

ООО КБ «РостФинанс»

УТВЕРЖДЕНО:

Правлением

ООО КБ «РостФинанс»

Протокол № 9 от «20» февраля 2019 г.

ВВЕДЕНО:

Председатель Правления

ООО КБ «РостФинанс»

А.Б. Прохвятилов

Приказ № 1112 от «27» 02 2019 г.



ПОЛОЖЕНИЕ

в отношении обработки персональных данных в информационной системе персональных данных «Взаимодействие с единой биометрической системой»

ООО КБ «РостФинанс»

г. Ростов-на-Дону

2019 год

СОДЕРЖАНИЕ

1. Общие положения	3
2. Цели и принципы обработки персональных данных в ИСПДн «ВЕБС».....	3
3. Правовое основание обработки персональных данных	4
4. Перечень действий с персональными данным, обрабатываемыми в ИСПДн «ВЕБС».....	5
5. Категории субъектов персональных данных.....	5
6. Состав обрабатываемых персональных данных	5
7. Права субъектов персональных данных и их представителей	6
8. Способы обработки персональных данных, применяемые в ИСПДн «ВЕБС».....	7
9. Сроки обработки и хранения персональных данных.....	8
10. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований.....	8
11. Обеспечение безопасности персональных данных.....	10
12. Ответственность за нарушение требований, предъявляемых к обработке персональных данных.....	11

1. Общие положения

Настоящее Положение в отношении обработки персональных данных, обрабатываемых в информационной системе персональных данных «Взаимодействие с единой биометрической системой» ООО КБ «РостФинанс», (далее - ИСПДн «ВЕБС») оператора персональных данных в лице ООО КБ «РостФинанс» (далее - Банк), разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее Федеральный закон № 152-ФЗ), Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации №321 от 25.06.2018г. «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации», постановлениями Правительства Российской Федерации, указами Президента Российской Федерации, иными правовыми актами законодательства Российской Федерации и руководящими документами полномочных органов исполнительной власти Российской Федерации, регламентирующим требованиям, порядок и правила обработки персональных данных.

Настоящее Положение в отношении обработки персональных данных, обрабатываемых в информационной системе персональных данных «Взаимодействие с единой биометрической системой» ООО коммерческого банка «РостФинанс» (далее Положение) служит основой локальных нормативных актов, регламентирующих вопросы обработки персональных данных субъектов, чьи персональные данные обрабатываются в ИСПДн «ВЕБС».

2. Цели и принципы обработки персональных данных в ИСПДн «ВЕБС»

Персональные данные обрабатываются в ИСПДн «ВЕБС» с целью осуществления функций, полномочий и обязанностей, возложенных на Банк ст. 14.1 Федерального Закона №149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. (ред. От 18.12.2018г.), Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации №321 от 25.06.2018г. «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к

информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации», в соответствии с которым сбор параметров биометрических персональных данных производится в целях идентификации гражданина Российской Федерации, в том числе с применением информационных технологий без его личного присутствия.

Обработка персональных данных в ИСПДн «ВЕБС» осуществляется с учетом следующих принципов:

- получение персональных данных осуществляется на законных основаниях;
- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением заранее определенных, законных целей;
- объединение баз данных, содержащих персональные данные, обработка которых осуществляется в несовместимых между собой целях, не допускается;
- обработке подлежат только персональные данные, которые отвечают целям обработки;
- содержание и объем персональных данных соответствует заявленным целям обработки;
- избыточность персональных данных по отношению к заявленным целям не допускается;
- обрабатываемые персональные данные уничтожаются по достижению целей обработки;
- хранение персональных данных осуществляется не дольше, чем требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством, договором, стороной которого является субъект персональных данных.

3. Правовое основание обработки персональных данных

Обработка персональных данных в ИСПДн «ВЕБС» осуществляется на основе следующих федеральных законов и нормативно-правовых актов:

- 1) Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее Федеральный закон № 152-ФЗ).
- 2) Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

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

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

5) Приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации №321 от 25.06.2018г. «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации»

б) Иных нормативных правовых актов Российской Федерации и нормативных документов уполномоченных органов государственной власти.

4. Перечень действий с персональными данным, обрабатываемыми в ИСПДн «ВЕБС»

При обработке персональных данных в ИСПДн «ВЕБС» будут осуществлять следующие действия с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

5. Категории субъектов персональных данных

К категориям субъектов, персональные данные которых обрабатываются в ИСПДн «ВЕБС», относятся физические лица, обратившиеся с запросом или обращением в Банк по вопросам, связанным с реализацией функций и обязанностей, возложенных на Банк приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации №321 от 25.06.2018г.

6. Состав обрабатываемых персональных данных

К персональным данным, обрабатываемым в ИСПДн «ВЕБС» для осуществления возложенных на Банк обязанностей, относятся ПДн физических лиц (граждан Российской Федерации), относящиеся к категориям: биометрических и иные категории ПДн, в составе:

- фамилия, имя, отчество (при наличии);
- пол;
- гражданство;
- дата рождения;
- место рождения;
- реквизиты документа, удостоверяющего личность (серия и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения);
- адрес места жительства (регистрации) или места пребывания;
- идентификационный номер налогоплательщика (ИНН);
- информация о страховом номере индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования (СНИЛС);
- контактная информация (номер абонентского устройства подвижной радиотелефонной связи и адрес электронной почты (при его наличии));
- биометрические данные¹:
 - данные изображения лица субъекта ПДн;
 - данные голоса субъекта ПДн

7. Права субъектов персональных данных и их представителей

Субъекты персональных данных или их представители имеет право на получение информации, касающейся обработки персональных данных, в том числе содержащей:

- подтверждение факта обработки его персональных данных;
- правовые основания и цели обработки персональных данных;
- применяемые способы обработки персональных данных;
- наименование и место нахождения оператора персональных данных, сведения о лицах (за исключением работников оператора персональных данных), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании нормативно-правовых актов, установленных законодательством Российской Федерации;

¹ Биометрические данные: Данные с выходов первичных измерительных преобразователей физических величин, совокупность которых образует биометрический образ конкретного человека (ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.»)

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством Российской Федерации;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению, если обработка персональных данных поручена или будет поручена такому лицу;
- иные сведения, предусмотренные законодательством Российской Федерации, за исключением случаев, когда доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

Информация предоставляется субъекту персональных данных или его представителю при обращении его лично, либо при получении от него письменного запроса в адрес Банка.

Письменный запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в правоотношениях с Банком (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо иные сведения, подтверждающие факт обработки его персональных данных в ИСПДн «ВЕБС»;
- подпись субъекта персональных данных или его представителя.

Письменный запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8. Способы обработки персональных данных, применяемые в ИСПДн «ВЕБС»

В ИСПДн «ВЕБС» применяются следующие способы обработки персональных данных:

- обработка персональных данных без использования средств автоматизации;
- обработка персональных данных с использованием средств автоматизации;

- смешанная обработка персональных данных.

9. Сроки обработки и хранения персональных данных

Общий срок обработки и хранения персональных данных определяется периодом времени, в течение которого Банк осуществляет действия (операции) в отношении персональных данных, обусловленные заявленными целями их обработки, если иной срок не установлен федеральным законом или договором, стороной которого является субъект персональных данных.

Обработка персональных данных прекращается:

- по достижении целей обработки персональных данных;
- в связи с отсутствием необходимости в достижении заранее заявленных целей обработки персональных данных;
- истечением срока согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, установленных федеральным законом или договором, стороной которого является субъект персональных данных.

Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством, договором, стороной которого является субъект персональных данных.

В случае, если персональные данные содержатся в документах Банка, для которых действующими правовыми актами, в том числе в области архивного дела, установлены конкретные сроки хранения, то срок хранения персональных данных приравнивается к установленному сроку хранения документов.

10. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

При достижении цели обработки персональных данных или при наступлении иных законных оснований Банк прекращает обработку персональных данных или обеспечивает прекращение их обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому

является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных, либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом №152-ФЗ или другими федеральными законами.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Банк прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных, либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом №152-ФЗ или другими федеральными законами.

При выявлении неправомерной обработки персональных данных, осуществляемой сотрудником Банка или лицом, действующим по поручению Банка, полномочный сотрудник Банка в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по ее поручению. В случае если обеспечить правомерность обработки персональных данных невозможно, сотрудник Банка в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение.

В случае отсутствия возможности уничтожения персональных данных в течение срока, регламентированного законодательством Российской Федерации, полномочный сотрудник Банка осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка), а также обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

Персональные данные не уничтожаются в случаях, если:

- договором, соглашением, стороной которого, выгодоприобретателем или поручителем является субъект персональных данных, предусмотрен иной порядок обработки персональных данных;
- законодательством установлены сроки обязательного архивного хранения материальных носителей персональных данных;
- в иных случаях, прямо предусмотренных законодательством Российской Федерации.

11. Обеспечение безопасности персональных данных

В целях обеспечения безопасности персональных данных Банк проводит повседневный контроль выполнения требований и правил обработки и обеспечения безопасности персональных данных в ИСПДн «ВЕБС».

Ответственность за проведение контроля выполнения требований и правил обработки и обеспечения безопасности персональных данных возложена на руководителей подразделений Банка, осуществляющих обработку персональных данных, а также на специально назначенных сотрудников Банка, отвечающих за организацию обработки и обеспечение безопасности персональных данных в ИСПДн «ВЕБС».

Выполнение требований и правил обработки и обеспечения безопасности персональных данных обеспечивается выполнением процедур, направленными на выявление и предотвращение нарушений, предусмотренных законодательством РФ, включающих в себя:

- осуществление внутреннего контроля соответствия обработки персональных данных нормам Федерального закона № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам;
- ознакомление лиц, осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе с требованиями по защите персональных данных, определенными нормативными правовыми актами по вопросам обработки персональных данных, а также обучение лиц, осуществляющих обработку персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- постоянный контроль над обеспечением уровня защищенности персональных данных.

При обнаружении нарушений порядка обработки персональных данных обработка персональных данных незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

12. Ответственность за нарушение требований, предъявляемых к обработке персональных данных

Сотрудники Банка, виновные в нарушении норм, регулирующих обработку персональных данных в ИСПДн «ВЕБС», несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством Российской Федерации.

Сотрудники Банка, а также контрагенты и иные участники процессов обработки персональных данных в ИСПДн «ВЕБС», которым в силу их служебного положения или

выполнения работ стали известны обрабатываемые в ИСПДн «ВЕБС» персональные данные, несут ответственность за их разглашение.

Все сотрудники с правом доступа к персональным данным подписывают Обязательство по соблюдению конфиденциальности персональных данных, обрабатываемых в ИСПДн «ВЕБС».

Обязательства по соблюдению конфиденциальности персональных данных, обрабатываемых в ИСПДн «ВЕБС», остаются в силе и после увольнения сотрудника Банка, имевшему ранее право доступа к обрабатываемым в ИСПДн «ВЕБС» персональным данным.