САРОВБИЗНЕСБАНК
SAROVBUSINESSBANK

«УТВЕРЖДЕНО»

Публичное акционерное общество
"САРОВБИЗНЕСБАНК"

Правлением
ПАО «САРОВБИЗНЕСБАНК»
(Протокол №20 от «16» августа 2018 г.)

Президент
_____И.А. Алушкина

ПОЛИТИКА

№ 32 от «16» августа 2018г.

в отношении обработки персональных данных

1. Общие положения

1.1. Настоящая Политика определяет основные принципы и подходы к обработке и обеспечению безопасности персональных данных и биометрических персональных данных в ПАО “САРОВБИЗНЕСБАНК” (далее – Банк).

1.2. Действие Политики распространяется на все процессы Банка, связанные с Обработкой персональных данных и биометрических персональных данных.

1.3. Настоящая Политика устанавливает обязательные для сотрудников Банка общие требования и правила по работе со всеми видами персональных данных, включая биометрические.

1.4. Политика обязательна для ознакомления и исполнения всеми лицами, допущенными к Обработке персональных данных и биометрических персональных данных в информационных системах персональных данных.

1.5. Политика разработана в соответствии с законодательством Российской Федерации в области персональных данных.

1.6. Настоящая политика является общедоступным документом и размещается на сайте Банка.

2. Перечень используемых нормативных документов

- Трудовой кодекс Российской Федерации;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персо-

нальных данных при их обработке в информационных системах персональных данных»;

- Приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 мая 2017 г. №94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения";
- иные нормативные правовые акты Российской Федерации и нормативные документы исполнительных органов государственной власти.
- Постановление Правительства РФ "Об определении состава сведений, размещаемых в единой системе персональных данных..." №772 от 30.06.2018 г.

3. Список терминов и определений

В данном Порядке используются следующие термины и определения:

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

Биометрические персональные данные (БПДн) - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

Оператор 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.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

сбор;
запись;
систематизацию;
накопление;
хранение;
уточнение (обновление, изменение);
извлечение;
использование;
передачу (распространение, предоставление, доступ);
обезличивание;
блокирование;
удаление;
уничтожение.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

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

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

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

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

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

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

4. Цели сбора и обработки персональных данных.

Основные целями обработки ПДн и БПДн в Банке являются: осуществление Банком банковских операций и иной деятельности, предусмотренной уставом, лицензиями, локальными нормативными актами Банка, нормативными актами Банка России, действующим законодательством и иными нормативными правовыми актами РФ, договорами, либо в рамках иных гражданско-правовых отношений с Банком, организация кадрового учета, обеспечение финансово-хозяйственной деятельности.

5. Перечень категорий субъектов персональных данных и обрабатываемых персональных данных

5.1. Банком осуществляется Обработка полученных в установленном законом порядке ПДн, принадлежащих кандидатам на работу и работникам Банка, клиентам – физическим лицам (владелец счета, открытого в Банке, заемщик, вкладчик, выгодоприобретатель и иные лица, пользующиеся финансовыми услугами Банка), в том числе потенциальным клиентам, представителям клиентов, уполномоченным представлять клиентов; руководителям и главным бухгалтерам юридических лиц, являющихся клиентами Банка (владелец счета, открытого в Банке, заемщик), поручителям, залогодателям, физическим лицам, заключившим с Банком гражданско-правовые договоры на оказание услуг Банку; работникам партнеров Банка, субподрядчиков, поставщиков и других юридических лиц, имеющих договорные отношения с Банком, с которым взаимодействуют работники Банка в рамках своей деятельности; посетителям Банка; бенефициарным владельцам (физическим лицам) клиентов Банка; контрагентам клиентов – физическим лицам.

5.2. Перечень ПДн и БПДн, обрабатываемых в Банке, определяется в соответствии с законодательством Российской Федерации и локальными актами Банка с учетом целей обработки ПДн и БПДн, указанных в разделе 4 Политики.

6. Принципы обработки персональных данных

6.1. Обработка ПДн в банке осуществляется на основе принципов:

- соблюдения законности целей и способов обработки ПДн;
- соответствия содержания ПДн и способов обработки ПДн целям обработки ПДн, заявленным в согласии на обработку Субъекта ПДн;
- обеспечения надлежащей конфиденциальности ПДн;

— поддержки точности и достоверности ПДн;
— недопустимости обработки избыточных ПДн, по отношению к целям, заявленным в согласии Субъекта ПДн;
— недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
— хранения ПДн в форме, позволяющей определить Субъекта ПДн, не дольше, чем этого требуют цели их обработки;
— уничтожения или обезличивания ПДн по достижении целей их обработки, если срок хранения ПДн не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн.

6.2. Обработка ПДн Субъекта ПДн осуществляется с его согласия на обработку ПДн, а также без такового, если обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект ПДн, а также для заключения договора по инициативе Субъекта ПДн или договора, по которому Субъект ПДн будет являться выгодоприобретателем или поручителем или в иных случаях, предусмотренных Законодательством о персональных данных.

6.3. Обработка специальной категории ПДн, касающейся состояния здоровья Субъекта ПДн осуществляется с согласия Субъекта ПДн на обработку своих ПДн в письменной форме, а также без такового, если ПДн сделаны общедоступными Субъектом ПДн.

6.4. Банк вправе поручить обработку ПДн другому лицу с согласия Субъекта ПДн, если иное не предусмотрено действующим законодательством РФ. Такая обработка ПДн осуществляется только на основании договора, заключенного между Банком и третьим лицом, в котором должны быть определены:
— перечень действий (операций) с ПДн, которые будут совершаться третьим лицом, осуществляющим обработку ПДн;
— цели обработки ПДн;
— обязанности третьего лица соблюдать конфиденциальность ПДн и обеспечивать их безопасность при обработке, а также требования к защите обрабатываемых ПДн.

6.5. Банк осуществляет передачу ПДн государственным органам в рамках их полномочий в соответствии с законодательством Российской Федерации.

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

6.7. Банк придерживается аналогичных принципов обработки, изложенных в данной главе и для БПДн.

6.8. Банк вправе осуществлять обработку БПДн с целью оказания банковских услуг и для использования в системе управления и контроля доступа на территории банка.

7. Порядок и Условия обработки персональных данных

7.1. В Банке назначены лица, ответственные за организацию обработки ПДн и осуществление контроля соблюдения требований законодательства РФ по вопросам обработки ПДн.

7.2. Право доступа к ПДн на бумажных и электронных носителях имеют работники банка в соответствии с их должностными обязанностями.

7.3. Обработка сведений о состоянии здоровья осуществляется в соответствии с положениями Трудового кодекса Российской Федерации, ФЗ «Об обязательном медицинском страховании в РФ», а также п.2.3 ч.2 ст.10 ФЗ «О персональных данных».

7.4. Хранение ПДн осуществляется на территории Российской Федерации, в соответствии с ч. 5 ст. 18 Федерального закона "О персональных данных".

8. Права субъектов персональных данных

8.1. Субъект, ПДн которого обрабатываются в Банке, имеет право:

- требовать от Банка уточнения или блокирования его ПДн в следующих случаях: ПДн являются неполными, устаревшими или неточными;
- требовать от Банка уничтожения его ПДн в следующих случаях: ПДн являются устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отозвать свое согласие на обработку ПДн;
- требовать устранения неправомерных действий Банка в отношении его ПДн.

8.2. Субъект ПДн имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки ПДн Банком;
- правовые основания и цели обработки ПДн;
- сведения о применяемых Банком способах обработки ПДн;
- наименование и место нахождения Банка;
- сведения о третьих лицах (за исключением работников Банка), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Банком или на основании федерального закона;
- перечень обрабатываемых ПДн, относящихся к гражданину, от которого поступил запрос и источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления гражданином прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществляемой или о предполагаемой трансграничной передаче ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению банка, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

9. Сведения о реализуемых требованиях к защите персональных данных

9.1. Банк при обработке ПДн принимает необходимые правовые, организационные и технические меры 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.

К защитным мерам в частности, относятся:

- назначение лица, ответственного за организацию обработки ПДн, и лиц, ответственных за обеспечение безопасности ПДн;
- определение угроз безопасности ПДн при их обработке;
- разработка и утверждение локальных актов по вопросам обработки и защиты ПДн;
- оценка вреда, который может быть причинен гражданам в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и прини-

маемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных законом «О персональных данных»;

- работники банка, непосредственно осуществляющие обработку ПДн, ознакомлены с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику банка в отношении обработки ПДн, локальными актами по вопросам обработки ПДн;
- соблюдение условий, исключающих несанкционированный доступ к материальным носителям ПДн и к средствам защиты ПДн;
- применение технических и программных мер защиты ПНд;
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию новой информационной системы Банка;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к ПДн, обрабатываемым в информационных системах Банка, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн;
- осуществление внутреннего контроля и аудита соответствия обработки ПДн Федеральному закону «О персональных данных» и подзаконным нормативным актам.

9.2. Банк принимает аналогичные правовые, организационные и технические меры, изложенные в данной главе и для защиты БПДн.

10. Ответственность

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

Код доступа - 3
Бизнес-процесс – 2.4; 2.1;
Размещение на сайте – да

Начальник отдела
информационной безопасности А.М. Баранов