числе на сайтах **Банка** в сети Интернет, за исключением случаев, когда опубликование и обязательное раскрытие **Персональных данных** установлено **Законодательством**.

8.4.2. Получение **Персональных данных Работников** у третьих лиц, в том числе – с целью проверки таких **Персональных данных**, а также в случаях, когда такие данные нельзя получить от самого **Работника**.

8.4.3. Передача **Персональных данных Работника** компаниям, оказывающим на основании договора услуги по покупке проездных документов и бронированию

гостиниц в целях обеспечения проезда к месту командирования, обучения и повышения квалификации и проживания там

8.4.4. Передача **Персональных данных Работника** третьим лицам в коммерческих целях, в том числе – страховым компаниям при заключении и исполнении договоров добровольного медицинского страхования **Работников** за счет **Банка** как работодателя, полиграфическим предприятиям, занимающимся изготовлением визитных карточек (бизнес-карт) **Работников** за счет работодателя, организаторам деловых выставок и конференций, организациям, занимающимся обеспечением командировок, бронированием билетов и гостиниц, компаниям, предоставляющим ключи электронной подписи и т.п.

8.4.5. Передача **Персональных данных Работника** нотариусам для оформления нотариально заверяемых доверенностей от имени **Банка** и совершения иных нотариальных действий.

8.4.6. Передача **Персональных данных Работника** организациям, оказывающим услуги и выполняющим работы по поддержке информационных систем **Банка**, внедрению программных продуктов и баз данных, предназначенных для автоматизации управления и учета в **Банке**.

8.4.7. Передача **Персональных данных** частной охранной организации с целью обеспечения внутриобъектового режима.

8.5. Не требуется согласия **Работников**, в отношении которых **Банком** должен проводиться контроль за их аффилированностью в соответствии с требованиями Банка России, на получение от иных лиц сведений, необходимых для проведения контроля за аффилированностью.

8.6. Специально выраженного согласия **Членов семей работников** не требуется, если **Обработка** их **Персональных данных** осуществляется на основании **Законодательства** (для начисления алиментов, оформления социальных выплат, предоставления льгот и гарантий и пр.), выполняется **Банком** как работодателем в соответствии с требованиями Трудового кодекса РФ и органов государственного статистического учета, а также в случаях, когда **Члены семей работников** являются **Выгодоприобретателями**, в том числе – застрахованными лицами по договорам, заключенным **Банком** как страховщиком в пользу **Членов семей работников**. Во всех остальных случаях необходимо получение доказываемого (подтверждаемого) согласия **Членов семей работников** на **Обработку** их **Персональных данных Банком**.

8.7. Специально выраженного согласия **Соискателей** на **Обработку** их **Персональных данных** не требуется, поскольку такая **Обработка** необходима в целях заключения трудовых договоров по инициативе **Соискателей - Субъектов Персональных данных**, за исключением случаев, когда необходимо получение согласия **Соискателя** в письменной форме для конкретных случаев **Обработки Персональных данных**. **Персональные данные Соискателя**, содержащиеся в его анкете, резюме, электронных письмах, направленных **Банку Соискателем** или специализированными организациями по подбору персонала, и других документах, уничтожаются в течение 30 дней с даты принятия решения о приеме **Соискателя** на работу или об отказе в приеме на работу.

8.8. **Персональные данные** лиц, подписавших договоры с **Банком**, и содержащиеся в единых государственных реестрах юридических лиц и индивидуальных

предпринимателей, являются открытыми и общедоступными, за исключением сведений о номере, дате выдачи и органе, выдавшем документ, удостоверяющий личность физического лица. Охрана их конфиденциальности и согласие **Субъектов Персональных данных** на **Обработку** таких данных не требуется.

Во всех остальных случаях необходимо получение согласия **Субъектов Персональных данных**, являющихся **Представителями контрагентов** или **Представителями клиентов**, за исключением лиц, подписавших договоры с **Банком**, предоставивших доверенности на право действовать от имени и по поручению контрагентов **Банка** и тем самым совершивших конклюдентные действия, подтверждающие их согласие с **Обработкой Персональных данных**, указанных в тексте договора (доверенности). Согласие **Представителя контрагента** или **Представителя клиента** на передачу его **Персональных данных Банку** и **Обработку** им таких данных может получить контрагент или **Клиент** в порядке, описанном в п.8.2 **Политики**. В этом случае получение **Банком** согласия **Субъекта** на **Обработку** его **Персональных данных** не требуется.

8.9. Согласие **Клиентов, Клиентов по страхованию, Получателей, Выгодоприобретателей** на **Обработку** их **Персональных данных** не требуется, поскольку такая **Обработка** необходима для исполнения договора, стороной которого является **Клиент** или **Клиент по страхованию**, для заключения договора по инициативе **Субъекта Персональных данных**, а также выполняется **Банком** в соответствии с требованиями **Законодательства**. Для **Обработки Персональных данных** в целях, выходящих за пределы договора банковского обслуживания, необходимо получение доказываемого согласия **Клиентов**.

8.10. **Идентифицируемые лица** дают свое согласие на обработку **Биометрических персональных данных** в письменной форме или в электронной форме с использованием электронной подписи порядком, установленным нормативными правовыми актами.

8.11. Согласие **Представителей субъектов** на **Обработку** их **Персональных данных** выражается в форме конклюдентных действий путем предоставления доверенности с правом действовать от имени и по поручению **Субъектов Персональных данных** и документа, удостоверяющего личность Представителя субъекта персональных данных.

8.12. Согласие **Пользователей сайтов** дается ими при заполнении форм заказа услуг и обратной связи на сайтах **Банка**.

8.13. Согласие **Зарегистрированных пользователей** дается ими при выполнении предварительной регистрации в системах Интернет-банкинга, в том числе в мобильных приложениях с использованием таких систем.

8.14. Согласие **Посетителей сайтов** на **Обработку** их **Персональных данных**, получаемых **Банком** при просмотре ими страниц сайта **Банка** в сети Интернет дается путем принятия условий «Политики в отношении использования файлов cookie» и простановки соответствующей отметки («галочки») в баннерах на сайтах **Банка** или закрытия баннера.

8.15. Согласие **Посетителей** дается в форме конклюдентных действий – предоставлении ими документа, удостоверяющего личность при проходе на охраняемую территорию **Банка**.

8.16. В случае необходимости получения согласия **Субъекта** на **Обработку Персональных данных** в письменной форме такое согласие может быть получено в форме электронного документа, подписанного электронной подписью в соответствии с требованиями, установленными **Законодательством**.

8.17. Согласие **Субъектов** на предоставление их **Персональных данных** не требуется при получении **Банком**, в рамках установленных полномочий, мотивированных запросов судов, органов прокуратуры, правоохранительных органов, органов следствия и дознания, органов безопасности, государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства, и иных органов, уполномоченных запрашивать информацию в соответствии с компетенцией, предусмотренной **Законодательством**.

Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации.

8.18. В случае поступления запросов от организаций, не обладающих соответствующими полномочиями, **Банк** обязан получить от **Субъекта**, не являющегося **Работником**, согласие на предоставление его **Персональных данных** в любой доказываемой форме и предупредить лиц, получающих **Персональные данные**, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, а также требовать от этих лиц подтверждения того, что указанное правило будет (было) соблюдено. Порядок получения согласия **Работников** на передачу их **Персональных данных** иным лицам описан в пункте 8.4 **Политики**.

8.19. Во всех случаях обязанность предоставить доказательство получения согласия **Субъекта Персональных данных** на **Обработку** его **Персональных данных** или доказательство наличия оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», возлагается на **Банк**.

9. Права субъектов персональных данных

9.1. **Субъект Персональных данных** имеет право на получение информации, касающейся **Обработки** его **Персональных данных**, в том числе содержащей:

- подтверждение факта **Обработки** его **Персональных данных Банком**;
- правовые основания и цели **Обработки Персональных данных**;
- сведения о применяемых **Банком** способах **Обработки Персональных данных**;
- наименование и место нахождения **Банка**, сведения о лицах (за исключением работников **Банка**), которые имеют доступ к **Персональным данным** или которым могут быть раскрыты **Персональные данные** на основании договора с **Банком** или на основании **Законодательства**;
- **Обрабатываемые Персональные данные**, относящиеся к соответствующему **Субъекту Персональных данных**, источник их получения;
- сроки **Обработки Персональных данных**, в том числе сроки их хранения;
- порядок осуществления **Субъектом Персональных данных** прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- информацию об осуществленной или о предполагаемой **Трансграничной передаче** данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего **Обработку Персональных данных** по поручению **Оператора**, если **Обработка** поручена или будет поручена такому лицу;
- иные сведения, предусмотренные **Законодательством**.

Сведения о наличии **Персональных данных** должны быть предоставлены **Субъекту Персональных данных** уполномоченным работником **Банка** в доступной форме, и в них не должны содержаться **Персональные данные**, относящиеся к другим **Субъектам Персональных данных**.

9.2. Запрос **Субъекта** об **Обработке** его **Персональных данных Банком** должен содержать:

- фамилию, имя и отчество **Субъекта Персональных данных** или его представителя;
- номер основного документа, удостоверяющего личность **Субъекта Персональных данных**, а также его представителя (если запрос направлен представителем), сведения о дате выдачи указанного документа (документов) и выдавшем его (их) органе (органах);
- сведения, подтверждающие участие **Субъекта Персональных данных** в отношениях с **Банком** (номер и дата заключения договора с **Банком** и (или) иные сведения, копию (отсканированную, фотографию) сообщения в форме письма или в электронной форме, в виде смс-сообщения, полученных от **Банка** и т.п.), либо сведения, иным образом подтверждающие факт **Обработки Персональных данных Банком**;
- подпись **Субъекта Персональных данных** или его представителя.

При отсутствии в запросе **Субъекта** указанных выше сведений **Банк** вправе отказать в предоставлении запрашиваемых сведений.

9.3. **Субъект Персональных данных** имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

10. Сведения о реализуемых требованиях к защите персональных данных

10.1. Безопасность **Персональных данных**, **Обрабатываемых Банком**, обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований **Законодательства** о персональных данных.

10.2. Правовые меры, принимаемые **Банком**, включают:

- разработку локальных актов **Банка**, реализующих требования **Законодательства** о персональных данных;
- отказ от любых способов **Обработки Персональных данных**, не соответствующих описанным в **Политике** целям и требованиям **Законодательства** о персональных данных**.**

10.3. Организационные меры, принимаемые **Банком**, включают:

- назначение **Лица, ответственного за организацию обработки персональных данных**;
- назначение **Лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных**;
- ограничение состава работников **Банка**, имеющих **Доступ** к **Персональным данным**, и организацию разрешительной системы доступа к ним;
- ознакомление работников **Банка**, непосредственно осуществляющих **Обработку Персональных данных**, с положениями законодательства о персональных данных, в том числе с требованиями к защите **Персональных данных**, с локальными нормативными актами **Банка** по вопросам **Обработки Персональных данных**;
- обучение всех категорий работников **Банка**, непосредственно осуществляющих **Обработку Персональных данных**, правилам работы с ними и обеспечения безопасности обрабатываемых данных;
- организацию учёта материальных носителей **Персональных данных** и их хранения, обеспечивающих предотвращение хищения, подмены, несанкционированного копирования и **Уничтожения**;
- определение типа угроз безопасности **Персональных данных**, актуальных для **Информационных систем персональных данных**, с учетом оценки возможного вреда **Субъектам Персональных данных**, который может быть причинен в случае нарушения требований безопасности, определение уровня защищенности **Персональных данных** и требований к защите **Персональных данных** при их **Обработке** в информационных системах, исполнение которых обеспечивает установленные уровни защищенности **Персональных данных**;
- определение угроз безопасности **Персональных данных** при их **Обработке** в информационных системах, формирование на их основе частной модели (моделей) актуальных угроз;
- размещение технических средств **Обработки Персональных данных** в пределах охраняемой территории;
- ограничение допуска посторонних лиц в помещения **Банка**, недопущение их нахождения в помещениях, где ведется работа с **Персональными данными** и размещаются технические средства их **Обработки**, без контроля со стороны работников **Банка**.

10.4. Технические меры, принимаемые **Банком**, включают:

- разработку на основе частной модели актуальных угроз системы защиты **Персональных данных** для установленных Правительством Российской Федерации уровней защищенности **Персональных данных** при их **Обработке** в информационных системах;
- использование для нейтрализации актуальных угроз средств защиты информации, прошедших процедуру оценки соответствия;

- оценку эффективности принимаемых мер по обеспечению безопасности **Персональных данных**;
- реализацию разрешительной системы **Доступа** работников к **Персональным данным**, **Обрабатываемым** в информационных системах, и к программно-аппаратным и программным средствам защиты информации;
- регистрацию и учёт действий с **Персональными данными** пользователей информационных систем, где **Обрабатываются Персональные данные**;
- предотвращение несанкционированного доступа к **Персональным данным**, выявление возможных случаев такого доступа и принятие мер по ликвидации и (или) локализации последствий такого доступа;
- ограничение программной среды;
- выявление и блокирование воздействия вредоносного программного обеспечения (применение средств защиты по воздействия вредоносного программного обеспечения) на серверах и рабочих станциях **Информационных систем персональных данных**, а также на обладающих соответствующей технической возможностью межсетевых экранах, применяемых для защиты сегментов вычислительных сетей, задействованных для защиты **Информационных систем персональных данных**;
- безопасное межсетевое взаимодействие (применение межсетевого экранирования);
- идентификацию и проверку подлинности пользователя при входе в **Информационную систему персональных данных** по паролю или иному идентификатору;
- контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;
- обнаружение вторжений в информационную систему **Банка**, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности **Персональных данных**;
- защиту среды виртуализации;
- защиту сетевых устройств и каналов связи, по которым осуществляется передача **Персональных данных**;
- восстановление **Персональных данных**, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (создание системы резервного копирования и восстановления **Персональных данных**);
- контроль за выполнением настоящих требований (самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации) не реже 1 раза в 3 года.
- контроль за выполнением настоящих требований (самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации) не реже 1 раза в 3 года.

10.5. При размещении информационной системы в **Дата-центре** (облачной инфраструктуре, у другого **Оператора**) меры безопасности могут быть обеспечены **Дата-центром** (провайдером облачных услуг, другим **Оператором**), что отражается в договоре между **Банком** и **Дата-центром** (провайдером облачных услуг, другим **Оператором**).

11. Заключительные положения

11.2. Иные обязанности и права **Банка** как **Оператора персональных данных** и лица, осуществляющим передачу на регулярной основе **Персональных данных Субъектов** другим **Операторам**, определяются **Законодательством** в области персональных данных.

11.3. Должностные лица и работники **Банка**, виновные в нарушении норм, регулирующих обработку и защиту **Персональных данных**, несут материальную, дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с **Законодательством**.

11.4. **Политика** пересматривается по мере необходимости. Обязательный пересмотр **Политики** проводится в случае существенных изменений действующих в сфере **Персональных данных:** международного законодательства, обязательного для применения **Банком,** законодательства Российской Федерации, национального законодательства иных стран, юрисдикция которого распространяется на деятельность **Банка**.

При внесении изменений в **Политику** учитываются:

- изменения в информационной инфраструктуре и (или) в используемых **Банком** информационных технологиях;
- сложившаяся в Российской Федерации практика правоприменения законодательства в области **Персональных данных**;
- изменение условий и особенностей обработки **Персональных данных Банком** в связи с внедрением в его деятельность новых информационных систем, процессов и технологий;
- изменение направлений деятельности **Банка**;
- изменение состава продуктов и услуг для **Клиентов**.