Утвержден
Приказом Генерального директора
АО «ДК РЕГИОН»
№ ДК-05 от 27.01.2020

Регламент
Электронного документооборота
Системы «Личный кабинет клиента»
АО «ДК РЕГИОН»
(новая редакция)

Москва
2020

Термины и определения

Сертификат ключа проверки электронной подписи (Сертификат) – электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки электронной подписи (Квалифицированный сертификат) – электронный документ или документ на бумажном носителе, выданный Аккредитованным удостоверяющим центром либо доверенным лицом Аккредитованного удостоверяющего центра, подтверждающий принадлежность ключа проверки электронной подписи владельцу квалифицированного сертификата ключа проверки электронной подписи и соответствующий требованиям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», и иным принимаемым в соответствии с ним нормативными правовыми актами.

Владелец сертификата ключа проверки электронной подписи - Участник, в лице своего Уполномоченного Представителя, которому в установленном порядке, Удостоверяющим центром (Аккредитованным удостоверяющим центром), выдан сертификат ключа проверки электронной подписи (квалифицированный сертификат ключа проверки электронной подписи).

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Время «Т» – момент проверки наличия совокупности правовых условий, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной.

Организатор ЭДО – АО «ДК РЕГИОН».

Подлинность электронной подписи в электронном документе – положительный результат проверки средством электронной подписи с использованием сертификата ключа проверки подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе.

Список отозванных сертификатов – электронный документ, подписанный электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей проверки подписей, которые на момент времени формирования списка отозванных сертификатов были отозваны или действие которых было приостановлено. Момент времени формирования списка отозванных сертификатов определяется по значению поля ThisUpdate списка отозванных сертификатов.

Аккредитованный удостоверяющий центр (Аккредитованный УЦ) – юридическое лицо или индивидуальный предприниматель, которые являются аккредитованными Министерством связи и массовых коммуникаций Российской Федерации удостоверяющими центрами, осуществляющими функции по созданию и выдаче Сертификатов ключей проверки электронной подписи, а также иные функции, предусмотренные Регламентом УЦ и Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». Перечень удостоверяющих центров приведен в Приложении №6 к настоящему Регламенту.

Удостоверяющий центр (УЦ) - Удостоверяющий центр «e-Notary» (Удостоверяющий центр, УЦ) – ЗАО «Сигнал-КОМ».

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра (Аккредитованного удостоверяющего центра) и наделенное

Удостоверяющим центром полномочиями по заверению от лица Удостоверяющего центра сертификатов ключей проверки подписей и списков отозванных сертификатов.

Регламент удостоверяющего центра – документ, разработанный и утвержденный УЦ (Аккредитованным УЦ), обязательный для исполнения любым лицом, вступающим во взаимоотношения с УЦ по выполнению последним функций, удостоверяющего центра, предусмотренных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». Регламент УЦ размещается на сайте УЦ (Аккредитованного УЦ) в сети интернет.

Средство криптографической защиты информации (СКЗИ) - шифровальное (криптографическое) средство, используемое для реализации следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи и имеющее подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»

Уполномоченный представитель – сотрудник Участника, которому Участником доверено подписание электронной подписью этого Участника электронных документов, формирование электронных сообщений, их прием, передача, учет и хранение, если владельцем сертификата ключа проверки подписи является этот Участник.

Участники – Участниками электронного документооборота являются юридические лица: Акционерное общество «Депозитарная компания РЕГИОН» (АО «ДК РЕГИОН») и его клиенты (Клиенты), присоединившиеся к настоящему регламенту и осуществляющие обмен информацией в электронной форме с использованием ЭП.

Формат электронного документа – структура содержательной части электронного сообщения, на основе которого сформирован электронный документ.

Электронный документ (ЭД) – информация, представленная в электронно-цифровой форме (файл данных в терминах операционной системы), представляющая собой совокупность структурированных данных, имеющих смысл для Участников и позволяющая обеспечить ее обработку программным и аппаратным обеспечением ЭДО.

Электронный журнал – взаимосвязанный набор электронных записей, отражающих последовательность действий с ЭД в Системе по приему, обработке и отправке ЭД, в том числе содержащий дату, время и содержание операций, производимых в системе.

Система «Личный кабинет клиента» (ЛКК) – корпоративная информационная система АО «ДК РЕГИОН», предназначенная для удаленного взаимодействия с клиентом, обеспечивающая подготовку, защиту, прием, передачу и обработку электронных документов с использованием сети «Интернет», доступная по адресу: https://lk.region-dk.ru.

Шаблон – электронный документ, который сочетает в себе совокупность установленных АО «ДК РЕГИОН» требований к Форме документа и Формату файла. В отношении файлов, обмен которыми Стороны будут осуществлять в Формате *.xml понятие Шаблон включает в себя XML–схему, предоставляемую Компанией Клиенту.

Специализированный депозитарий/ Специализированный регистратор/Депозитарий - Акционерное общество «Депозитарная компания РЕГИОН», Адрес в пределах места нахождения: 119021, г. Москва, бульвар Зубовский, д. 11А, этаж 7, помещение I, комната 1, ИНН 7708213619, КПП 997950001, имеющее лицензию № 22-000-0-00088 от «13» мая 2009 года, выданную ФСФР России, на осуществление деятельности специализированного депозитария инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, а также лицензию профессионального участника рынка ценных бумаг на осуществление депозитарной деятельности № 045-09028-000100 от «04» апреля 2006 года, выданную ФСФР России.

1. Общие положения

1.1. Настоящий Регламент электронного документооборота (далее – «Регламент») определяет порядок и условия применения электронной подписи, электронного документооборота в **ЛКК** с другими Участниками.
1.2. Настоящий Регламент регулирует отношения между Участниками в области электронного документооборота, использования электронных подписей при совершении юридически значимых действий.
1.3. Субъектами Регламента являются Участники и Уполномоченные представители, а также Удостоверяющие центры и Уполномоченные лица.
1.4. Настоящий Регламент публикуется на сайте АО «ДК РЕГИОН» http://region-dk.ru.
1.5. Правовое регулирование отношений в области использования ЭДО осуществляется в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи», другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, а также настоящим Регламентом и заключенными между Участниками соглашениями.
1.6. Настоящий Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.
1.7. Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления в АО «ДК РЕГИОН» Заявления о присоединении к Регламенту по форме Приложения №1 настоящего Регламента.
1.8. Факт присоединения к Регламенту является полным принятием условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации Заявления о присоединении.
1.9. Внесение изменений и/или дополнений в Регламент производится АО «ДК РЕГИОН» в одностороннем порядке. Внесение изменений и/или дополнений в Регламент осуществляется в форме новой редакции. Изменения и дополнения, вносимые в Регламент, вступают в силу и становятся обязательными для всех участников в дату, определенную при их утверждении.
1.10. Уведомление остальных Участников о внесении изменений и/или дополнений в Регламент осуществляется путем публикации сообщения на сайте АО «ДК РЕГИОН» не позднее 1 (Одного) рабочего дня до даты их вступления в силу.

2. Удостоверяющий центр и сертификаты ключей

2.1. Удостоверяющим центром, обладающим необходимым комплексом программно-технических средств, обеспечивающее изготовление и обслуживание неквалифицированных Сертификатов ключей проверки электронной подписи Уполномоченных представителей Участников является Удостоверяющий центр «e-Notary» (Удостоверяющий центр, УЦ) – ЗАО «Сигнал-КОМ».
2.2. Участники настоящего Регламента обязаны знакомиться с содержанием и изменениями Регламента удостоверяющего центра, выдавшего сертификат ключа проверки электронной подписи самостоятельно. Участники самостоятельно несут ответственность за нарушение указанного Регламента удостоверяющего центра.
2.3. При организации и функционировании ЭДО принимаются и признаются Сертификаты ключей проверки подписей, изданные Удостоверяющим центром, в составе и формате, определяемом Удостоверяющим центром. А также Квалифицированные сертификаты ключа проверки электронной подписи выданные Аккредитованным удостоверяющим центром, в составе и формате, определяемом Аккредитованным Удостоверяющим центром.
2.4. Сертификат признается изданным Удостоверяющим центром, если подтверждена подлинность электронной подписи этого сертификата, сделанной Уполномоченным лицом Удостоверяющего центра.
2.5. Квалифицированный сертификат признается изданным Аккредитованным удостоверяющим центром, если подтверждена подлинность электронной подписи этого

сертификата, сделанной Уполномоченным лицом Аккредитованного удостоверяющего центра.

2.6. Идентификационные данные, занесенные в поле «Субъект» (Subject Name) Сертификата или Квалифицированного сертификата, однозначно идентифицируют Владельца сертификата ключа проверки подписи и соответствуют идентификационным данным Владельца сертификата ключа проверки подписи.

2.7. Для определения статуса Сертификата (Квалифицированного сертификата), получения актуального списка отозванных сертификатов, актуальных сертификатов уполномоченных лиц УЦ участниками ЭДО используется сертифицированное ФСБ России СКЗИ.

2.8. Порядок регистрации Уполномоченных представителей Участников, изготовления сертификатов, замены ключей, отзыва сертификатов устанавливается в соответствующих документах УЦ (Аккредитованного УЦ), являющихся обязательными для Участников. АО «ДК РЕГИОН» не несет ответственности за нарушение документов УЦ, которые являются обязательными для всех участников.

2.9. Для изготовления сертификата ключа неквалифицированной электронной подписи Участникам (Клиентам) необходимо предоставить Организатору ЛКК документы, перечень которых предусмотрен в Приложении №1 и заявление на изготовление данного сертификата, которое передается в удостоверяющий центр ЗАО «Сигнал-КОМ» через ООО «ЦИТ «РЕГИОН». Форма заявления является Приложением №3 к настоящему Регламенту.

2.10. Для отзыва сертификата ключа неквалифицированной электронной подписи Участникам (Клиентам) необходимо предоставить Организатору ЛКК заявление по Форме приведенной в Приложении №7 к настоящему Регламенту.

3. Документы, подписываемые ЭП

3.1. Перечень электронных документов, подписание которых электронной подписью предполагается в рамках настоящего Регламента, приведены в Приложении №1 к Правилам ведения реестра владельцев инвестиционных паев специализированного депозитария АО «ДК РЕГИОН», в Приложениях № 1 и №2 к Регламенту специализированного депозитария ипотечного покрытия АО «ДК РЕГИОН», в Приложении к «Регламенту специализированного депозитария Акционерного общества «Депозитарная компания «РЕГИОН» и Регламенте депозитарного обслуживания.

3.2. Шаблоны могут визуально отличаться от форм, указанных в соответствующих Регламентах при сохранении всех необходимых для такого документа реквизитов.

4. Порядок формирования и проверки электронной подписи , условия равнозначности электронной подписи собственноручной

4.1. Все документы в Системе «Личный кабинет клиента» подписываются электронными подписями Уполномоченных представителей

4.2. При подписании электронных документов Участники используют квалифицированную и неквалифицированную усиленную электронную подпись с поддержкой штампов времени.

4.3. Неквалифицированной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

4.4. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным им Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».

4.5. Для формирования и проверки электронной подписи в ЛКК используется сертифицированное ФСБ России СКЗИ.
4.6. Формирование электронной подписи электронного документа может быть осуществлено только уполномоченным представителем Участника - владельцем сертификата ключа проверки подписи, ключ электронной подписи которого действует на момент формирования электронной подписи электронного документа.
4.7. Ключ электронной подписи действует на определенный момент времени (действующий ключ), если:
- наступил момент времени начала действия ключа;
- срок действия ключа не истек;
- сертификат ключа проверки подписи, соответствующий данному ключу действует на данный момент времени.
4.8. Сертификат ключа проверки подписи действует (действующий сертификат) на определенный период времени, характеризующийся:
- наступлением момента времени начала его действия;
- не истекшим сроком его действия;
- тем, что он не аннулирован (отозван) и действие его не приостановлено;
- подтверждением подлинности (корректности) электронной подписи Уполномоченного лица удостоверяющего центра в данном сертификате.
4.9. Сертификат ключа проверки электронной подписи считается аннулированным (отозванным) с момента публикации УЦ списка отозванных сертификатов, в котором содержится серийный номер данного сертификата.
4.10. Размещенные в ЛКК электронные документы, подписанные корректной ЭП, имеют равную юридическую силу с документами на бумажном носителе, подписанными Участниками и скрепленными оттисками печатей.
4.11. Электронная подпись считается корректной, если получен положительный результат проверки подписи.
4.12. Результат проверки ЭП считается положительным, если:
- подтверждена Подлинность электронной подписи документа
- ключ электронной подписи действителен на момент подписи
4.13. Момент времени подписи определяется из штампа времени электронной подписи

5. Права и Обязанности Участников электронного взаимодействия

5.1. АО «ДК РЕГИОН» имеет право:
5.1.1. В любое время проводить профилактические и иные работы в ЛКК, прекращая доступ Клиентов к данной системе с предварительным уведомление Клиента путем размещения информации на сайте по адресу: https://lk.region-dk.ru
5.1.2. В любое время изменять сервисы ЛКК, программное обеспечение, дизайн, содержание, как с уведомлением Клиента, так и без такового.
5.1.3. Отказать в приеме ЭД, если есть основания считать, что такие документы отправлены от имени Клиента другим лицом, в том числе злоумышленником.
5.1.4. В случае возникновения обоснованных сомнений в подлинности ЭД, являющегося основанием для проведения операции, запросить любым доступным для него способом подтверждение Клиента о факте направления Клиентом ЭД.
5.1.5. Отказать в проведении операции, носящей сомнительный характер, в случае отсутствия подтверждения Клиентом факта направления ЭД.

5.2. АО «ДК РЕГИОН» обязуется:
5.2.1. Консультировать Клиента по вопросам функционирования ЛКК, приема-передачи ЭД, информации и технологий их обработки в рамках технической поддержки приема/передачи ЭД посредством ЛКК.
5.2.2. Осуществлять прием ЭД Клиента согласно условиям организации и проведения электронного документооборота, установленного настоящим Регламентом.
5.2.3. В случае получения некорректных ЭД – документов, оформленных с нарушением требований Регламента СД, Правил ведения реестра владельцев инвестиционных паев, Регламента депозитария, переданных Клиентом посредством ЛКК в срок не позднее 1

(одного) рабочего дня с даты получения соответствующего ЭД информировать Клиента о невозможности исполнения таких ЭД.

5.2.4. Вести и хранить архив ЭД, принятых от Клиента с использованием ЛКК не менее 5 (пяти) лет с даты прекращения отношений с Клиентом.

5.2.5. Вести электронный журнал, обеспечивать его целостность, а также защиту информации, содержащейся в Электронном журнале, и хранить его не менее 5 (пяти) лет после прекращения настоящего Регламента.

5.2.6. Прекращать доступ Клиента к ЛКК на основании его письменного заявления, поданного в АО «ДК РЕГИОН».

5.2.7. Принимать меры по защите и обеспечению целостности информации, находящейся в Электронном журнале.

5.2.8. Совершать операции в порядке и сроки, предусмотренные действующим законодательством Российской Федерации, нормативными правовыми актами Банка России, Правилами ведения реестра владельцев инвестиционных паев, Регламентом специализированного депозитария и Регламентом депозитария.

5.3. Клиент имеет право:

5.3.1. Получать консультации по вопросам функционирования ЛКК, приема-передачи ЭД, информации и технологий их обработки в рамках технической поддержки приема/передачи ЭД посредством ЛКК.

5.3.2. Осуществлять передачу ЭД согласно порядку организации и проведения электронного документооборота, установленного настоящим Регламентом.

5.3.3. Требовать предоставление информации о причинах неисполнения ЭД.

5.3.4. Получать необходимые подтверждения выполненных операций, в случаях и форме, установленных законодательством РФ.

5.4. Клиент обязан:

5.4.1. Эксплуатировать средства электронной подписи в соответствии с правилами их использования.

5.4.2. Обеспечивать конфиденциальность ключей электронных подписей.

5.4.3. Не допускать несанкционированного использования электронных подписей.

5.4.4. Уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

5.4.5. Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

5.4.6. Использовать те средства ЭП, которых имеют сертификат ФСБ России.

5.4.7. Не размещать в ЛКК недостоверную и/или заведомо ложную информацию.

5.4.8. Соблюдать условия организации и проведения электронного документооборота, установленные настоящим Регламентом.

5.4.9. Не разглашать третьим лицам, за исключением случаев, предусмотренных законодательством конкретные способы защиты информации, реализованные в ЛКК.

5.4.10. Выполнять требования к программно-техническим средствам.

5.4.11. Ознакомиться с уведомлением о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц, являющимся Приложением №8 к настоящему Регламенту.

5.5. Участники совместно обязуются:

5.5.1. Не предпринимать действий, способных нанести ущерб другой Стороне вследствие использования ЛКК.

5.5.2. Незамедлительно уведомить другую Сторону в случае обнаружения возможных угроз безопасности обмена ЭД посредством ЛКК, для принятия мер по защите.

5.5.3. Незамедлительно информировать друг друга обо всех случаях возникновения технических неисправностей, препятствующих обмену ЭД через ЛКК.

6. Порядок обмена электронными документами

6.1. Участник-отправитель подготавливает электронные документы для отправки Участнику-получателю с использованием средств личного кабинета.
6.2. Подготовленные электронные документы Участник-отправитель регистрирует средствами собственной системы регистрации в соответствии с правилами регистрации входящей и исходящей корреспонденции.
6.3. Зарегистрированные электронные документы Участник-отправитель подписывает с использованием ключа электронной подписи, реализованных в применяемом средстве электронной подписи.
6.4. АО «ДК РЕГИОН» принимает электронные документы в электронной форме при условии соответствия этих документов требованиям законодательства РФ, Договора, форматам, установленным ЛКК, а также наличия корректной ЭП.
6.5. Документы, оформленные ненадлежащим образом, для которых в ЛКК установлен формат и перечень реквизитов к заполнению, направленные в свободном формате, ЛКК не принимаются.
6.6. Поступившие в ЛКК ЭД Клиента принимаются в сроки, установленные законодательством РФ и соответствующим договором (Регламентом) при условии, что проверка на подлинность ЭП дала положительный результат, документ оформлен правильно, не противоречит действующему законодательству Российской Федерации и нормативным актам Банка России.
6.7. Документы свободного формата, направляемые посредством ЛКК и исполненные в виде файлов, содержащих сканированные копии, принимаются при наличии качественного изображения, позволяющего идентифицировать информацию и сведения, необходимые для реализации АО «ДК РЕГИОН» своих прав и обязанностей, а также при наличии на данных документах подписей и печатей (при необходимости).
6.8. Одной ЭП могут быть подписаны несколько связанных между собой Электронных документов (пакет Электронных документов). При подписании ЭП пакета Электронных документов, каждый из Электронных документов, входящих в этот пакет, считается подписанным ЭП, которой подписан пакет Электронных документов.
6.9. Клиент уведомляется о приеме к исполнению / отказе в приеме к исполнению Распоряжения в форме ЭД путем изменения статуса ЭД в ЛКК с указанием:
- в случае принятия к исполнению – информации, позволяющей Клиенту идентифицировать Распоряжение, и даты приема его к исполнению;
- в случае отказа в приеме к исполнению - информации, позволяющей Клиенту идентифицировать Распоряжение, даты отказа, а также причины.

6.10. Обязанность по уведомлению о приеме к исполнению / отказе в приеме к исполнению Распоряжения Клиента считается исполненной, а соответствующее уведомление считается полученным Клиентом, при размещении в ЛКК соответствующей информации.
6.11. Датой получения Клиентом от АО «ДК РЕГИОН» документов и информации, сформированных в электронном виде с помощью ЛКК, является дата размещения АО «ДК РЕГИОН» документов и информации в ЛКК.
6.12. Датой представления Клиентом в АО «ДК РЕГИОН» документов и информации, сформированных в электронном виде с помощью ЛКК, является дата их получения: дата размещения Клиентом подписанных ЭП Электронных документов в ЛКК в соответствии с настоящим Регламентом.
6.13. Ни один из Участников, ни какие-либо третьи лица не имеют возможность вносить изменения в ЭД, хранящийся в ЛКК.

7. Учет и хранение электронных документов

7.1. Ответственным за учет и хранение электронных документов является Уполномоченный представитель Организатора ЭДО.
7.2. Все документы, переданные с использованием ЛКК, а также соответствующие им по времени использования все сертификаты ключей проверки ЭП должны храниться в течение сроков, предусмотренных действующими нормативными правовыми актами Российской Федерации для хранения соответствующих документов. При этом должны обеспечиваться:

- доступ к электронным документам, информации о датах и времени их получения (отправки), адресатах, а также возможность поиска документов по их реквизитам;
- резервное копирование электронных документов осуществляется уполномоченными представителями Участников по необходимости по мере поступления документов в соответствии с внутренним регламентом Участника;
- архивное хранение электронных документов, их реквизитов, включая информацию о датах и времени получения (отправки) и адресатах осуществляется уполномоченными представителями Участников с использованием компонентов ЭДО;
- возможность восстановления электронных документов реализуется штатными средствами почтовых клиентов, используемых Участниками. Хранение электронного документа осуществляется только в виде записи информации, составляющей электронный документ, на машинном носителе.

7.3. Электронные документы должны храниться в архивах электронных документов обеих сторон в том же формате, в котором они были отправлены или получены.

7.4. Каждая из сторон самостоятельно обеспечивает защиту собственных архивов электронных документов от несанкционированного доступа, изменения, уничтожения.

7.5. Участники обязаны по требованию Банка России и в соответствии с указанным требованием представить:

- документ в электронной форме и (или) его копию на бумажном носителе, заверенную в установленном порядке;
- информацию о датах и времени получения (отправки), адресатах электронных Документов.

8. Разрешение споров

8.1. Все споры, разногласия, требования, возникающие из настоящего Регламента или касающиеся его нарушения, прекращения недействительности подлежат путем переговоров.

8.2. В случае невозможности разрешения разногласий путем переговоров, споры разрешаются в Арбитражном суде г. Москвы в порядке, установленном действующим законодательством РФ, с обязательным соблюдением досудебного претензионного порядка.

8.3. Претензия оформляется в письменном виде и направляется заказным письмом с уведомлением, с приложением копий документов подтверждающих обоснование заявленной претензии.

8.4. Срок ответа на претензию устанавливается в 15 (пятнадцать) дней с момента ее получения.

9. Обстоятельства непреодолимой силы (Форс-мажор)

9.1. Участники не несут ответственности в случае невыполнения, несвоевременного или ненадлежащего выполнения ими какого-либо из обязательств настоящего Регламента, если это обусловлено исключительно наступлением и/или действием обстоятельств непреодолимой силы (форс-мажор).

9.2. Затронутый форс-мажорными обстоятельствами Участник без промедления информирует другого Участника об этих обстоятельствах и об их возможных последствиях и принимает все возможные меры с целью максимально ограничить отрицательные последствия, вызванные указанными обстоятельствами.

9.3. Участник, затронутый форс-мажорными обстоятельствами, обязан без промедления известить другого Участника о прекращении действия этих обстоятельств.

9.4. К обстоятельствам непреодолимой силы относятся: военные действия, стихийные бедствия, пожары, забастовки, массовые беспорядки, изменения гражданского или налогового законодательства, изменение или введение новых нормативных актов, существенно ухудшающих условия выполнения настоящего Регламента или делающих невозможным выполнение настоящего Регламента полностью или частично.

10. Ответственность сторон за несоблюдение настоящего Регламента

10.1. За несоблюдение настоящего Регламента Участники несут имущественную ответственность в соответствии с действующим законодательством Российской Федерации.

10.2. Участник освобождается от ответственности за убытки, причиненные другому Участнику в случае, если представленные электронные документы, передаваемые другим Участником, не приняты к исполнению Участником, получившим документ, по причине невыполнения условий настоящего Регламента.

10.3. Участники не несут ответственности за любые убытки других Участников, не связанные с нарушением сторонами своих обязательств по настоящему Регламенту.

11. Заключительные положения

11.1. Все изменения, дополнения и приложения к настоящему Регламенту, оформленные надлежащим образом, являются его неотъемлемой частью.

11.2. Участники не вправе передавать права и обязанности, связанные с исполнением настоящего Регламента, третьим лицам.

11.3. Во всем остальном, что не предусмотрено настоящим Регламентом, Участники руководствуются действующим законодательством РФ.

Приложение №1
К Регламенту электронного документооборота
Системы «Личный кабинет клиента»

Список документов, предоставляемых Участником ЛКК.

Для российских юридических лиц:

- Устав Участника ЛКК со всеми изменениями (нотариально заверенная копия);
- Выписка из ЕГРЮЛ в отношении Участника ЛКК давностью выдачи не более 1 месяца до даты представления документов (нотариальная копия или оригинал);
- Решение (протокол) об избрании единоличного исполнительного органа/коллегиального исполнительного органа Участника ЛКК (нотариально заверенная копия);
- Приказ о назначении на должность единоличного исполнительного органа Участника ЛКК (копия, заверенная Участником ЛКК);
- Приказ о назначении на должность главного бухгалтера Участника ЛКК (копия, заверенная Участником ЛКК);
- Банковская карточка Участника ЛКК (нотариально заверенная копия);
- Документ, удостоверяющий личность будущего Владельца сертификата ключа подписи (нотариальная копия или копия, заверенная Организатором ЛКК при предъявлении оригинала указанного документа);
- Подписанное заявление о присоединении по форме Приложения №2 к Правилам
- Подписанное заявление на изготовление Сертификата ключа подписи с печатью Участника ЛКК Приложения №3 к Правилам;
- Подписанное согласие на обработку персональных данных будущего Владельца сертификата ключа подписи по форме Приложения №4 к Правилам;
- Анкета участника ЛКК Приложения №5 к Правилам
- Доверенность на предоставление заявления на изготовление Сертификата открытого ключа подписи на имя Уполномоченных представителей Участника ЛКК в случае, если заявление предоставляется лицом, не имеющим права действовать от имени Участника ЛКК без доверенности (оригинал).

Для иностранных юридических лиц:

- Учредительные документы, являющиеся таковыми для юридического лица в соответствии с законодательством страны его регистрации, со всеми зарегистрированными изменениями и дополнениями к ним (нотариально заверенные копии документов, надлежащим образом апостилированных и переведенных на русский язык);
- Документ(ы), подтверждающий(е) в соответствии с законодательством страны регистрации юридического лица государственную регистрацию юридического лица с указанием в нём (в них) государственного регистрационного номера, места государственной регистрации и адреса местонахождения юридического лица (сертификаты, свидетельства, выписки и т.п.) (нотариально заверенные копии документов, надлежащим образом апостилированных и переведенных на русский язык);
- Для юридических лиц, осуществляющих деятельность в РФ через постоянное представительство (филиал, другое обособленное подразделение), и/или имеющих на территории РФ недвижимое имущество / транспортные средства - Свидетельство о постановке на учет в налоговом органе РФ (нотариально заверенные копии документов);
- Для юридических лиц, подлежащих учету в налоговом органе по месту постановки на учет банка (по месту нахождения филиала), в котором им открыт счет - Свидетельство об учете в налоговом органе (нотариально заверенные копии документов);
- Документ, удостоверяющий личность будущего Владельца сертификата ключа подписи (нотариальная копия или копия, заверенная Организатором ЛКК при предъявлении оригинала указанного документа);
- Подписанное заявление о присоединении по форме Приложения №2 к Правилам
- Подписанное заявление на изготовление Сертификата ключа подписи с печатью Участника ЛКК Приложения №3 к Правилам;
- Подписанное согласие на обработку персональных данных будущего Владельца сертификата ключа подписи по форме Приложения №4 к Правилам;
- Анкета участника ЛКК Приложения №5 к Правилам

- Доверенность на предоставление заявления на изготовление Сертификата открытого ключа подписи на имя Уполномоченных представителей Участника ЛКК в случае, если заявление предоставляется лицом, не имеющим права действовать от имени Участника ЛКК без доверенности (оригинал или нотариально заверенная копия, надлежащим образом апостилированные и переведенные на русский язык).

Для индивидуальных предпринимателей:

- Документ, удостоверяющий личность (нотариальная копия или копия, заверенная Организатором ЛКК при предъявлении оригинала указанного документа);
- Свидетельство о внесении записи в Единый государственный реестр индивидуальных предпринимателей (нотариальная копия);
- Документ, подтверждающий постановку индивидуального предпринимателя на налоговый учет (нотариальная копия);
- Для иностранных физических лиц и лиц без гражданства дополнительно предоставляются документы, указанные в разделе «Для физических лиц – иностранных граждан или лиц без гражданства»;
- Подписанное заявление о присоединении по форме Приложения №2 к Правилам
- Подписанное заявление на изготовление Сертификата ключа подписи с печатью Участника ЛКК Приложения №3 к Правилам;
- Подписанное согласие на обработку персональных данных будущего Владельца сертификата ключа подписи по форме Приложения №4 к Правилам;
- Анкета участника ЛКК Приложения №5 к Правилам
- Нотариальная доверенность на предоставление заявления на изготовление Сертификата открытого ключа подписи на имя Участника ЛКК в случае, если заявление предоставляется уполномоченным представителем (оригинал или нотариально заверенная копия).

Для физических лиц – граждан Российской Федерации:

- Документ, удостоверяющий личность (нотариальная копия или копия, заверенная Организатором ЛКК при предъявлении оригинала указанного документа);
- Свидетельство о постановке на учет в налоговом органе (нотариальная копия либо копия, заверенная Организатором ЛКК при предъявлении оригинала указанного документа);
- Подписанное заявление о присоединении по форме Приложения №2 к Правилам
- Подписанное заявление на изготовление Сертификата ключа подписи с печатью Участника ЛКК Приложения №3 к Правилам;
- Подписанное согласие на обработку персональных данных будущего Владельца сертификата ключа подписи по форме Приложения №4 к Правилам;
- Анкета участника ЛКК Приложения №5 к Правилам
- Нотариальная доверенность предоставление заявления на изготовление Сертификата открытого ключа подписи на имя Участника ЛКК в случае, если заявление предоставляется уполномоченным представителем (оригинал или нотариально заверенная копия).

Для физических лиц – иностранных граждан или лиц без гражданства:

- Общегражданский паспорт или иной документ, установленный законодательством РФ или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина или лица без гражданства (нотариальная копия или копия, заверенная Организатором ЛКК при предъявлении оригинала указанного документа);
- Миграционная карта (если в соответствии с действующим законодательством она должна была быть оформлена при пересечении данным иностранным гражданином или лицом без гражданства границы РФ) (нотариальная копия или копия, заверенная Организатором ЛКК при предъявлении оригинала указанного документа);
- Документ, подтверждающий право иностранного гражданина или лица без гражданства на пребывание (проживание) в Российской Федерации (нотариальная копия или копия, заверенная Организатором ЛКК при предъявлении оригинала указанного документа);

- Подписанное заявление о присоединении по форме Приложения №2 к Правилам
- Подписанное заявление на изготовление Сертификата ключа подписи с печатью Участника ЛКК Приложения №3 к Правилам;
- Подписанное согласие на обработку персональных данных будущего Владельца сертификата ключа подписи по форме Приложения №4 к Правилам;
- Анкета участника ЛКК Приложения №5 к Правилам
- Нотариальная доверенность на предоставление заявления на изготовление Сертификата открытого ключа подписи на имя Участника ЛКК в случае, если заявление предоставляется уполномоченным представителем (оригинал или нотариально заверенная копия).

Приложение № 2
К Регламенту электронного документооборота
Системы «Личный кабинет клиента»

Заявление о присоединении

Сведения о заявителе – Участнике ЭДО			
Полное наименование			
ОГРН			
ИНН		КПП	
Место нахождения			
Почтовый адрес			

Настоящим заявитель полностью и безусловно присоединяется согласно ст. 428 ГК РФ к Регламенту электронного документооборота Системы «Личный кабинет клиента» АО «ДК РЕГИОН» (далее – Регламент), а также всем приложениям к ним, заключая тем самым договор на использование системы «Личный кабинет клиента» электронного документооборота АО «ДК РЕГИОН». Заявитель подтверждает, что полностью прочитал, ознакомлен и согласен с содержанием и условиями Регламента и приложениями к ним, обязуется полностью, своевременно и в полном объеме выполнять принятые на себя обязательства и соблюдать положения Регламента. Заявитель заявляет, что намерен осуществлять обмен электронными документами в системе «Личный кабинет клиента», порядок которого устанавливает Организатор ЭДО.
После подачи настоящего заявления заявитель не может ссылаться на то, что он не ознакомился с вышеуказанными документами (полностью или частично) либо не признает их обязательность при осуществлении электронного документооборота.

Контактная информация			
Контактный телефон			
Адрес электронной почты (e-mail)			
Должность руководителя		ФИО Руководителя	
Дата заявления		Подпись уполномоченного лица заявителя	

М.П.

Приложение №3
к Регламенту электронного документооборота
Системы «Личный кабинет клиента»

(Форма заявления на изготовление сертификата ключа подписи Пользователя для юридических лиц)

Заявление
на изготовление сертификата ключа подписи Пользователя

_____
Полное наименование юридического лица, включая организационно-правовую форму

в лице _____
должность руководителя юридического лица или уполномоченного сотрудника

_____
фамилия, имя, отчество

действующего на основании _____,
основание полномочий

просит изготовить сертификат ключа подписи своего уполномоченного представителя в соответствии со следующими идентификационными данными:

Страна (RU для России)	RU
Область/Район	
Город/Село	
Организация (краткое или полное наименование по уставу)	
Подразделение	
Должность	
Фамилия, имя, отчество	
Адрес электронной почты	

Владелец сертификата ключа подписи _____ _____
подпись Ф.И.О.

паспорт серии № выдан « » 20 года

_____

наименование органа, выдавшего документ

_____ _____ _____
Руководитель (должность) подпись Ф.И.О.

« » 20 года

М.П.

Форма заявления на изготовление сертификата ключа подписи Пользователя
для индивидуальных предпринимателей и физических лиц

Заявление
на изготовление сертификата ключа подписи Пользователя

Я, _____
фамилия, имя, отчество

паспорт серии _____ № _____ выдан «____» _____ года

_____
наименование органа, выдавшего документ

прошу изготовить сертификат ключа подписи в соответствии со следующими данными:

Страна (RU для России)	RU
Область/Район	
Город/Село	
Должность (если имеется)	
Фамилия, имя, отчество	
Адрес электронной почты	

Владелец сертификата ключа подписи[1] _____ _____
подпись Ф.И.О.

паспорт серии _____ № _____ выдан «____» _____ 20____ года

_____
наименование органа, выдавшего документ

_____ _____
подпись Ф.И.О. Заявителя

«____» _____ 20____ года

1 Для ИП, заполняется в случае изготовления сертификата не на заявителя.

Приложение №4
к Регламенту электронного документооборота
Системы «Личный кабинет клиента»

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, ___*ФИО*___, ___*Документ, удостоверяющий личность*___, проживающий по адресу _____

настоящим даю свое согласие АО «ДК РЕГИОН», 119021, г. Москва, бульвар Зубовский, д. 11А, этаж 7, помещение I, комната 1 (далее – Оператор) на обработку Оператором (включая получение от меня и/или любых третьих лиц) моих персональных данных.

Согласие дается мною с целью выполнения Оператором своих функций, полномочий и обязанностей, вытекающих из федеральных законов, иных правовых актов (в том числе актов федеральных органов власти, Банка России), из условий гражданско-правовых договоров, а также из условий гражданско-правовых договоров Оператора с юридическими или физическими лицами, от имени которых я действую.

Согласие распространяется на следующую информацию, включая (но, не ограничиваясь): мои фамилию, имя, отчество, год, месяц, дата и место рождения; гражданство (подданство); сведения о документе, удостоверяющем личность; сведения о документе, подтверждающем право иностранного гражданина или лица без гражданства на пребывание (проживание) в РФ; данные миграционной карты; адрес места жительства (регистрации); места пребывания (почтовый адрес); адреса средств (систем) связи (номера телефонов, факсов, электронные адреса); индивидуальный номер налогоплательщика (ИНН); занимаемую должность; и любую иную информацию, относящуюся к моей личности, доступную либо известную в любой конкретный момент времени Оператору (далее - «Персональные данные») и предусмотренную Федеральным законом от 27.07.2006 №152-ФЗ РФ «О персональных данных».

Настоящее согласие дается мною бессрочно, но может быть отозвано в письменном виде. При этом Оператор должен прекратить обработку моих персональных данных и уничтожить их в соответствии ст.21 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», за исключением персональных данных, включенных в документы, обязанность по хранению которых прямо предусмотрена законодательством и внутренними документами Оператора. В случае отзыва настоящего согласия персональные данные, включенные в документы, образующиеся в деятельности Оператора, в том числе внутренние документы Оператора в период действия согласия, могут передаваться третьим лицам в объеме и в случаях, указанных в настоящем согласии.

Настоящее согласие предоставляется на автоматизированную и неавтоматизированную обработку моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая, без ограничения: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение, трансграничную передачу, а также осуществление любых иных действий с моими Персональными данными с учетом действующего законодательства.

Настоящим я признаю и подтверждаю, что в случае необходимости предоставления персональных данных для достижения указанных выше целей третьим лицам, Оператор вправе, в необходимом объеме, раскрывать информацию обо мне лично (включая мои персональные данные) таким третьим лицам, их уполномоченным лицам, а также предоставлять таким лицам соответствующие документы, содержащие такую информацию. Также настоящим признаю и подтверждаю, что настоящее согласие считается данным мною любым третьим лицам, указанным выше, с учетом соответствующих изменений, и любые такие третьи лица имеют право на обработку моих персональных данных на основании настоящего согласия при условии соблюдения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и иных действующих федеральных законов.

Подпись:

_____

(Ф.И.О. полностью, подпись)

«__» _____ 201_ г.

Приложение №5
к Регламенту электронного документооборота
Системы «Личный кабинет клиента

АНКЕТА УЧАСТНИКА ЛКК

Участник ЛКК (Наименование организации, ОГРН для юридического лица; ФИО, паспортные данные для физического лица и ИП**)**	
Почтовый адрес для направления корреспонденции (с указанием индекса**)**	
ФИО, контактный телефон и адрес электронной почты для решения вопросов оплаты счетов, оформления, подписания и предоставления финансовых документов.	
ФИО, контактный телефон и адрес электронной почты для решения организационных вопросов	
ФИО, контактный телефон и адрес электронной почты для решения технических вопросов	

Список сотрудников Организации Участника ЛКК:

ФИО сотрудника	**Email**	**Телефон**	**ИНН**	**Паспортные данные**	**Доверенность**	**Доступные пулы**	**Полномочия**[1]

[1] Возможные полномочия сотрудника:

- Полный доступ
- Действия без подписи
- Только просмотр

Приложение №6
к Регламенту электронного документооборота
Системы «Личный кабинет клиента»

Перечень удостоверяющих центров

Наименование	Сайт	телефон
ЗАО «Национальный удостоверяющий центр»	https://nucrf.ru/	8(495)690-92-22
Удостоверяющий центр «e-Notary» компании ЗАО «Сигнал-КОМ»	https://www.e-notary.ru	8(495)663-30-73

Приложение №7
к Регламенту электронного документооборота
Системы «Личный кабинет клиента»

Форма заявления на отзыв сертификата ключа проверки электронной подписи Пользователя

Заявление
об отзыве сертификата ключа проверки электронной подписи

Прошу Вас отозвать сертификат ключа проверки электронной подписи, идентифицируемый перечисленными ниже параметрами:

Серийный номер сертификата	
ФИО владельца сертификата	
Причина отзыва	Например: - Изменение сведений, указанных в сертификате - увольнение с работы - перевод на другую должность - смена персональных данных владельца сертификата - выявление ошибок в реквизитах - компрометация ключа

Владелец сертификата/Руководитель организации

_____ / _____ /

« __ » _____ 201_ г.

М.П.

Настоящим подтверждаю, что Заявление на отзыв сертификата ключа проверки электронной подписи на имя

_____получено,
(Ф.И.О.)
личность идентифицирована, сведения, указанные в Заявлении проверены.

Администратор УЦ: _____ /_____ /

(подпись) фамилия, инициалы

«____» _____ 20___г

Приложение №8
к Регламенту электронного документооборота
Системы «Личный кабинет клиента»

Уведомление клиентов о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц, не имеющим право совершать транзакции от лица клиента. Рекомендации клиентам по защите от противоправного доступа и о рисках вредоносных программ

I. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц,

В соответствии с требованиями Положения об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций (утв. Банком России 17.04.2019 № 684-П) **Акционерное общество «Депозитарная компания «РЕГИОН»** (далее – «Общество») настоящим **уведомляет** клиентов Общества о возможных рисках финансовых потерь из-за:

- несанкционированного доступа к Вашей информации лицами, не обладающими правом осуществления финансовых операций;

- потери (хищения) носителей ключей электронной подписи, с использованием которых, осуществляются финансовые операции;

- воздействия вредоносного кода на устройства, с которых совершаются финансовые операции;

- совершения в отношении Вас иных противоправных действий.

При осуществлении финансовых операций следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, такие риски могут быть обусловлены включая, но не ограничиваясь следующими примерами:

a. Кража пароля и идентификатора доступа или иных конфиденциальных данных, например, закрытого ключа посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа.

b. Установка на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от Вашего имени.

c. Использования злоумышленником утерянного или украденного телефона для получения СМС кодов, которые могут применяться Обществом в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту.

d. Кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами Общества для получения данных и/или несанкционированного доступа к сервисам с этого устройства.

e. Получение пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Общества или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные; или направляет поддельные почтовые сообщения или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привес к компрометации устройства;

f. Перехвата почтовых сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша почта используется для информационного обмена с Обществом. В случае получения доступа к вашей почте, отправка сообщений от Вашего имени в Общество.

Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к информационным системам Общества несет Владелец учётных данных.

Общество не несет ответственность в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами информационной безопасности.

II. Меры по предотвращению несанкционированного доступа к защищаемой информации.

1. Обеспечьте защиту устройства, с которого вы пользуетесь услугами Общества, к таким мерам включая, но не ограничиваясь могут быть отнесены:
   - Использование только лицензированного программного обеспечения, полученного из доверенных источников.
   - Запрет на установку программ из непроверенных источников.
   - Наличие средства защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран, защита накопителя.
   - Настройка прав доступа к устройству с целью предотвращения несанкционированного доступа.
   - Хранение, использование устройства с целью избежать рисков кражи и/или утери.
   - Своевременные обновления операционной системы.
   - Активация парольной или иной защиты для доступа к устройству.
   - В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль.
   - Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины.
2. Обеспечьте конфиденциальность:
   - Храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Общества: пароли, СМС коды, кодовые слова, закрытые ключи, сертификаты, а в случае компрометации немедленно примите меры для смены и/или блокировки;
   - Соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC кодах, в случае если у вас запрашивают указанную информацию, в привязке к сервисам Общества по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон контакт центра Общества.
3. Проявляйте осторожность и предусмотрительность:
   - Будьте осторожны при получении писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к Вам через почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве.
   - Внимательно проверяйте адресата, от которого пришло письмо. Входящее письмо может быть от злоумышленника, который маскируется под Общество или иных доверенных лиц.
   - Будьте осторожны при просмотре/работе с интернет сайтами, так как вредоносный код может быть загружен с сайта.
   - Будьте осторожны с файлами в архиве с паролем, так как в таком файле может быть вредоносный код.
   - Не заходите в системы удаленного доступа с недоверенных устройств, которые вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию.
   - Анализируйте информацию в прессе и на сайте Общества о последних критичных уязвимостях и о вредоносном коде.
   - При наличии в рамках вашего продукта сервиса контакт центра, осуществляйте звонок только по номеру телефона, указанному в договоре. Важно учесть, что от лица

Общества не могут поступать звонки или сообщения, в которых от Вас требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д.

- Имейте в виду, что если Вы передаете ваш телефон и/или устройство другим пользователям, они могу установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Общества, которыми пользовались Вы.
- При утере, краже телефона, используемого для получения СМС кодов или доступа к системам Общества необходимо:
    a. незамедлительно проинформировать Общество через контактный центр;
    b. целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить сим карту;
    c. сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Общество.
- При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Общество, в отношении ключевой информации, если это уместно для Вашей услуги – отозвать скомпрометированный закрытый ключ, в соответствии с правилами, отраженными в договорных и/или процедурных документах;
- Помните, что наличие резервной копии может облегчить и ускорить восстановление Вашего устройства;
- Лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Вас;
- Контролируйте свой телефон, используемый для получения СМС кодов. В случае выхода из строя сим карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.
- Регулярно выполняйте резервное копирование важной информации.
- Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

4. При работе с ключами электронной подписи необходимо:
    - Использовать для хранения секретных ключей электронной подписи внешние носители.
    - Крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они не используются для работы.
    - Использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи, не хранить пароли в текстовых документах на компьютере.
5. При работе на компьютере необходимо:
    - Использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);
    - Своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);
    - Использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы;
    - Использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;
    - Использовать сложные пароли;
    - Ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.
6. При работе с мобильным устройством необходимо:
    - Не оставлять свое Мобильное устройство без присмотра, чтобы исключить несанкционированное использование;
    - Использовать только официальные Мобильные приложения;
    - Не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Общества;
    - Установить на Мобильном устройстве пароль для доступа к устройству.

7. При обмене информацией через сеть Интернет необходимо:
    - Не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;
    - Не вводить персональную информацию на подозрительных сайтах и других неизвестных Вам ресурсах;
    - Ограничить посещения сайтов сомнительного содержания;
    - Не сохранять пароли в памяти интернет-браузера, если к компьютеру есть доступ третьих лиц;
    - Не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;
    - Открывать файлы только известных Вам расширений (docx, png, xlsx и т.д.).

При подозрении в компрометации ключей или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов необходимо незамедлительно обращаться в Общество (тел. +7 (495) 777-29-64, email: depo@region.ru)

Ознакомлен:

Клиент _____

«___»_____ 20__г.

Всего 24 листа.

Генеральный директор
АО «ДК РЕГИОН»
Зайцева А.А.

Акционерное общество * ОГРН 1037708002144 *
"Депозитарная компания "РЕГИОН"
МОСКВА