

УТВЕРЖДАЮ:
Председатель Правления
РНКО «Платежный Центр» (ООО)
Г.М. Мац

«18» марта 2019 г.

Соглашение об оказании услуг по переводу денежных средств по номеру карты (Оферта)

Настоящее Соглашение об оказании услуг по переводу денежных средств по номеру карты (далее - Соглашение) является публичной офертой, адресованной заинтересованному иностранному банку или иностранной организации, который(ая) вправе осуществлять операции перевода денежных средств (в том числе, в рамках осуществления банковской деятельности) в соответствии с законодательством страны своего происхождения (инкорпорации) и эмиссию платежных карт международных и/или национальных платежных систем, является стороной Международных переводов «Золотая Корона» (Договора об оказании услуг по переводу денежных средств) (Оферты), а также зарегистрирован(а) на территории страны, указанной в Приложении №1 к Соглашению, и располагает организационными и техническими средствами для возможности взаимодействия с РНКО в целях оказания услуг по зачислению переводов денежных средств по номеру карты (далее – БАНК), и должно рассматриваться как официальное предложение **Расчетной небанковской кредитной организации «Платежный Центр» (общество с ограниченной ответственностью)**, Лицензия Банка России № 3166-К от 14.04.2014 г., именуемой в дальнейшем «РНКО», заключить Соглашение. РНКО и БАНК далее по тексту совместно именуется Стороны, а по отдельности – Сторона.

Настоящее Соглашение может быть заключено Сторонами при условии, что в рамках Корпоративной Информационной Системы «BeSafe» и Правил электронного документооборота корпоративной информационной Системы «BeSafe» (далее – Правила КИС «BeSafe»)) РНКО и БАНК являются клиентами Системы «BeSafe».

Настоящее публичное предложение содержит все существенные условия заключаемого договора. Заключение договора на условиях Соглашения осуществляется путем присоединения БАНКА к Соглашению посредством акцепта публичного предложения в соответствии со ст. 428, п. 2 ст. 437 и п. 3 ст. 438 Гражданского кодекса Российской Федерации. Предложение о заключении договора действует до его отзыва РНКО.

Текст Соглашения размещен в сети Интернет на сайте www.rnko.ru. Настоящее Соглашение в качестве неотъемлемых частей включает в себя Приложения, в том числе Тарифы.

1. ТЕРМИНЫ

- 1.1. Доступ – доступ к конфиденциальной информации, к ПАК и/или Серверам Сторон.
- 1.2. Закрытый ключ – уникальная последовательность символов, однозначно связанная с Открытым ключом, доступная только владельцу TLS-сертификата и предназначенная для аутентификации владельца TLS-сертификата Открытого ключа при организации Защищенного канала связи по технологии протокола TLS.
- 1.3. Защищенный канал связи – канал связи, организованный в соответствии со стандартами PCI DSS по одной из следующих технологий: 1) IPsec (VPN-соединение), для организации которого Стороны используют Ключ, оборудование Cisco и IP-адреса (уникальный идентификатор (адрес) устройства (компьютера), подключенного к локальной сети или сети Интернет), указанные в последнем действующем перечне, оформленном по форме Приложения № 3 к

Соглашению; 2) протокол TLS (Transport Layer Security), для организации которого Стороны используют IP-адреса и TLS-сертификаты, указанные в последних действующих перечнях, оформленных по форме Приложения № 3 и Приложения № 4 к Соглашению соответственно; – для обмена Официальными уведомлениями между Сторонами. Технология организации Защищенного канала связи указывается БАНКОМ в Заявке по форме Приложения №2 к Соглашению.

- 1.4. Карта – платежная карта международных платежных систем MasterCard Worldwide или Visa International, а также платежная карта национальной платежной системы страны инкорпорации БАНКА, эмитированная БАНКОМ, при этом принадлежность Карты к эмиссии БАНКА определяется по наличию банковского идентификационного номера (далее - БИН) Карты в последнем действующем перечне БИНов, оформленном по форме Приложения №7 к Соглашению.
- 1.5. Клиент – физическое лицо - держатель Карты, в пользу которого БАНК зачисляет Перевод на условиях Соглашения.
- 1.6. Ключ Preshared Key (далее – Ключ) – уникальная последовательность символов размерностью от 20 до 159 символов, сформированная Сторонами и предназначенная для аутентификации Сторон при организации Защищенного канала связи по технологии IPsec.
- 1.7. Компрометация Ключа/Ключа Электронной подписи/Закрытого ключа – нарушение конфиденциальности Ключа/Ключа электронной подписи/Закрытого ключа, констатация Стороной обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование Ключа/Закрытого ключа неуполномоченными лицами.
- 1.8. Нерабочий день – любой день с 00:00:00 до 23:59:59 новосибирского времени, кроме Рабочих дней.
- 1.9. Несанкционированный Доступ – несанкционированное получение Доступа неуполномоченными лицами.
- 1.10. Операционный день – Рабочий день либо период времени, включающий в себя Рабочий день и предшествующие ему Нерабочие дни, в течение которого Стороны осуществляют взаимодействие в соответствии с Соглашением.
- 1.11. Открытый ключ – уникальная последовательность символов, однозначно связанная с Закрытым ключом и предназначенная для аутентификации владельца TLS-сертификата при организации Защищенного канала связи по технологии протокола TLS, доступная уполномоченным работникам другой Стороны.
- 1.12. Отправитель - физическое лицо, вступившее в договорные отношения для целей получения услуг по Переводу: 1) с РНКО на основании соответствующих договоров о комплексном обслуживании клиента, текст которых размещен в сети Интернет на сайте <https://rnko.ru>; либо 2) с организациями, в том числе иностранными, вступившими в соответствующие договорные отношения с РНКО и указанными в сети Интернет на сайте <https://koronapay.com>, - в соответствии с Условиями осуществления переводов «Золотая Корона».
- 1.13. Официальное уведомление – электронный документ, сформированный в ПАК Стороны в случаях, установленных Соглашением.
- 1.14. ПАК – программно-аппаратные комплексы Сторон, обеспечивающие информационное и технологическое взаимодействие между Сторонами.
- 1.15. Перевод – действия обслуживающей Отправителя организации и РНКО с целью предоставления Клиенту денежных средств, переведенных Отправителем, а также совершаемые в целях исполнения Официального уведомления РНКО действия БАНКА по осуществлению перевода денежных средств в Сумме перевода по номеру Карты (под номером Карты понимается PAN Карты).
- 1.16. Рабочий день – любой день с 00:00:00 до 23:59:59 новосибирского времени, который не признается в соответствии с законодательством Российской Федерации выходным (суббота, воскресенье) и (или) нерабочим праздничным днем.
- 1.17. Реестр – реестр, составленный по форме, указанной в Приложении №5 к Соглашению, на

основании информации, полученной в Официальном уведомлении БАНКА, содержащий информацию о Переводах, осуществленных БАНКОМ в предыдущем календарном дне (с 00:00:00 до 23:59:59 новосибирского времени).

- 1.18. Серверы – серверы Сторон, для установления взаимодействия между которыми Стороны используют IP-адреса, указанные в последнем действующем документе, оформленном по форме Приложения № 3 к Соглашению.
- 1.19. Системный журнал – база данных, предназначенная для непрерывной регистрации отправки и получения Официальных уведомлений, которыми Стороны обмениваются в рамках Соглашения, а также их хранения. Системный журнал для Официальных уведомлений, формируемых при зачислении перевода по номеру Карты национальных платежных систем, ведет ЗАО «ЗОЛОТАЯ КОРОНА». В остальных случаях каждая Сторона в своем ПАК ведет свой Системный журнал в электронном виде. Системные журналы ведутся в рабочем порядке непрерывно, постоянно, в автоматическом режиме. Формат Системного журнала исключает модификацию и удаление записей о регистрируемых действиях, а также внесение записей способами, не предусмотренными работой ПАК Сторон. Целями ведения Системного журнала являются выявление ситуаций, связанных с несанкционированными действиями, мониторинг событий для осуществления контроля, разрешение спорных и конфликтных ситуаций, связанных с работой в ПАК. Стороны признают информацию, содержащуюся в Системном журнале, достоверной и служащей основанием для разборов спорных вопросов.
- 1.20. Сумма перевода – сумма денежных средств в валюте, указанной в Официальном уведомлении РНКО, подлежащая перечислению в пользу Клиента.
- 1.21. Счет БАНКА – корреспондентский счет БАНКА, реквизиты и валюта которого указаны в Заявке БАНКА по форме Приложения №2 к Соглашению.
- 1.22. Требование о выдаче перевода - волеизъявление Клиента о получении перевода денежных средств, отправленного Отправителем, путем перечисления денежных средств по номеру Карты, составленное, удостоверенное и переданное Клиентом в РНКО в соответствии с условиями договора между Клиентом и РНКО.
- 1.23. Удостоверяющий Центр – Удостоверяющий Центр «AUTHORITY», осуществляющий изготовление Сертификатов, в соответствии с Правилами работы Удостоверяющего Центра «AUTHORITY», размещенными в сети Интернет на сайте www.authority.ru.
- 1.24. Merchant ID – идентификатор электронного устройства БАНКА, зарегистрированный в ПАК БАНКА, используемый в целях исполнения Официального уведомления РНКО и указанный в Заявке БАНКА.
- 1.25. TLS-сертификат – документ на бумажном носителе, заверенный Удостоверяющим Центром, или электронный документ с электронной подписью эмитента (Удостоверяющего Центра) сертификата, содержащий Открытый ключ.
- 1.26. Термины «Ключ электронной подписи», «Ключ проверки электронной подписи», «Сертификат ключа проверки электронной подписи» (далее – Сертификат) и иные термины, используемые в Соглашении, имеют значение, придаваемое им Правилами КИС «BeSafe», размещенными в сети Интернет по адресу www.besafe.ru.

2. ПРЕДМЕТ И ПОРЯДОК ЗАКЛЮЧЕНИЯ СОГЛАШЕНИЯ

- 2.1. Соглашение регулирует:
 - 2.1.1. Порядок и условия зачисления БАНКОМ Перевода по номеру Карты (PAN), а также размер и порядок оплаты вознаграждения БАНКУ.
 - 2.1.2. Порядок и условия осуществления расчетов между Сторонами при исполнении Соглашения.
- 2.2. Присоединение БАНКА к Соглашению осуществляется путем подачи БАНКОМ Заявки по форме Приложения №2 к Соглашению и предоставления РНКО в надлежащей форме документов, перечень которых публично размещен в сети Интернет на сайте www.rnko.ru,

после признания РНКО БАНКА соответствующим требованиям Соглашения, а предоставленных БАНКОМ документов надлежащими и достаточными для заключения договора на условиях Соглашения. Подача Заявки является подтверждением и доказательством ознакомления и согласия БАНКА с условиями Соглашения и не является акцептом на иных условиях.

- 2.3. В течение 5 (Пяти) рабочих дней с момента получения оригинала Заявки РНКО осуществляет проверку соответствия информации, указанной в Заявке, документам БАНКА, проверку возможности ее исполнения, и принимает Заявку к исполнению или отказывает в ее исполнении. Информация о результатах рассмотрения Заявки направляется РНКО БАНКУ письмом в электронном виде по адресу электронной почты БАНКА, указанному в Заявке.
- 2.4. В случае, если в исполнении Заявки будет отказано, Соглашение между Сторонами не будет заключено. РНКО вправе отказать в исполнении Заявки БАНКА без объяснения причин, при этом такой отказ не влечет какую-либо ответственность РНКО перед БАНКОМ. В случае принятия Заявки к исполнению в письме РНКО указывается дата, с которой Соглашение считается заключенным Сторонами. Моментом акцепта публичного предложения и присоединения Банка к Соглашению считается день принятия РНКО Заявки.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. РНКО вправе:

- 3.1.1. Привлекать третьих лиц для исполнения обязательств по Соглашению. При этом полную ответственность перед БАНКОМ за действия таких третьих лиц несет РНКО.
- 3.1.2. В одностороннем внесудебном порядке принимать решения о приостановлении или прекращении деятельности БАНКА в рамках Соглашения в случае нарушения БАНКОМ (в том числе, однократного) условий Соглашения, о чем уведомлять БАНК после приостановления/прекращения деятельности БАНКА в рамках Соглашения, если иной порядок уведомления не будет признан РНКО необходимым.
- 3.1.3. При получении Требования о выдаче перевода в соответствии с условиями договора между Клиентом и РНКО, до формирования Официального уведомления РНКО посредством ПАК РНКО направить в ПАК БАНКА реквизиты Карты национальной платежной системы, введенные Клиентом при формировании Требования о выдаче перевода для проверки принадлежности Карты Клиенту по правилам соответствующей национальной платежной системы.

3.2. РНКО обязуется:

- 3.2.1. Создать Открытый ключ, Закрытый ключ и получить TLS-сертификат в Удостоверяющем Центре, применяемые для организации Защищенного канала связи и передать в БАНК перечень TLS-сертификатов (по форме Приложения № 4 к Соглашению).
- 3.2.2. Принимать и направлять Официальные уведомления через Защищенный канал связи, кроме случаев, когда настоящее Соглашение прямо предусматривает возможность взаимодействия без организации Защищенного канала связи, в порядке, предусмотренном статьей 4 Соглашения.
- 3.2.3. В полном объеме нести ответственность по всем Официальным уведомлениям, сформированным с помощью ПАК РНКО, а также Реестрам.
- 3.2.4. Ежедневно в автоматическом режиме формировать и передавать БАНКУ Реестр по адресу электронной почты БАНКА, указанному в Заявке БАНКА, с целью сверки БАНКОМ расчетов по исполненным на основании Официальных уведомлений Переводам. Передача Реестра по адресу электронной почты БАНКА осуществляется в защищенном виде с помощью Сертификата БАНКА, переданного БАНКОМ в РНКО

по последнему по дате акту приема-передачи Сертификата, составленному по форме Приложения № 6 к Соглашению.

При получении уведомления о Компрометации Ключа Электронной подписи/ Несанкционированном Доступе РНКО обязана приостановить обмен данными с использованием скомпрометированного Ключа ЭП до получения от БАНКА в соответствии с п.3.4.4 Соглашения уведомления об устранении обстоятельств, повлекших Несанкционированный Доступ, и возобновлении информационного обмена.

- 3.2.5. Обеспечивать невозможность Несанкционированного Доступа применительно к ПАК и/или Серверам РНКО и обрабатываемой РНКО конфиденциальной информации.
- 3.2.6. Исключать возможность неквалифицированного обслуживания и ненадлежащего использования ПАК РНКО, в том числе возможность воздействия вредоносных программ на ПАК РНКО, в тех случаях, когда РНКО с использованием необходимых технических/технологических/программных средств могла предотвратить такое воздействие.
- 3.2.7. В течение 5 (Пяти) рабочих дней с момента получения в соответствии с подпунктом 3.4.10 Соглашения Перечня БИНов по форме Приложения № 7 к Соглашению, обеспечить возможность формирования Клиентом Требований о выдаче перевода по номеру Карты с БИНами, указанными в полученном Перечне БИНов.
- 3.2.8. В случае направления БАНКУ мотивированных запросов в электронной форме в виде сканированного документа по электронному адресу БАНКА, указанному в Заявке БАНКА, в последующем досылать оригинал документа на бумажном носителе по почтовому адресу БАНКА, указанному в Заявке БАНКА.

3.3. БАНК вправе:

- 3.3.1. В течение 3 (Трех) рабочих дней, определяемых по законодательству страны инкорпорации БАНКА, с даты получения Реестра, предусмотренного подпунктом 3.2.4 Соглашения, направить РНКО мотивированное возражение по данным, предоставленным в Реестре. Если в указанный срок такое мотивированное возражение не будет направлено БАНКОМ, Реестр считается принятым БАНКОМ. Мотивированное возражение, отправляемое по открытым каналам связи, не должно содержать конфиденциальной информации, в том числе, но не ограничиваясь, полного номера PAN.
- 3.3.2. Привлекать третьих лиц для исполнения обязательств по Соглашению. При этом ответственность перед РНКО за действия таких третьих лиц несет БАНК.

3.4. БАНК обязуется:

- 3.4.1. Принимать и направлять Официальные уведомления через Защищенный канал связи, кроме случаев, когда настоящее Соглашение прямо предусматривает возможность взаимодействия без организации Защищенного канала связи, в порядке, предусмотренном статьей 4 Соглашения.
- 3.4.2. Обеспечивать невозможность Несанкционированного Доступа применительно к ПАК и/или Серверам БАНКА и обрабатываемой БАНКОМ конфиденциальной информации.
- 3.4.3. В целях передачи РНКО Реестров в БАНК, создать Ключ электронной подписи (далее – Ключ ЭП), Ключ проверки электронной подписи (далее – Ключ проверки ЭП), получить для Ключа проверки ЭП Сертификат в Удостоверяющем Центре, и передать в РНКО Сертификат по акту приема-передачи Сертификата, составляемому по форме Приложения № 6 к Соглашению. По истечении срока действия полученного Сертификата или при Компрометации Ключа ЭП или при подозрении на Компрометацию Ключа ЭП, Банк обязуется получить новый Ключ ЭП, Ключ проверки ЭП и Сертификат, а также передать Сертификат в РНКО в порядке, указанном в настоящем пункте.
- 3.4.4. Если у БАНКА имеются основания предполагать, что его Ключ ЭП получен лицом, не обладающим соответствующими полномочиями, БАНК обязан направить уведомление

РНКО о Компрометации Ключа ЭП/ Несанкционированном Доступе по электронному адресу РНКО: support@perevod-korona.com. Датой и временем Компрометации Ключа ЭП / Несанкционированного Доступа считаются дата и время получения такого уведомления РНКО с добавлением времени реагирования на данное уведомление. Время реагирования РНКО на уведомление о Компрометации Ключа ЭП / Несанкционированном Доступе не может превышать 1 (Одного) Рабочего дня. Об устранении обстоятельств, повлекших Несанкционированный Доступ, и возобновлении информационного обмена БАНК уведомляет РНКО с использованием вышеуказанного электронного адреса.

- 3.4.5. Создать Открытый ключ, Закрытый ключ и получить TLS-сертификат в Удостоверяющем Центре, применяемые для организации Защищенного канала связи по протоколу TLS и передать в РНКО перечень TLS-сертификатов (по форме Приложения № 4 к Соглашению).
- 3.4.6. Исключать возможность неквалифицированного обслуживания, ненадлежащего использования или неисправности ПАК БАНКА, в том числе, возможность воздействия вредоносных программ на ПАК БАНКА, в тех случаях, когда БАНК с использованием необходимых технических/технологических/программных средств мог предотвратить такое воздействие.
- 3.4.7. После получения Официального уведомления, Реестра, при осуществлении Перевода обеспечивать конфиденциальность и безопасность полученной информации, в том числе персональных данных субъектов такого Перевода, содержащихся в Официальных уведомлениях и Реестрах, и соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством Российской Федерации и законодательством страны инкорпорации БАНКА. БАНК обязан принимать необходимые организационные и технические меры для защиты конфиденциальной информации, в том числе персональных данных, от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий третьих лиц, в том числе действий, не связанных с исполнением настоящего Соглашения и осуществлением Перевода.
- 3.4.8. Зачислять Перевод без удержания из суммы Перевода и/или взимания с Клиента каких-либо комиссионных сборов.
- 3.4.9. При получении от РНКО зашифрованного Реестра осуществлять его расшифровку и обработку.
- 3.4.10. Информировать РНКО на постоянной основе о БИНах Карт, эмитированных БАНКОМ. В первый раз информирование осуществляется путем подписания и направления БАНКОМ в РНКО Перечня БИНов по форме Приложения № 7 к Соглашению. В случае внесения изменений в БИНЫ БАНК обязуется в течение 5 (Пяти) рабочих дней с момента изменения БИНов подписать со своей стороны обновленный перечень БИНов по форме Приложения № 7 к Соглашению и направить его в электронной форме в виде сканированного документа по адресу РНКО: support@perevod-korona.com с последующей досылкой оригинала документа на бумажном носителе по почтовому адресу РНКО, указанному в сети Интернет на сайте www.rnko.ru.
- 3.4.11. В течение не более 2 (Двух) рабочих дней по законодательству страны инкорпорации БАНКА с момента получения мотивированного запроса РНКО в электронной форме в виде сканированного документа по электронному адресу БАНКА, указанному в Заявке БАНКА, предоставить РНКО информацию, необходимую для рассмотрения претензий Клиентов и формирования ответов на запросы государственных органов, в электронной форме в виде сканированного документа по электронному адресу РНКО: support@perevod-korona.com с последующей досылкой оригинала документа на бумажном носителе по почтовому адресу РНКО, указанному в сети Интернет на сайте www.rnko.ru.

- 3.4.12. Регулярно знакомиться с Соглашением, обеспечивать выполнение его положений своими работниками, а также иными лицами, привлечёнными БАНКОМ для работы в рамках Соглашения.
- 3.4.13. В течение 5 (Пяти) рабочих дней с момента изменения данных, указанных в Заявке БАНКА, направлять в электронной форме в виде сканированного документа по электронному адресу РНКО: support@perevod-korona.com уведомление об изменении данных БАНКА в свободной форме с последующей досылкой оригинала документа на бумажном носителе по почтовому адресу РНКО, указанному в сети Интернет на сайте www.rnko.ru.
- 3.4.14. После получения от ПАК РНКО данных, предусмотренных п. 3.1.3 Соглашения, с использованием ПАК БАНКА незамедлительно передавать их в национальную платежную систему. После получения ответа от национальной платежной системы о принадлежности/отсутствии принадлежности Карты Клиенту, ПАК БАНКА незамедлительно передает в ПАК РНКО такой ответ национальной платежной системы в целях проведения РНКО идентификации Клиента в соответствии с действующим законодательством Российской Федерации.
- 3.5. Стороны договорились считать подлинными Сертификат, предназначенный для шифрования Реестров, полученный РНКО от БАНКА по акту приема-передачи, составленному по форме Приложения № 6, и зашифрованный на этом Сертификате Реестр, полученный БАНКОМ от РНКО по адресу электронной почты, указанному в Заявке БАНКА.

4. ПОРЯДОК ЗАЧИСЛЕНИЯ ПЕРЕВОДА ПО НОМЕРУ КАРТЫ

- 4.1. При получении Требования о выдаче перевода в соответствии с условиями договора между Клиентом и РНКО, а для Карт национальных платежных систем дополнительно – при получении от ПАК БАНКА положительного ответа национальной платежной системы, РНКО посредством ПАК РНКО формирует Официальное уведомление, содержащее, в том числе, Merchant ID, PAN Карты, Сумму перевода, валюту, ФИО Клиента, ФИО Отправителя, адрес регистрации Отправителя, и направляет его БАНКУ.
- 4.2. При получении Официального уведомления РНКО БАНК незамедлительно осуществляет проверку Карты на наличие возможности зачисления Суммы перевода по PAN Карты, определенному в Официальном уведомлении РНКО.
- 4.3. При положительном результате проверки Карты БАНК:
- 4.3.1. Незамедлительно зачисляет Перевод в Сумме перевода по PAN Карты, определенному в Официальном уведомлении РНКО.
- 4.3.2. После зачисления Перевода БАНК с использованием ПАК БАНКА незамедлительно формирует Официальное уведомление БАНКА о зачислении Перевода, содержащее, в том числе PAN Карты, код авторизации, и направляет его РНКО.
- 4.4. При отрицательном результате проверки Карты БАНК незамедлительно с использованием ПАК БАНКА формирует Официальное уведомление БАНКА о невозможности зачислить Перевод и направляет его РНКО.
- 4.5. Для обеспечения информационного и технологического взаимодействия между Сторонами в части обмена Официальными уведомлениями с использованием ПАК Сторон РНКО привлекает ЗАО «ЗОЛОТАЯ КОРОНА». РНКО признает, что все действия, совершенные ЗАО «ЗОЛОТАЯ КОРОНА», считаются действиями РНКО, за которые РНКО несет всю полноту ответственности. В случае организации Защищенного канала связи по технологии IPSec, БАНК обязуется заключить с ЗАО «ЗОЛОТАЯ КОРОНА» соглашение, в рамках которого БАНК и ЗАО «ЗОЛОТАЯ КОРОНА» организуют между ПАК Сторон Защищенный канал связи для обмена Официальными уведомлениями и определяют порядок такого обмена между ПАК Сторон. Взаимодействие Сторон в целях осуществления Перевода по PAN Карты национальных платежных систем допускается исключительно при привлечении БАНКОМ ЗАО

«ЗОЛОТАЯ КОРОНА» для обмена Официальными уведомлениями с использованием ПАК и обеспечивается без организации Защищенного канала связи.

5. РАЗМЕР И ПОРЯДОК ОПЛАТЫ ВОЗНАГРАЖДЕНИЯ

- 5.1. Размер вознаграждения БАНКА за оказание услуги по осуществлению Перевода указан в Тарифах к Соглашению (Приложение №8 к Соглашению). БАНК соглашается с тем, что размеры вознаграждения БАНКА могут различаться в зависимости от территории, где Отправителю были оказаны услуги по Переводу, а также вида договора, на основании которого Отправителю были оказаны соответствующие услуги.
- 5.2. На момент размещения текста Соглашения в сети Интернет на сайте www.rnko.ru, вознаграждение БАНКА не облагается в Российской Федерации налогом на добавленную стоимость на основании статей 146 и 148 Налогового кодекса Российской Федерации и не облагается налогом на прибыль на основании пункта 2 статьи 309 Налогового кодекса Российской Федерации.
В случае изменения законодательства Российской Федерации, предусматривающего какие бы то ни было вычеты/удержания с платежей, подлежащих перечислению БАНКУ, вознаграждение БАНКА подлежит увеличению таким образом, чтобы сумма, подлежащая перечислению БАНКУ, соответствовала сумме вознаграждения БАНКА, предусмотренной условиями Соглашения, которую получил бы БАНК в случае отсутствия таких вычетов и удержаний.
- 5.3. БАНК принимает на себя все обязательства, касающиеся уплаты налогов, подлежащих уплате в стране инкорпорации БАНКА при оказании услуг по осуществлению Перевода, включая, но, не ограничиваясь, с вознаграждения БАНКА, выплачиваемого РНКО Банку.
- 5.4. Вознаграждение БАНКА, предусмотренное пунктом 5.1 Соглашения, рассчитывается по каждому осуществленному Переводу.
- 5.5. Уплата вознаграждения БАНКА осуществляется в соответствии со статьей 6 Соглашения.

6. ПОРЯДОК РАСЧЕТОВ

- 6.1. На основании Официального уведомления БАНКА о зачислении Перевода, полученного от БАНКА, РНКО формирует распоряжение на Сумму перевода и распоряжение на сумму вознаграждения БАНКА за осуществление Перевода в валюте, указанной в соответствующем Официальном уведомлении.
- 6.2. На основании сформированных распоряжений, предусмотренных пунктом 6.1 Соглашения, РНКО безусловно перечисляет на Счет БАНКА в соответствующей валюте Перевода в полном объеме причитающуюся БАНКУ Сумму переводов и соответствующее вознаграждение БАНКА, определенное в соответствии с Тарифами к Соглашению, в течение Операционного дня, следующего за календарным днем (с 00:00:00 до 23:59:59 новосибирского времени) зачисления БАНКОМ таких Переводов. Операции за выходные дни включаются в расчеты первого рабочего дня РНКО. В случае, если Операционный день является выходным днем в стране инкорпорации БАНКА, либо стране банка корреспондента, РНКО перечисляет денежные средства в первый рабочий день в стране инкорпорации БАНКА, стране банка корреспондента, соответственно.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

- 7.1. За неисполнение или ненадлежащее исполнение условий Соглашения Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.
- 7.2. Сторона, допустившая нарушение обязательств по Соглашению, обязуется возместить реальный ущерб, причиненный другой Стороне, возникший вследствие неисполнения либо ненадлежащего исполнения обязательств Стороной.
- 7.3. Возмещение ущерба не освобождает Стороны от исполнения принятых по Соглашению

обязательств.

- 7.4. Стороны договорились, что не несут ответственность друг перед другом в случае неисполнения обязательств в результате сбоев, поломок и неполадок в ПАК, аппаратуре, системах, каналах связи и программах, которые Стороны не могли контролировать или предупредить разумными методами, которые препятствуют осуществлению Сторонами своих обязательств по Соглашению.

8. ПОРЯДОК ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

- 8.1. При направлении и получении Сторонами Официальных уведомлений привлеченное Сторонами лицо выполняет требования стандарта PCI DSS. Получение и использование средств создания и проверки Сертификата и TLS-сертификата Сторонами должно осуществляться в соответствии с условиями Правил Удостоверяющего центра «AUTHORITY», которые размещены в сети Интернет по адресу: www.authority.ru. Электронный документооборот осуществляется в соответствии с Правилами КИС «BeSafe», размещенными в сети Интернет на сайте www.besafe.ru.
- 8.2. Электронный документооборот может включать:
- 8.2.1. Формирование Официальных уведомлений в формате, предусмотренном ПАК Сторон.
 - 8.2.2. Отправление и доставку Официальных уведомлений.
 - 8.2.3. Учет Официальных уведомлений.
 - 8.2.4. Хранение Официальных уведомлений (ведение архивов Официальных уведомлений).
- 8.3. Отправление и доставка Официальных уведомлений:
- 8.3.1. Официальное уведомление считается исходящим от Стороны, если Официальное уведомление отправлено:
 - 8.3.1.1. самой Стороной;
 - 8.3.1.2. от имени Стороны запущено автоматическим процессом, который представляет собой часть ПАК этой Стороны.
- 8.4. Учет Официальных уведомлений осуществляется путем ведения Системных журналов. Технология ведения Системных журналов должна включать программно-технологические процедуры заполнения и администрирования Системных журналов и средства хранения этой информации.
- 8.5. Хранение Официальных уведомлений должно сопровождаться хранением соответствующих Системных журналов и программных средств, обеспечивающих возможность работы с Системными журналами.
- 8.6. Системные журналы должны храниться в электронных архивах. Электронные архивы подлежат защите от Несанкционированного Доступа и преднамеренного или непреднамеренного уничтожения и/или искажения. Срок хранения Системных журналов не может быть менее 5 (Пяти) лет.
- 8.7. Для направления и получения Официальных уведомлений через Защищенный канал связи, Стороны обязаны использовать исключительно IP-адреса и в случае его организации по протоколу TLS TLS-сертификаты, указанные в последних действующих перечнях, оформленных по форме Приложения № 3 и Приложения №4 к Соглашению соответственно. При изменении IP-адресов одной из Сторон Сторона, IP-адрес которой изменился, присылает другой Стороне новый перечень IP-адресов, а с момента его получения предыдущие перечни IP-адресов утрачивают свою силу.
- 8.8. При смене Ключа/Закрытого ключа, в случаях Компрометации Ключа/Закрытого ключа Стороны формируют новый Ключ/Закрытый и Открытый ключ и перенастраивают Защищенный канал связи.
- 8.8.1. В случае организации Защищенного канала связи по технологии протокола TLS по окончании срока действия TLS-сертификата, при изменении данных, позволяющих установить владельца TLS-сертификата, содержащихся в последнем действующем

перечне TLS-сертификатов (по форме Приложения № 4 к Соглашению), в случаях Компрометации, иных обстоятельствах, приводящих к смене Открытого ключа и Закрытого ключа, владельцу TLS-сертификата надлежит получить новый TLS-сертификат. В данном случае Сторона, данные TLS-сертификата которой изменились, предоставляет другой Стороне новый перечень TLS-сертификатов с указанием данных, предусмотренных Приложением № 4 к Соглашению. С момента получения другой Стороной нового перечня TLS-сертификатов Стороны предыдущие перечни утрачивают свою силу.

- 8.9. Стороны подтверждают и гарантируют, что при любых обстоятельствах лица, имеющее доступ к ПАК и/или Серверам Стороны, в том числе работники привлеченной согласно подпунктов 3.1.1, 3.3.2 и пункта 4.5 Соглашения организации, обладают полномочиями на совершение ими действий с помощью ПАК/Серверов Стороны и отправку/получение Официальных уведомлений.
- Такие действия считаются действиями Стороны, учитывая, в том числе, потенциальную возможность совершения таким лицом ошибок, а также Компрометации Ключа или получение Доступа неуполномоченными лицами. Сторона несет самостоятельную ответственность за Несанкционированный Доступ на ее стороне.
- 8.10. Если у Стороны имеются основания предполагать, что на ее стороне Ключ Стороны / Закрытый ключ/ Доступ может быть использован / получен лицом, не обладающим соответствующими полномочиями, Сторона обязана направить уведомление другой Стороне о Компрометации Ключа / с указанием идентифицирующей его информации (например, значения соответствующего Открытого ключа или TLS-сертификата) / Несанкционированном Доступе по электронному адресу БАНКА, указанному в Заявке БАНКА, или электронному адресу РНКО: support@perevod-korona.com. Датой и временем Компрометации Ключа / Закрытого ключа / Несанкционированного Доступа считаются дата и время получения такого уведомления другой Стороной с добавлением времени реагирования на данное уведомление. Время реагирования Сторон на уведомление о Компрометации Ключа / закрытого Ключа / Несанкционированном Доступе другой Стороны не может превышать 1 (Одного) Рабочего дня. Сторона, получившая уведомление о Компрометации Ключа / Закрытого ключа / Несанкционированном Доступе обязана приостановить обмен данными с использованием скомпрометированного Ключа/Закрытого ключа/ПАК Стороны. Об устранении обстоятельств, повлекших Несанкционированный Доступ, и возобновлении информационного обмена Сторона, направившая уведомление о Несанкционированном Доступе уведомляет другую Сторону с использованием вышеуказанных электронных адресов.
- 8.11. Официальное уведомление одной Стороны, отправленное по Защищенному каналу связи, организованному с использованием скомпрометированного Ключа/Закрытого ключа, или отправленные в результате Несанкционированного Доступа Стороны, признается ненадлежащим и не порождает никаких последствий для Сторон только в том случае, когда такое Официальное уведомление получено принимающей Стороной позже даты и времени получения уведомления о компрометации Ключа / Закрытого ключа / Несанкционированного Доступа, с добавлением времени реагирования, определенного в соответствии с п.8.10 Соглашения. Сторона не несет ответственности за последствия исполнения документов в электронном виде, отправленных другой Стороной по Защищенному каналу связи с использованием скомпрометированного Ключа/Закрытого ключа или Несанкционированного Доступа, до получения уведомления о Компрометации Ключа / Закрытого ключа, Несанкционированном Доступе с добавлением времени реагирования на такое уведомление, определенного в соответствии с п. 8.10 Соглашения.
- 8.12. Стороны признают и гарантируют юридическую силу используемых во взаимоотношениях между Сторонами Официальных уведомлений, сформированных, отправленных, доставленных, учтенных и хранящихся в соответствии с порядком электронного документооборота, принятого в рамках Соглашения, равной юридической силе документов на

бумажном носителе, подписанных собственноручной подписью представителя соответствующей Стороны и заверенных ее печатью при соблюдении следующего:

8.12.1. Официальное уведомление сформировано, отправлено и получено с использованием ПАК.

8.12.2. Сторонами не было получено уведомлений о Компрометации Ключа/ Закрытого ключа / Несанкционированном Доступе.

9. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ, ВОЗНИКШИХ В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

9.1. В связи с осуществлением электронного документооборота возможно возникновение конфликтных ситуаций, в частности, в следующих случаях:

9.1.1. оспаривание факта формирования Официального уведомления;

9.1.2. заявление Стороны об искажении Официального уведомления;

9.1.3. оспаривание факта отправления и/или доставки Официального уведомления;

9.1.4. оспаривание времени отправления и/или доставки Официального уведомления;

9.1.5. иные случаи возникновения конфликтных ситуаций, связанных с функционированием ПАК Сторон.

9.2. Уведомление о конфликтной ситуации.

9.2.1. В случае возникновения конфликтной ситуации Сторона, считающая, что ее права были нарушены, должна не позднее чем в течение 3 (Трех) рабочих дней со дня, когда Стороне стало известно или должно было стать известно о нарушении ее права, направить уведомление о конфликтной ситуации другой Стороне.

9.2.2. Уведомление о предполагаемом наличии конфликтной ситуации должно содержать информацию о существовании конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации. Уведомление должно содержать реквизиты, позволяющие определить Официальное уведомление (не содержащие конфиденциальной информации), а также фамилию, имя, отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.

9.2.3. Стороны обмениваются заверенными выписками из Системных журналов, содержащих регистрацию событий, имеющих отношение к предмету спора в течение 3 (Трех) рабочих дней с момента получения Стороной уведомления о конфликтной ситуации. Если предполагаемая конфликтная ситуация связана с зачислением Перевода по номеру Карты национальной платежной системы, Стороны получают заверенные выписки из Системных журналов от ЗАО «ЗОЛОТАЯ КОРОНА».

9.3. Разрешение конфликтной ситуации в рабочем порядке.

9.3.1. Уведомление о предполагаемой конфликтной ситуации, которая связана с зачислением Перевода по номеру Карты национальной платежной системы, признается безосновательным, если выписка из Системного журнала содержит информацию, подтверждающую совершение оспариваемых действий.

В противном случае, Стороны с привлечением ЗАО «ЗОЛОТАЯ КОРОНА» осуществляют анализ конфликтной ситуации и готовят заключение с описанием причин ее возникновения и предлагаемых способов ее разрешения.

9.3.2. Уведомление о предполагаемой конфликтной ситуации, не указанное в подпункте 9.3.1 настоящего пункта Соглашения, признается безосновательным в случае, если выписки из Системных журналов содержат одинаковую информацию, подтверждающую совершение оспариваемых действий.

В противном случае, Сторона, в Системном журнале которой содержится информация, подтверждающая совершение оспариваемых действий, готовит заключение по конфликтной ситуации с описанием причин ее возникновения и предлагаемых способах

ее решения. Для подготовки заключения может быть привлечено лицо, уполномоченное Стороной обслуживать ПАК.

- 9.3.3. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от другой Стороны или ЗАО «ЗОЛОТАЯ КОРОНА». В случае если уведомитель не удовлетворен такой информацией, он направляет другой Стороне претензию в письменном виде.

10. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ (ФОРС-МАЖОР)

- 10.1. Сторона освобождается от ответственности за частичное или полное неисполнение обязательств по Соглашению, если это неисполнение явилось следствием обстоятельств непреодолимой силы (форс-мажор), возникших после заключения Соглашения, которые Сторона не могла ни предвидеть, ни предотвратить разумными мерами. В рамках Соглашения к обстоятельствам непреодолимой силы (форс-мажора) относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, военные действия, вступление в силу законодательных актов, правительственных постановлений и распоряжений государственных органов, прямо или косвенно запрещающих указанные в Соглашении виды деятельности.
- 10.2. Сторона, ссылающаяся на обстоятельства непреодолимой силы (форс-мажора), обязана предпринять все разумные усилия по минимизации ущерба и письменно предупредить другую Сторону любым доступным способом не позднее 3 (Трех) рабочих дней с даты наступления обстоятельств непреодолимой силы (форс-мажора). Если Сторона, ссылающаяся на обстоятельства непреодолимой силы (форс-мажора), по своей вине не уведомила другую Сторону в течение 3 (Трех) рабочих дней, то она не имеет права ссылаться на обстоятельства непреодолимой силы (форс-мажора).
- 10.3. Сторона, понесшая убытки в связи с наступлением обстоятельств непреодолимой силы, вправе потребовать от Стороны, ссылающейся на такие обстоятельства, документальное подтверждение о масштабах происшедших событий, а также об их влиянии на исполнение обязательств по Соглашению.

11. КОНФИДЕНЦИАЛЬНОСТЬ

- 11.1. Стороны принимают на себя обязательства не разглашать полученные в ходе исполнения Соглашения сведения, составляющие конфиденциальную информацию, в том числе коммерческую тайну, банковскую тайну каждой из Сторон, а также персональные данные субъектов Перевода, данные PAN Карт кроме случаев, предусмотренных законодательством Сторон и для целей исполнения Соглашения. Под сведениями, составляющими коммерческую тайну, в Соглашении понимается не являющаяся общедоступной информация об управлении, банковской, финансовой и иной деятельности каждой из Сторон, разглашение которой может привести к возникновению убытков и/или негативно повлиять на деловую репутацию любой из Сторон включая, но не ограничиваясь: информацию о технических и программных сведениях, полученных от Сторон (IP-адреса, Ключ, Закрытый ключ, Ключ ЭП, тип оборудования Cisco); любую информацию о проводимых операциях, Клиентах, объеме операций; коммерческие договоренности Сторон; сведения о методике и содержании информационного обмена между Сторонами.
- 11.2. Информация, указанная в пункте 11.1 Соглашения, может быть сообщена третьим лицам только при наличии письменного разрешения другой Стороны за исключением случаев, предусмотренных действующим законодательством Сторон.

12. ПОРУЧЕНИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТА

- 12.1. В целях исполнения Соглашения РНКО поручает БАНКУ обработку персональных данных Клиента. Перечень действий с персональными данными Клиента, которые будет осуществлять БАНК: запись, систематизация, накопление, хранение, извлечение, использование, передача

(предоставление, доступ), обезличивание, удаление, уничтожение персональных данных, как с использованием средств автоматизации, так и без использования таковых (неавтоматизированная обработка). При обработке персональных данных Клиента БАНК обязуется вести их обработку лишь в целях исполнения настоящего Соглашения и соблюдения законодательства страны инкорпорации БАНКА.

- 12.2. При обработке персональных данных Клиента БАНК обязан обеспечивать их безопасность и конфиденциальность, а также соблюдать принципы и правила обработки персональных данных, предусмотренных законодательством Российской Федерации и законодательством страны инкорпорации БАНКА.
- 12.3. При обработке персональных данных Клиента, БАНК обязан в соответствии с законодательством Российской Федерации и законодательством страны инкорпорации БАНКА принимать необходимые организационные и технические меры для защиты персональных данных Клиента, полученных в рамках исполнения Соглашения, от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, передачи, распространения, а также от иных неправомерных действий в отношении персональных данных Клиента, в том числе действий, не связанных с исполнением настоящего Соглашения и осуществлением Перевода.
- 12.4. Хранение персональных данных БАНКОМ осуществляется не дольше, чем этого требуют цели обработки персональных данных, определенные настоящим Соглашением. БАНК производит удаление и уничтожение персональных данных Клиента, не позднее тридцати дней с даты достижения БАНКОМ целей обработки персональных данных, определенных настоящим Соглашением

13. ПОРЯДОК РАСТОРЖЕНИЯ И ИЗМЕНЕНИЯ СОГЛАШЕНИЯ

- 13.1. Соглашение становится обязательным для исполнения Сторонами с даты, указанной РНКО в письме БАНКУ о принятии Заявки БАНКА к исполнению. Соглашение может быть расторгнуто:
 - 13.1.1. по инициативе БАНКА путем направления письменного уведомления РНКО за 30 (Тридцать) календарных дней до предполагаемой даты прекращения действия Соглашения, по истечении указанного срока Соглашение прекращается и считается расторгнутым;
 - 13.1.2. по инициативе РНКО путем направления письменного уведомления БАНКУ не менее чем за 30 (Тридцать) календарных дней до предполагаемой даты прекращения действия Соглашения, по истечении указанного срока Соглашение прекращается и считается расторгнутым.
- 13.2. РНКО в одностороннем порядке вправе вносить изменения в Соглашение, путем заблаговременного размещения изменений в сети Интернет на сайте www.rnko.ru до даты вступления новой редакции Соглашения в силу.
- 13.3. В течение срока действия Соглашения любая Сторона вправе немедленно расторгнуть Соглашение, посредством направления письменного уведомления другой Стороне в случае внесения изменений в законодательство любой из Сторон либо в случае внесения изменений в Соглашение, в результате которых становится невозможным для любой из Сторон оказывать услуги по денежным переводам в соответствии с порядком и процедурой, изложенными в Соглашении, при условии, что Стороны не достигли соглашения об изменении правил оказания услуг по денежным переводам таким образом, чтобы их оказание осуществлялось в соответствии с такими изменениями законодательства.
- 13.4. В случае наступления любого из следующих событий Соглашение прекращается автоматически с даты получения Стороной информации о наступлении указанных событий в отношении другой Стороны:
 - 13.4.1. Отзыв у одной из Сторон необходимых разрешений (лицензии) либо приостановления

их действия;

- 13.4.2. Сторона стала неплатежеспособной, объявляет о своей ликвидации, в отношении нее инициирована процедура несостоятельности (банкротства);
 - 13.4.3. БАНКОМ закрыт Счет БАНКА, при этом Сторонами не согласован порядок осуществления Перевода и расчетов.
- 13.5. РНКО в одностороннем внесудебном порядке вправе отказаться от исполнения Соглашения с БАНКОМ, в случае нарушения БАНКОМ условий Соглашения. Соглашение расторгается путем направления БАНКУ письменного уведомления об отказе от исполнения Соглашения без соблюдения сроков, предусмотренных п.13.1.2 Соглашения.

14. ПОРЯДОК РАССМОТРЕНИЯ ПРЕТЕНЗИЙ И СПОРОВ

- 14.1. В случае возникновения споров между Сторонами по условиям Соглашения или в связи с ним, Сторона, считающая что ее права нарушены, обязуется направить другой Стороне претензию в письменном виде. Срок рассмотрения претензии – 10 (Десять) рабочих дней.
- 14.2. В случае если споры между Сторонами не будут урегулированы в претензионном порядке, спор должен быть передан в Арбитражный суд Новосибирской области. Арбитражное разбирательство ведется на русском языке. При разрешении спора применяется законодательство Российской Федерации.
- 14.3. Соглашение заключено и подлежит толкованию в соответствии с законодательством Российской Федерации.