УТВЕРЖДАЮ

Председатель Правления

ООО КБ «РостФинанс»

_____ А.Б. Прохватилов

Протокол №5 от 06.02.2015

ПУБЛИЧНАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО КБ «РОСТФИНАНС»

2015

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящая Политика обеспечения информационной безопасности при обработке персональных данных (далее – Политика) разработана ООО КБ «РостФинанс» (далее – Банк) в целях исполнения требований Федерального закона «О персональных данных» № 152-ФЗ от 27.06.2006 г. Настоящая Политика является общедоступным документом.

1.2. Настоящая Политика определяет содержание и порядок осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ООО КБ «РостФинанс», представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных как с использованием средств автоматизации, так и без использования таких средств, а также устанавливает требования к сбору, хранению, передаче, использованию, уничтожению и любым другим видам обработки персональных данных.

2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

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

2.2. Информационная система персональных данных (ИСПДн): Совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

2.3. Обработка ПДн: Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

2.4. Оператор (ПДн): Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн. Банк выступает как оператор по обработке ПДн.

2.5. Персональные данные (ПДн): Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

2.6. Предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

2.7. Распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц.

2.8. Субъект ПДн — физическое лицо, которое прямо или косвенно определено или определяемо с помощью ПДн.

2.9. Трансграничная передача ПДн: Передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.10. Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Банк, при обработке ПДн, принимает необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от

иных неправомерных действий в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в информационных системах ПДн, установленными действующим законодательством Российской Федерации, регламентирующим вопросы обеспечения информационной безопасности ПДн.

3.2. Безопасность ПДн при их обработке в ИСПДн достигается путем снижения вероятности осуществления несанкционированного доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

3.3. При обработке ПДн в ИСПДн должно быть обеспечено:

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

– своевременное обнаружение фактов несанкционированного доступа к ПДн;

– недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

– возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– непрерывный контроль и анализ уровня защищенности ПДн.

3.4. Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью системы защиты, включающей организационные мероприятия и средства защиты информации (в том числе криптографические средства, средства предотвращения несанкционированного доступа, программно-технических воздействий на технические средства обработки информации), а также используемые в ИСПДн информационные технологии.

4. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с принципами обработки ПДн, указанными в настоящей Политике, в Банке определены состав и цели обработки ПДн, требования к обработке ПДн, а также методы и способы обработки ПДн.

В Банке обрабатываются ПДн следующих категорий субъектов ПДн:

сотрудников; соискателей на вакантные должности; потенциальных клиентов Банка; клиентов – физических лиц; представителей клиентов - юридических лиц; бенефициарных владельцев клиента; выгодоприобретателей – физических лиц; контрагента клиента; физических лиц, в отношении которых имеются сведения об их участии в экстремистской деятельности; представителей контрагентов - юридических лиц; контрагентов банка - физических лиц.

ПДн сотрудников (фамилия, имя, отчество (при наличии), должность, рабочие телефоны, рабочий e-mail, стаж работы в Банке) признаются общедоступными с письменного согласия сотрудников.

Банк осуществляет обработку ПДн с целью обеспечения соответствия требованиям действующего законодательства Российской Федерации, а также ведения учета в кадровом делопроизводстве, рассмотрения резюме и отбора кандидатов на вакантную должность для дальнейшего трудоустройства в Банк, оказания услуг в рамках основной деятельности и исполнения требований законодательства Российской Федерации, оказания услуг в рамках хозяйственной деятельности.

Сотрудники должны быть ознакомлены под подпись с документами Банка, устанавливающими порядок обработки их ПДн, а также их правами и обязанностями в этой области, в соответствии с действующим законодательством Российской Федерации;

Сбор, хранение, использование и распространение ПДн лица не допускаются без его письменного согласия.

Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя:

фамилию, имя, отчество (при наличии); адрес субъекта ПДн; номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе; код подразделения; адрес представителя субъекта ПДн; реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн); наименование или фамилию, имя, отчество (при наличии) и адрес оператора, получающего согласие субъекта ПДн; цель обработки ПДн; перечень ПДн, на обработку которых дается согласие субъекта ПДн; наименование или фамилию, имя, отчество (при наличии) и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу; перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн; срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено действующим законодательством Российской Федерации; подпись субъекта ПДн.

В Банк поступают бумажные носители (документы), содержащие ПДн в виде резюме, автобиографий, справок, анкет и пр. Учет и прием документов осуществляется в соответствии с порядком документооборота кадровых документов в Банке.

Банк также осуществляет периодический сбор ПДн, путем анкетирования субъектов ПДн, либо запросом дополнительных сведений о субъекте ПДн, в рамках заявленных целей обработки ПДн, не противоречащих положениям действующего законодательства Российской Федерации в области обработки и защиты ПДн.

При использовании в Банке форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - форма), выполняются следующие условия:

- в форму или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы и т. д.) включаются сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, наименование и адрес Банка, фамилия, имя, отчество (при наличии) и адрес субъекта ПДн, сведения о документе, удостоверяющем личность, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых в Банке способов обработки ПДн;
- в форму включается поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку ПДн;
- форма составляется таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;
- в форме исключается объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

В Банке обеспечено раздельное хранение ПДн при разных целях обработки и не допускается фиксации на одном бумажном носителе ПДн, цели обработки которых заведомо несовместимы. Для обработки каждой категории ПДн используется отдельный бумажный носитель.

При необходимости использования или распространения определенных ПДн отдельно от находящихся на том же бумажном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн.

Информационные системы ПДн, позволяющие осуществлять обработку ПДн с использованием средств автоматизации в Банке, выявлены, описаны и классифицированы в соответствии с порядком отнесения автоматизированных банковских систем к ИСПДн,

представленного во внутренних документах Банка по обеспечению информационной безопасности. Перечень информационных систем ПДн представлен во внутренних документах Банка по обеспечению информационной безопасности.

Банк осуществляет дополнительное накопление ПДн, получаемых по электронной почте или из общедоступных электронных источников (Интернет сайты организаций - рекрутинговых агентств и т. д.).

При необходимости использования или распространения определенных ПДн отдельно от находящихся на том же машинном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн.

Распространение и передача, в том числе и трансграничная передача ПДн при их обработке в информационных системах осуществляется Банком только по защищенным либо выделенным каналам связи. Банк передает по незащищенным каналам передачи только общедоступные ПДн.

Уничтожение записей, содержащихся на машинных носителях, осуществляется способом исключающим восстановление уничтоженных ПДн.

5. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Права субъекта ПДн

Субъект ПДн имеет право:

– на полную информацию о своих ПДн и о порядке их обработки;

– требовать исключения, исправления или уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или если они не являются необходимыми для заявленной цели обработки, а также данных, обработанных с нарушением требований законодательства Российской Федерации;

– при отказе Банка исключить или исправить ПДн субъекта, он имеет право заявить в письменном виде о своем несогласии с соответствующим обоснованием такого несогласия;

– требовать об извещении Банком всех лиц, которым ранее были сообщены неверные или неполные ПДн субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– определять своих представителей для защиты своих ПДн;

– на доступ к своим ПДн, включая право на получение копии любой записи, содержащей ПДн, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

ПДн оценочного характера субъект ПДн имеет право дополнить заявлением, выражающим его собственную точку зрения.

Банк в целях исполнения положений действующего законодательства Российской Федерации в области обработки и защиты ПДн, предоставляет доступ субъекту ПДн или его законному представителю к ПДн на основании соответствующего запроса.

Запрос субъекта ПДн должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором, собственноручная подпись субъекта ПДн или его представителя. Запрос также может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

При предоставлении информации необходимо руководствоваться документом Банка, определяющим порядок реагирования на запросы субъектов ПДн.

Банк предоставляет субъекту информацию:

- о месте нахождения (адрес оператора);
- о факте обработки ПДн;
- цели обработки ПДн;
- способах обработки ПДн;
- о лицах, осуществляющих обработку ПДн;
- перечень обрабатываемых ПДн и источник получения ПДн.

Сведения о наличии ПДн должны быть предоставлены субъекту ПДн в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

Если Банк принимает решения на основании исключительно автоматизированной обработки ПДн, субъект имеет право требовать разъяснений принимаемых решений, о возможных юридических последствиях таких решений, а также заявлять возражения против принимаемых решений.

Ограничение прав субъекта ПДн:

- Банк не предоставляет доступ к информации субъекту ПДн, если предоставление ПДн нарушает конституционные права и свободы других лиц.

5.2. Обязанности субъекта ПДн

Субъект ПДн обязан предоставлять Банку достоверные ПДн и своевременно сообщать о произошедших в них изменениях.

6. ПРАВА И ОБЯЗАННОСТИ БАНКА

6.1. Права Банка.

Банк имеет право:

- требовать от субъекта ПДн предоставления достоверных сведений о себе в порядке и объеме, предусмотренном законодательством Российской Федерации, а в случае их изменений своевременно уведомлять об этом Банк;
- отказать субъекту ПДн или его законному представителю, уполномоченному органу по защите прав субъектов предоставление доступа к информации по формальным признакам в случае несоответствия порядка предоставления запросов от субъектов и (или) уполномоченного органа по защите прав субъектов ПДн;
- поручать обработку ПДн третьим лицам на договорной основе, с согласия субъекта ПДн.

Банк не имеет право:

- получать и обрабатывать ПДн субъекта ПДн о его политических, религиозных и иных убеждениях и частной жизни;
- получать и обрабатывать ПДн субъекта ПДн о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

6.2. Обязанности Банка.

Для защиты ПДн субъектов, Банк обязан:

- обеспечить защиту ПДн субъекта ПДн от неправомерного их использования или утраты в порядке, установленном действующим законодательством Российской Федерации;
- возложить персональную ответственность за обработку ПДн на сотрудников, допущенных к ПДн и осуществляющих эту обработку;
- осуществлять передачу ПДн субъекта ПДн только в соответствии с настоящей Политикой и законодательством Российской Федерации;

– обеспечить субъекту ПДн доступ к своим ПДн, включая право на получение копий документов, содержащих его ПДн, за исключением случаев, предусмотренных действующим законодательством Российской Федерации;

– по требованию субъекта ПДн предоставить ему полную информацию о его ПДн и обработке этих данных;

– разъяснить субъекту ПДн юридические последствия отказа предоставить свои ПДн, если обязанность предоставления ПДн субъектом установлена действующим законодательством Российской Федерации (включая налоговое, трудовое законодательство).

В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн Банк обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Банк обязан осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

В случае подтверждения факта неточности ПДн Банк на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязан уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

В случае выявления неправомерной обработки ПДн, осуществляемой Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Банка. В случае, если обеспечить правомерность обработки ПДн невозможно, Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Банк обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

В случае достижения цели обработки ПДн Банк обязан прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) 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 действующим законодательством Российской Федерации.

В случае отзыва субъектом ПДн согласия на обработку его ПДн Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн 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 ПДн, иным соглашением между Банком и субъектом ПДн либо если Банк не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных действующим законодательством Российской Федерации.

Сроки обработки ПДн определяются в соответствии со сроком действия договора с субъектом ПДн, сроком исковой давности, сроками хранения документов, установленными Приказом Министерства Культуры Российской Федерации от 25 августа 2010 г. N 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», иными требованиями действующего законодательства Российской Федерации и нормативными документами Банка России, а также сроком предоставленного субъектом ПДн согласия на обработку ПДн, в случаях, когда такое согласие должно быть предоставлено в соответствии с требованиями действующего законодательства Российской Федерации.

До начала обработки ПДн Банк обязан уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона «О персональных данных» № 152-ФЗ от 27.06.2006 г.

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом Банка.