

Казахстан – **Сентябрь 2026**

Цифровой кодекс Республики Казахстан

12 июля 2026 года вступил в силу Цифровой кодекс Республики Казахстан от 9 января 2026 года № 255-VIII «Цифровой кодекс Республики Казахстан» (далее – **«Цифровой кодекс»**). Кодекс формирует единую правовую основу для отношений в цифровой среде, связанных с созданием, обращением, хранением, передачей и использованием цифровых данных и цифровых объектов. Цифровым кодексом и иными законами РК по вопросам регулирования отношений в цифровой среде применяются положения Цифрового кодекса. При этом международные договоры, ратифицированные РК, имеют приоритет перед Цифровым кодексом¹.

С момента введения Цифрового кодекса в действие утратил силу Закон РК от 7 января 2003 года «Об электронном документе и электронной цифровой подписи». Соответствующие вопросы теперь регулируются непосредственно Цифровым кодексом.

Ключевые принципы нового регулирования включают защиту прав и законных интересов человека, безопасность цифровой среды, свободу обращения цифровых данных и применения цифровых технологий, баланс частных и публичных интересов, технологическую нейтральность и цифровую этику². Ниже приведены основные положения, которые, на наш взгляд, могут иметь практическое значение для бизнеса.

1. Цифровые данные и цифровые объекты

Цифровой кодекс закрепляет общий принцип свободного создания, сбора, хранения, обработки, использования и передачи цифровых данных. Для данных, содержащих персональные данные, государственные секреты, конфиденциальную или иную охраняемую законом информацию, сохраняются специальные требования соответствующего законодательства³.

Цифровой кодекс также закрепляет права физических и юридических лиц, к которым относятся обрабатываемые в цифровой среде данные. Такие лица вправе получать доступ к своим данным, контролировать их использование, требовать их удаления или ограничения обработки, а также получать информацию о целях, правовых основаниях и способах обработки. Субъект персональных данных вправе требовать удаления, анонимизации или ограничения обработки своих персональных данных, кроме случаев, когда их сохранение необходимо для исполнения требований законодательства или договора, защиты прав третьих лиц, осуществления правосудия, государственной статистики либо выполнения государственных функций⁴.

Кодекс также систематизирует правовой режим цифровых объектов. К ним, в частности, относятся цифровые записи, цифровые активы, цифровые ресурсы, программное обеспечение,

¹ Ст. 1-2 Цифрового кодекса РК;

² Ст. 4 Цифрового кодекса РК;

³ Ст. 16 Цифрового кодекса РК;

⁴ Ст. 37 и 41 Цифрового кодекса РК;

цифровые системы, цифровые платформы, объекты цифровой инфраструктуры и продукты цифровых данных⁵. Собственники и владельцы цифровых объектов обязаны соблюдать права третьих лиц, включая требования о защите персональных данных и конфиденциальной информации, и принимать меры против неправомерного доступа, копирования, изменения или удаления цифровых данных и объектов.

Отдельно регулируются объекты цифровой инфраструктуры, включая центры обработки данных, телекоммуникационные сети и средства связи, а также распределенные цифровые объекты. Последние могут быть централизованно-распределенными или децентрализованными. Для совместного владения, пользования и распоряжения распределенными цифровыми объектами Цифровой кодекс вводит конструкцию «цифрового кондоминиума», права участников которого определяются соглашением или смарт-контрактом⁶.

Цифровые активы остаются предметом специального регулирования: особенности их выпуска, обращения, хранения и учета определяются Законом РК «О цифровых активах в РК», а положения Цифрового кодекса применяются в части, не урегулированной специальным законодательством⁷.

2. Цифровые платформы и оборот продуктов цифровых данных

Цифровой кодекс различает обычных пользователей цифровых платформ и бизнес-пользователей. Бизнес-пользователями признаются физические или юридические лица, использующие платформу для продажи товаров, выполнения работ, оказания услуг или иной деятельности, связанной с извлечением дохода. Деятельность на платформах и требования к их пользователям дополнительно регулируются отраслевым законодательством.

Для владельцев цифровых платформ ключевым требованием является прозрачность условий использования платформы, которые должны быть отражены в пользовательском соглашении.

Требования к цифровым платформам должны соответствовать выполняемым ими функциям, степени их влияния на права неопределенного круга лиц и характеру контроля над цифровыми данными, услугами, товарами и результатами взаимодействия пользователей⁸.

Отдельный режим установлен для платформ обмена и оборота продуктов цифровых данных. Под продуктом цифровых данных понимается агрегированный и формализованный результат обработки цифровых данных, включающий структурированные или иным образом преобразованные данные, пригодные для использования, обмена и (или) оборота в цифровой среде. Такие платформы могут создаваться, в том числе, субъектами частного предпринимательства при соблюдении требований в сфере цифровизации и кибербезопасности⁹.

Их собственники и владельцы обязаны:

⁵ Ст. 20 Цифрового кодекса РК;

⁶ Ст. 25, 35 Цифрового кодекса РК;

⁷ Ст. 22 Цифрового кодекса РК;

⁸ Ст. 29 Цифрового кодекса РК;

⁹ Ст. 30 Цифрового кодекса РК;

- вести перечень размещенных продуктов цифровых данных и обеспечивать условия доступа, обмена и использования;
- принимать меры против несанкционированного доступа, утечки и ограниченной законом трансграничной передачи продуктов цифровых данных;
- с момента начала деятельности направлять уведомление в Агентство Республики Казахстан по стратегическому планированию и реформам в соответствии с законодательством о разрешениях и уведомлениях.

Для таких платформ также установлен ряд запретов, включая оборот исходных (необработанных) данных, в том числе персональных данных, если иное прямо не предусмотрено законом, а также передачу продуктов цифровых данных третьим лицам без согласия их собственника или владельца, за исключением предусмотренных законом случаев¹⁰.

3. Алгоритмические системы и искусственный интеллект

Цифровой кодекс не заменяет Закон РК «Об искусственном интеллекте», но устанавливает общие правила для алгоритмических систем и полностью автоматизированных решений. Алгоритмическая система определяется как цифровая система, которая принимает решения или влияет на их принятие на основе автоматизированной обработки данных, включая системы искусственного интеллекта¹¹.

Решения, принимаемые с использованием алгоритмических систем, не должны приводить к дискриминации. Лицо, в отношении которого применяется полностью автоматизированное решение, вправе получить информацию о факте использования алгоритмической системы, а также объяснение ключевых факторов и критериев, повлиявших на решение, без раскрытия алгоритма, исходного кода или охраняемой законом тайны. Если решение влечет юридические последствия либо способно повлиять на права и законные интересы лица, оно вправе потребовать, чтобы решение было пересмотрено уполномоченным сотрудником той организации или того государственного органа, которые применяют алгоритмическую систему и принимают соответствующее решение¹².

Цифровой кодекс также предусматривает аудит качества цифровых объектов. При аудите качества систем искусственного интеллекта учитываются качество и правомерность использования библиотек данных, применяемых для обучения моделей, а также наличие запрещенных функциональных возможностей в соответствии с законодательством об искусственном интеллекте¹³.

4. Цифровая идентификация, электронная цифровая подпись и электронные документы

Правоотношения в цифровой среде осуществляются с использованием технологий, позволяющих идентифицировать участников, подтверждать их волеизъявление и фиксировать юридически значимые факты. Уникальными идентификаторами являются ИИН для физических лиц и БИН для юридических лиц, филиалов и представительств, а также индивидуальных

¹⁰ Ст. 31 Цифрового кодекса РК;

¹¹ Ст. 43 Цифрового кодекса РК;

¹² Ст. 43 Цифрового кодекса РК;

¹³ Ст. 100 Цифрового кодекса РК;

предпринимателей, осуществляющих деятельность в форме совместного предпринимательства¹⁴.

Цифровая аутентификация используется для подтверждения личности физического лица или правоспособности юридического лица при доступе к цифровым услугам и объектам. Цифровая аутентификация с использованием многофакторных средств может служить основанием для возникновения, изменения или прекращения правоотношений в цифровой среде, а также использоваться для доказывания юридически значимых действий¹⁵.

Кодексы, пароли, одноразовые цифровые идентификаторы, push-уведомления, биометрические подтверждения и другие предусмотренные Цифровым кодексом инструменты могут использоваться в качестве цифрового подтверждения в случаях, установленных законодательством или соглашением сторон. Однако цифровое подтверждение не является ЭЦП и само по себе не обеспечивает достоверность и неизменность содержания цифровой записи.

Электронная цифровая подпись (далее – «ЭЦП») равнозначна собственноручной подписи при соблюдении установленных Цифровым кодексом условий. Сертификат открытого ключа должен быть выдан удостоверяющим центром, аккредитованным в РК, либо иностранным удостоверяющим центром, зарегистрированным в доверенной третьей стороне РК. Поэтому иностранная ЭЦП признается в Казахстане только при соблюдении установленного механизма трансграничного подтверждения ее подлинности¹⁶.

Передача закрытого ключа ЭЦП другому лицу и его использование другим лицом запрещаются. Владелец сертификата обязан защищать закрытый ключ от неправомерного доступа и использования. Сертификат ЭЦП подлежит отзыву, в частности, при смене руководителя или наименования юридического лица, а также при его реорганизации или ликвидации¹⁷.

Электронный документ, подписанный ЭЦП уполномоченного лица, равнозначен документу на бумажном носителе. Руководитель юридического лица вправе уполномочить работника или иное назначенное лицо на подписание электронных документов, однако соответствующее лицо должно использовать сертификат и закрытый ключ ЭЦП, выданные на его собственное имя.

Цифровой кодекс также регулирует смарт-контракты, предусматривающие автоматическое исполнение согласованных сторонами условий. Условия смарт-контракта могут быть выражены программным кодом, если содержание прав и обязанностей сторон можно однозначно определить и воспроизвести в доступной для восприятия человеком форме. Смарт-контракт должен предусматривать порядок разрешения споров, при котором окончательное решение принимается человеком¹⁸.

5. Цифровое государственное управление

Значительная часть Цифрового кодекса посвящена цифровизации государственного управления. Кодекс устанавливает основы цифровой архитектуры государства и «цифрового правительства»,

¹⁴ Ст. 44 и 45 Цифрового кодекса РК;

¹⁵ Ст. 46 и 47 Цифрового кодекса РК;

¹⁶ Ст. 49 и 57 Цифрового кодекса РК;

¹⁷ Ст. 51, 58, 59 и 62 Цифрового кодекса РК;

¹⁸ Ст. 40 Цифрового кодекса РК;

регулирует единые государственные цифровые платформы, веб-портал «цифрового правительства», цифровые события, проактивное предоставление государственных услуг, а также жизненный цикл государственных цифровых объектов¹⁹.

Государственные органы и иные субъекты, имеющие доступ к национальным регистрам, обязаны получать необходимые сведения непосредственно из соответствующих источников и не должны требовать от физических и юридических лиц документы, если необходимые сведения уже содержатся в национальных регистрах. Кроме того, государственные извещения, направляемые через единую точку уведомлений, признаются доставленными при наличии информации об их надлежащей доставке²⁰.

Для бизнеса эти положения имеют практическое значение в части получения электронных государственных услуг и взаимодействия с государственными цифровыми системами. Компаниям рекомендуется обеспечивать актуальность своих контактных данных и регулярно проверять государственные цифровые сервисы, поскольку надлежащим образом доставленные цифровые извещения могут иметь юридические последствия.

6. Кибербезопасность, государственный контроль и ответственность

Цифровой кодекс устанавливает два отдельных правовых режима для доверенных и критически важных цифровых объектов. Цифровой объект признается доверенным, если он соответствует установленным требованиям безопасности, надежности, локализации и технической поддержки и включен в реестр доверенных цифровых объектов. Государственные органы, государственные юридические лица и субъекты квазигосударственного сектора приобретают цифровые объекты, включенные в реестр доверенных цифровых объектов. Цифровые объекты в сфере здравоохранения, банковской деятельности, связи, транспорта, промышленности и иных значимых отраслях могут быть признаны критически важными. Их владельцы обязаны соблюдать специальные требования кибербезопасности и в предусмотренных законодательством случаях проводить аудит кибербезопасности²¹.

Цифровой кодекс закрепляет государственный контроль в сфере цифровизации, электронного документа и ЭЦП. Контроль может осуществляться в форме проверок и профилактического контроля в соответствии с Предпринимательским кодексом РК и законодательством о кибербезопасности²².

Защита цифровых объектов возлагается на их собственников и владельцев. Защита цифровых данных должна включать технические, организационные, правовые и иные меры, направленные на предупреждение, выявление и устранение киберугроз²³. Для определенных законодательством цифровых объектов испытания на соответствие требованиям кибербезопасности являются обязательными. В остальных случаях испытания и аудит могут проводиться по инициативе собственника или владельца цифрового объекта. Владельцы

¹⁹ Ст. 68 Цифрового кодекса РК;

²⁰ Ст. 64 и 66 Цифрового кодекса РК;

²¹ Ст. 32 и 33 Цифрового кодекса РК;

²² Ст. 96 Цифрового кодекса РК;

²³ Ст. 97 и 98 Цифрового кодекса РК;

критически важных цифровых объектов обязаны проводить аудит кибербезопасности в случаях, предусмотренных законами РК²⁴.

Нарушение цифрового законодательства влечет ответственность, установленную законами РК. Привлечение к административной или уголовной ответственности не освобождает виновное лицо от обязанности устранить допущенные нарушения²⁵.

В целом Цифровой кодекс формирует базовый правовой режим для цифровых данных, цифровых объектов и платформ, алгоритмических систем, цифровой идентификации, электронных документов и кибербезопасности. Компаниям рекомендуется определить свой статус в соответствии с Цифровым кодексом, проверить необходимость включения используемых платформ и цифровых объектов в соответствующие реестры, актуализировать пользовательские соглашения и внутренние правила обработки данных, а также обеспечить соблюдение требований к цифровой аутентификации, ЭЦП и кибербезопасности.

Контакты:



Зафар Вахидов

Партнер, Vakhidov & Partners
Казахстан/Узбекистан
ZV@vakhidovlaw.com



Жанибек Нурғали

Юрист, Vakhidov & Partners
Казахстан
ZhanibekN@vakhidovlaw.com

²⁴ Ст. 33 и 99 Цифрового кодекса РК;

²⁵ Ст. 105 Цифрового кодекса РК;