УТВЕРЖДЕНО
Приказом Генерального директора
АО «ДК РЕГИОН»
№ ДК-25Д от 24.06.2026 г.

Дата вступления в силу 09.07.2026 г.

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

Москва
2026

Термины и определения

Аккредитованный удостоверяющий центр (Аккредитованный УЦ, УЦ) – юридическое лицо или индивидуальный предприниматель, получившие аккредитацию федерального органа исполнительной власти, уполномоченного в сфере использования электронной подписи, осуществляющие 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 Аккредитованных УЦ опубликован на официальном сайте федерального органа исполнительной власти, уполномоченного в сфере использования электронной подписи.

Владелец Квалифицированного сертификата ключа проверки электронной подписи - Участник, в лице своего Уполномоченного Представителя, которому в установленном порядке Аккредитованным удостоверяющим центром выдан Квалифицированный сертификат ключа проверки электронной подписи.

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

Квалифицированный сертификат ключа проверки электронной подписи (Квалифицированный сертификат) – электронный документ или документ на бумажном носителе, выданный Аккредитованным удостоверяющим центром, подтверждающий принадлежность ключа проверки электронной подписи владельцу квалифицированного сертификата ключа проверки электронной подписи и соответствующий требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами.

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

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

Организатор электронного документооборота (ЭДО) – АО «ДК РЕГИОН».

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

Регламент удостоверяющего центра – документ, разработанный и утвержденный 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 Аккредитованного УЦ в сети интернет.

Система «Личный кабинет клиента» (ЛКК, Система) – 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.

Специализированный депозитарий/ Специализированный регистратор/ Депозитарий - Акционерное общество «Депозитарная компания РЕГИОН», 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.

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.

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».

УКЭП, усиленная квалифицированная электронная подпись, электронная подпись - усиленная квалифицированная электронная подпись, которая соответствует определению и признакам, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Аккредитованного удостоверяющего центра и наделенное полномочиями по заверению от лица Удостоверяющего центра сертификатов ключей проверки подписей и списков отозванных сертификатов.

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 электронного документооборота - Акционерное общество «Депозитарная компания РЕГИОН» (АО «ДК РЕГИОН») и его клиенты (далее также - Клиенты), присоединившиеся к настоящему Регламенту и осуществляющие обмен информацией в электронной форме с использованием УКЭП.

Формат электронного документа – набор требований к структуре и реквизитам электронного документа.

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

Электронный документ (ЭД) – документированная информация, представленная в электронно-цифровой форме (файл данных в терминах операционной системы), представляющая собой совокупность структурированных данных, пригодных для восприятия Участниками с использованием электронных вычислительных машин, и позволяющая обеспечить ее передачу и 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 информацию о дате, времени и содержании операций, производимых в Системе.

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 Аккредитованные 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 и Анкеты по форме Приложения № 2 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, но не ранее чем через 10 (Десять) рабочих дней с даты опубликования новой редакции Регламента на сайте АО «ДК РЕГИОН».
1.10. Уведомление Участников о внесении изменений и/или дополнений в Регламент осуществляется путем публикации сообщения на сайте АО «ДК РЕГИОН» одновременно с опубликованием новой редакции Регламента.

2. Аккредитованный удостоверяющий центр и сертификаты ключей

2.1. 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.
2.2. При организации и функционировании ЭДО принимаются и признаются Квалифицированные сертификаты ключа проверки электронной подписи, выданные Аккредитованным удостоверяющим центром, в составе и формате, определяемом Аккредитованным удостоверяющим центром.
2.3. Квалифицированный сертификат признается изданным Аккредитованным удостоверяющим центром, если подтверждена подлинность электронной подписи этого сертификата, сделанной Уполномоченным лицом Аккредитованного удостоверяющего центра.
2.4. Идентификационные данные, занесенные в поле «Субъект» (Subject Name) Квалифицированного сертификата, однозначно идентифицируют Владельца сертификата ключа проверки подписи и соответствуют идентификационным данным Владельца сертификата ключа проверки подписи.
2.5. Для определения статуса Квалифицированного сертификата, получения актуального списка отозванных сертификатов, актуальных сертификатов уполномоченных лиц УЦ участниками ЭДО используется сертифицированное ФСБ России СКЗИ.

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

3. Документы, подписываемые УКЭП

3.1. Перечень электронных документов, подписание которых УКЭП предполагается в рамках настоящего Регламента, приведены:
– в Приложении № 1 к Правилам ведения реестра владельцев инвестиционных паев паевых инвестиционных фондов специализированного депозитария АО «ДК РЕГИОН»,
- Приложениях № 1 и № 2 к Регламенту специализированного депозитария ипотечного покрытия АО «ДК РЕГИОН»,
- Регламенте депозитарного обслуживания АО «ДК РЕГИОН».

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 УКЭП Уполномоченных представителей.

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

4.3. Усиленной квалифицированной электронной подписью является электронная подпись, которая соответствует признакам, указанным в Федеральном законе от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4.4. Для формирования и проверки электронной подписи в ЛКК используется сертифицированное ФСБ России СКЗИ.

4.5. 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.

4.6. 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.

4.7. 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.

4.8. Сертификат ключа проверки электронной подписи считается аннулированным (отозванным) с момента публикации УЦ списка отозванных сертификатов, в котором содержится серийный номер данного сертификата.

4.9. Размещенные в ЛКК электронные документы, подписанные корректной УКЭП, имеют равную юридическую силу с документами на бумажном носителе, подписанными Участниками и скрепленными оттисками печатей.

4.10. Электронная подпись считается корректной, если получен положительный результат проверки подписи.

4.11. Результат проверки ЭП считается положительным, если:
- подтверждена Подлинность электронной подписи в электронном документе,

- ключ электронной подписи действителен на момент подписи.

4.12. 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 Регламентов и Правил, перечисленных в п. 3.1 настоящего Регламента, 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, Регламентами и Правилами, перечисленными в п. 3.1 настоящего Регламента.

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, которые 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, не имеющими право совершать транзакции от лица клиента, являющимся Приложением № 3 к настоящему Регламенту.

5.5. Участники совместно обязуются:
5.5.1. Не предпринимать действий, способных нанести ущерб другому Участнику вследствие использования ЛКК.
5.5.2. Незамедлительно уведомить другого Участника 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 ЛКК.
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, Регламентов и Правил, перечисленных в п. 3.1 настоящего Регламента, договоров, заключенных между Участниками, форматам, установленным ЛКК, а также наличия корректной УКЭП.
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 УКЭП 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 УКЭП 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 УКЭП, 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 Участником документов и информации, сформированных в электронном виде с помощью ЛКК, является дата размещения Участником подписанных УКЭП документов и информации в ЛКК в соответствии с настоящим Регламентом.

6.12. 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 УКЭП 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;

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

7.4. Каждый из Участников 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 о вручении, с приложением копий документов, подтверждающих обоснование заявленной претензии.

8.4. Срок ответа на претензию -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 Участников 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 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»

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/ уполномоченного представителя		ФИО Руководителя/ уполномоченного представителя	
	Доверенность № _____ от _____ г.		
Дата заявления		Подпись	

М.П.

Приложение № 2
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**)**	
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 (полностью)	**Email**	**№ и дата договора с АО «ДК РЕГИОН»**	**Доступные пулы (№ счетов)**	**Полномочия[1]**

[1] Возможные полномочия сотрудника:

- Полный доступ
- Действия без подписи
- Только просмотр

_____ (должность) _____ (подпись)
_____(ФИО)

М.П.

_____ дата

Приложение № 3
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 имеющих 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 20.04.2021 № 757-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. Использование 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. Перехват почтовых сообщений и получение 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.