“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=382

2026-yil
8-son
avgust
ISSN 3093-8546

Международные документы по кибербезопасности в Международном коммерческом арбитраже (протокол Icca – New York City Bar – CPR, Руководство IBA по кибербезопасности): перспективы гражданско-правовой рецепции в законодательстве Республики Узбекистан

Бегаим Кайбылдаева,
Независимый исследователь
Ташкентский государственный юридический университет
e-mail: begaimkaibyldaeva@gmail.com

Аннотация. Maqola xalqaro tijorat arbitrajida kiberxavfsizlik bo‘yicha xalqaro tavsiyaviy hujjatlar – ICCA – New York City Bar – CPR Protokoli va IBA kiberxavfsizlik bo‘yicha qo‘llanmasi tahliliga hamda ularning O‘zbekiston Respublikasi qonunchiligida fuqarolik-huquqiy istiqbollariga bag‘ishlangan. Ushbu softlaw hujjatlarining huquqiy tabiati, tuzilishi va mazmuni, shuningdek ularning arbitraj ishtirokchilari uchun tegishli ehtiyotkorlik standartlariga ta’siri ochib beriladi. O‘zbekiston Respublikasi Fuqarolik kodeksi, “Xalqaro tijorat arbitraji to‘g‘risida”gi, “Kiberxavfsizlik to‘g‘risida”gi va “Shaxsiy ma’lumotlar to‘g‘risida”gi qonunlar tahlili asosida milliy tartibga solishning xalqaro protokollar bilan mos nuqtalari, shuningdek mavjud bo‘shliqlar aniqlanadi. Xalqaro standartlarni retsepsiya qilishning shartnomaviy, normativ va huquqni qo‘llash kanallari taklif etilib, qonunchilikka aniq o‘zgartirishlar shakllantiriladi.

Калит сўзлар. xalqaro tijorat arbitraji, kiberxavfsizlik, ICCA – New York City Bar – CPR Protokoli, IBA kiberxavfsizlik bo‘yicha qo‘llanmasi, fuqarolik-huquqiy retsepsiya, shaxsiy ma’lumotlar, axborot xavfsizligi, O‘zbekiston, yumshoq huquq.

Аннотация. Статья посвящена анализу международных рекомендательных документов по кибербезопасности в международном коммерческом арбитраже – ПротоколаICCA–NewYorkCityBar–CPRи РуководстваIBAпо кибербезопасности и перспективам их гражданско-правовой рецепции в законодательстве Республики Узбекистан. Раскрывается правовая природа указанныхsoftlaw-документов, их структура и содержание, а также механизм влияния на стандарты должной осмотрительности участников арбитражного разбирательства. На основе анализа Гражданского кодекса, Закона о международном коммерческом арбитраже, Закона о кибербезопасности и Закона о персональных данных Республики Узбекистан выявляются точки соприкосновения национального регулирования с международными протоколами, а также существующие

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

пробелы. Предлагаются договорный, нормотворческий и правоприменительный каналы рецепции международных стандартов и формулируются конкретные изменения в законодательство.

Ключевые слова. международный коммерческий арбитраж, кибербезопасность, Протокол ICCA – New York City Bar – CPR, Руководство IBA по кибербезопасности, гражданско-правовая рецепция, персональные данные, информационная безопасность, Узбекистан, мягкое право.

Annotation. The article examines international soft-law instruments on cybersecurity in international commercial arbitration – the ICCA – New York City Bar – CPR Cybersecurity Protocol and the IBA Cybersecurity Guidelines and the prospects for their civil-law reception in the legislation of the Republic of Uzbekistan. It reveals the legal nature, structure and content of these instruments and their influence on the due-diligence standards applicable to arbitration participants. Based on an analysis of the Civil Code, the Law on International Commercial Arbitration, the Law on Cybersecurity and the Law on Personal Data of the Republic of Uzbekistan, the article identifies points of convergence between national regulation and the international protocols, as well as existing gaps. Contractual, legislative and adjudicative channels of reception are proposed, together with concrete legislative amendments.

Keywords. international commercial arbitration, cybersecurity, ICCA - New York City Bar - CPR Protocol, IBA Cybersecurity Guidelines, civil-law reception, personal data, information security, Uzbekistan, soft law.

Введение. Международный коммерческий арбитраж на протяжении последнего десятилетия претерпел глубокую технологическую трансформацию: обмен процессуальными документами, проведение слушаний, хранение доказательств и коммуникация между сторонами, арбитрами и администрирующими институтами всё в большей степени осуществляются в электронной форме. Эта цифровизация повлекла за собой возрастание рисков кибербезопасности, поскольку арбитражные разбирательства нередко затрагивают коммерческую тайну, персональные данные и иные сведения ограниченного доступа, представляющие интерес для злоумышленников. Реакцией международного арбитражного сообщества на данные риски стала разработка ряда рамочных документов рекомендательного характера, среди которых особое место занимают Протокол по кибербезопасности в международном арбитраже, подготовленный Международным советом по коммерческому арбитражу совместно с Нью-Йоркской ассоциацией адвокатов и Международным институтом по предотвращению и разрешению конфликтов, а также Руководство по кибербезопасности Международной ассоциации юристов.

Указанные документы относятся к так называемому мягкому праву и не обладают юридически обязывающей силой, однако их практическое влияние на формирование стандартов должной осмотрительности в арбитражной практике неуклонно возрастает. В этой связи возникает закономерный научный и практический вопрос о возможности и целесообразности гражданско-правовой рецепции соответствующих подходов в национальном законодательстве Республики Узбекистан, стремящейся утвердиться в качестве привлекательной площадки для проведения международных коммерческих арбитражей.

Настоящая статья ставит целью решение следующих задач: во-первых, раскрыть юридическую природу и содержание Протокола ICCA – Нью-Йоркская коллегия адвокатов – CPR и Руководства IBA по кибербезопасности; во-вторых, определить их место в системе источников регулирования международного коммерческого арбитража; в-третьих, оценить степень соответствия действующего гражданского и специального законодательства Республики Узбекистан заложенным в указанных документах принципам; в-четвёртых, сформулировать предложения по гражданско-правовой рецепции соответствующих механизмов.

Понятие и правовая природа международных softlaw-документов по кибербезопасности в арбитраже. Под международными softlaw-документами по кибербезопасности в арбитраже понимаются разработанные профессиональными и научными объединениями рекомендательные акты, устанавливающие стандарты информационной безопасности, применимые к участникам арбитражного разбирательства. Их отличительной особенностью является отсутствие формальной юридической силы: они не являются международными договорами и не подлежат ратификации, однако приобретают правовое значение опосредованно через включение в арбитражные регламенты, договорные условия между сторонами и администрирующими институтами, а также через формирование обычной практики (best practice), учитываемой при оценке разумности и добросовестности поведения участников разбирательства.

С гражданско-правовой точки зрения значение подобных документов проявляется в нескольких аспектах. Во-первых, они способны выступать источником толкования содержания обязательства по обеспечению конфиденциальности и информационной безопасности, вытекающего из арбитражного соглашения или регламента арбитражного института. Во-вторых, отступление от стандартов, зафиксированных в общепризнанных протоколах, может учитываться при установлении вины оператора информационной системы или иного субъекта, ответственного за защиту данных, в рамках деликтной или договорной

ответственности. В-третьих, инкорпорация подобных стандартов в процессуальные акты (регламенты, приказы о ведении дела) способна трансформировать рекомендательные положения в договорные обязательства, наделённые исковой защитой.

Протокол ICCA – Нью-Йоркская коллегия адвокатов – CPR: содержание и механизм применения. Протокол по кибербезопасности в международном арбитраже стал результатом многолетней совместной работы Международного совета по коммерческому арбитражу, Ассоциации адвокатов города Нью-Йорка и Международного института по предотвращению и разрешению конфликтов. Работа над документом была начата в 2017 году, консультационный проект представлен на Конгрессе ICCA в Сиднее в 2018 году, а окончательная редакция 2020 года подготовлена по итогам обширных консультаций, в которых приняли участие более двухсот сорока организаций и объединений, включая арбитражные институты, юридические фирмы и неправительственные организации [9]. Обновлённая редакция 2022 года была презентована на Конгрессе ICCA в Эдинбурге одновременно с запуском смежного документа дорожной карты по защите персональных данных в международном арбитраже, подготовленной совместно с Международной ассоциацией юристов [9].

Структурно Протокол построен по принципу трёхуровневой архитектуры: общие принципы, комментарии к ним и приложения (схемы), содержащие детализированные практические указания. Первые принципы определяют сферу применения документа: Протокол призван служить рекомендательной основой для определения разумных мер информационной безопасности применительно к конкретному арбитражному делу, а не устанавливать унифицированный обязательный стандарт [9]. Ключевая методологическая особенность заключается в отказе от единого («золотого») стандарта кибербезопасности в пользу гибкого, учитывающего обстоятельства конкретного спора подхода: степень чувствительности информации, характер сторон, юрисдикционные риски и ресурсные возможности участников.

Принципиальное значение для целей настоящего исследования имеет то обстоятельство, что Протокол прямо возлагает бремя оценки и внедрения информационно-защитных мер на всех «хранителей» арбитражной информации стороны, арбитров и администрирующие институты, исходя из идеи распределённой, а не централизованной ответственности. Кроме того, документ содержит примерный протокол уведомления об инцидентах кибербезопасности, что представляет особый интерес для сопоставления с публично-правовыми обязанностями операторов

информационных систем, установленными законодательством Республики Узбекистан.

Руководство IBA по кибербезопасности и его место в системе международных стандартов. Руководство по кибербезопасности Международной ассоциации юристов было подготовлено Президентской целевой группой по кибербезопасности, учреждённой в 2017 году, и представлено на ежегодной конференции ассоциации в Риме в октябре 2018 года [10]. В отличие от Протокола ICCA - Нью-Йоркская коллегия адвокатов - CPR, ориентированного непосредственно на арбитражное разбирательство, Руководство IBA адресовано более широкому кругу субъектов – юридическим фирмам и практикующим юристам в целом, однако его положения признаются применимыми и к деятельности арбитражных институтов, что подтверждается практикой их упоминания в качестве ориентира надлежащей осмотрительности в специализированной литературе по арбитражу [11].

Данная трёхкомпонентная модель, при её сопоставлении с законодательством Республики Узбекистан о кибербезопасности, обнаруживает существенное структурное сходство с обязанностями операторов информационных систем, однако узбекское законодательство не детализирует организационные и обучающие аспекты в той мере, в какой это делает Руководство IBA [11].

Важно также отметить взаимодополняющий характер рассматриваемых документов: Протокол по кибербезопасности в международном арбитраже прямо ссылается на дорожную карту по защите данных, разработанную совместно ICCA и IBA, подчёркивая, что соблюдение требований Протокола способствует также соответствию международным режимам защиты персональных данных, в том числе Общему регламенту Европейского союза о защите данных [9, С.1]. Кроме того, пересмотренные в 2020 году Правила Международной ассоциации юристов о представлении доказательств в международном арбитраже прямо включили вопросы кибербезопасности и защиты данных в перечень вопросов, подлежащих обязательному обсуждению между составом арбитража и сторонами на начальном этапе разбирательства (статья 2.2(e)) [10]. Данное обстоятельство свидетельствует о постепенной институционализации кибербезопасности как самостоятельного элемента процессуальной справедливости арбитражного разбирательства.

Соотношение международных протоколов с гражданским законодательством Республики Узбекистан. Гражданский кодекс Республики Узбекистан [1] не содержит специальных норм, регулирующих обязательства участников арбитражного разбирательства по обеспечению информационной безопасности. Регулирование данного вопроса осуществляется

опосредованно, посредством общих норм об обязательствах, о возмещении вреда (глава 57 Кодекса) и об оказании услуг. Закон Республики Узбекистан «О международном коммерческом арбитраже» [2] также не упоминает кибербезопасность в числе принципов арбитражного разбирательства и не содержит отсылок к международным протоколам подобного рода, что создаёт нормативный вакуум при определении применимого стандарта должной осмотрительности.

Вместе с тем ключевые содержательные элементы, зафиксированные в международных протоколах, находят частичное отражение в отраслевом законодательстве Республики Узбекистан. Закон «О кибербезопасности» [3] закрепляет обязанности операторов информационных систем по защите обрабатываемых данных, предотвращению инцидентов и уведомлению уполномоченных органов (статьи 12–14), что концептуально созвучно принципам уведомления об инцидентах, заложенным в Протоколе ICCA – Нью-Йоркская коллегия адвокатов – CPR. Закон «О персональных данных» [4] возлагает на операторов персональных данных обязанность принимать организационные и технические меры защиты, соотносимую с трёхкомпонентной моделью Руководства IBA. Постановление Кабинета Министров Республики Узбекистан № 570 [5] детализирует уровни защищённости персональных данных в зависимости от категории обрабатываемых сведений, что методологически сближается с дифференцированным, риск-ориентированным подходом международных протоколов, отвергающим единый обязательный стандарт защиты для всех случаев.

Постановление Президента Республики Узбекистан № ПП-167 [7], устанавливающее требования к операторам объектов критической информационной инфраструктуры, демонстрирует наиболее развёрнутый в национальном законодательстве пример детализированных технических и организационных требований, сопоставимых по глубине регулирования с международными протоколами. Однако арбитражные институты и обслуживающие их технологические платформы прямо не отнесены к объектам критической инфраструктуры, что оставляет данный сегмент вне сферы применения указанного постановления.

Таким образом, действующее законодательство Республики Узбекистан содержит отдельные фрагменты, функционально соотносимые с положениями международных протоколов, однако лишено специальной, системной привязки этих требований к арбитражному разбирательству как таковому. Данное обстоятельство обусловливает необходимость целенаправленной гражданско-правовой рецепции соответствующих международных подходов.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Проблемы и перспективы гражданско-правовой рецепции. Под гражданско-правовой рецепцией в настоящей статье понимается процесс адаптации и включения содержательных элементов международных рекомендательных документов в систему национального гражданского и специального законодательства посредством нормотворчества, договорной практики и правоприменения. Применительно к рассматриваемым протоколам можно выделить три возможных канала рецепции.

Первый канал – договорный. Стороны арбитражного соглашения и администрирующие институты вправе включать положения международных протоколов непосредственно в текст договора об организации арбитражного разбирательства либо в регламент арбитражного института, придавая им тем самым обязательную силу в силу принципа свободы договора, закреплённого гражданским законодательством Республики Узбекистан. Такой подход не требует изменения законодательства и может быть реализован уже в настоящее время постоянно действующими арбитражными учреждениями, функционирующими на территории республики.

Второй канал – нормотворческий. Он предполагает прямое закрепление в Законе «О международном коммерческом арбитраже» [2] отсылочной нормы, допускающей применение международно признанных стандартов кибербезопасности в качестве ориентира при определении разумных мер защиты информации, а также установление обязанности постоянно действующих арбитражных учреждений разрабатывать собственные регламенты кибербезопасности с учётом международной практики. Подобный подход обеспечивает гибкость регулирования, свойственную самим протоколам, избегая при этом излишней технической детализации на уровне закона.

Третий канал – судебный (правоприменительный). Международные протоколы способны выступать источником толкования оценочных понятий гражданского законодательства, таких как «разумность», «добросовестность» и «должная осмотрительность», при разрешении споров о возмещении вреда, причинённого нарушением кибербезопасности в ходе арбитражного разбирательства. Использование содержания международных протоколов в качестве ориентира при толковании норм главы 57 Гражданского кодекса Республики Узбекистан [1] не требует изменения законодательства, однако предполагает соответствующую правоприменительную практику и повышение осведомлённости судейского корпуса.

Сравнительно-правовой аспект. Международная практика демонстрирует различные модели интеграции протоколов кибербезопасности в регулирование арбитража. Гонконгский

международный арбитражный центр включил в свой регламент 2018 года положения, прямо признающие загрузку документов в согласованное сторонами защищённое хранилище надлежащим способом коммуникации между участниками разбирательства. Лондонский международный третейский суд в редакции регламента 2020 года прямо предусмотрел обязанность состава арбитража на раннем этапе разбирательства рассмотреть вопрос о принятии специальных мер информационной безопасности и мер по защите персональных данных [12, С.1]. Данные примеры свидетельствуют о том, что институциональная модель рецепции, то есть закрепление требований кибербезопасности на уровне регламентов арбитражных институтов, а не непосредственно в законе, получает всё более широкое распространение и представляется совместимой с традицией диспозитивного регулирования, свойственной международному коммерческому арбитражу.

Для Республики Узбекистан, законодательство которой в сфере международного коммерческого арбитража ориентировано на Типовой закон ЮНСИТРАЛ о международном торговом арбитраже [13], наиболее целесообразной представляется комбинированная модель, сочетающая точечное законодательное закрепление общих принципов (обязанность обеспечения конфиденциальности и информационной безопасности, распределение ответственности между участниками разбирательства) с делегированием детализации на уровень регламентов постоянно действующих арбитражных учреждений и договорной практики, что соответствует и подходу, заложенному в самом Протоколе ICCA- Нью-Йоркская коллегия адвокатов - CPR, отвергающем единый обязательный технический стандарт [9].

Предложения по совершенствованию законодательства Республики Узбекистан. По итогам проведённого анализа представляется целесообразным сформулировать следующие предложения.

Во-первых, дополнить Закон «О международном коммерческом арбитраже» [2] нормой о праве состава арбитража и сторон согласовывать применение международно признанных стандартов информационной безопасности, включая Протокол ICCA – Нью-Йоркская коллегия адвокатов – CPR и Руководство IBA по кибербезопасности, в качестве ориентира при определении разумных мер защиты информации в конкретном деле.

Во-вторых, закрепить в подзаконных актах, принимаемых во исполнение Закона «О кибербезопасности» [3], требование к постоянно действующим арбитражным учреждениям и обслуживающим их информационным платформам о разработке собственных регламентов кибербезопасности с

учётом международной практики и об уведомлении сторон разбирательства о применяемых мерах защиты информации.

В-третьих, дополнить главу 57 Гражданского кодекса Республики Узбекистан [1] либо принять соответствующее разъяснение высшей судебной инстанции о возможности использования международно признанных протоколов кибербезопасности в качестве критерия оценки разумности и добросовестности поведения оператора информационной системы при разрешении споров о возмещении вреда, причинённого нарушением кибербезопасности в ходе арбитражного разбирательства.

В-четвёртых, предусмотреть в Законе «О персональных данных» [4] специальную норму о том, что арбитражный институт и обслуживающая его технологическая платформа выступают совместными операторами персональных данных, обрабатываемых в ходе разбирательства, с распределением ответственности по аналогии с подходами, заложенными в дорожной карте по защите данных, разработанной ICCA и IBA.

В-пятых, рекомендовать постоянно действующим арбитражным учреждениям Республики Узбекистан включать в свои регламенты и типовые договоры с технологическими платформами положения об обязательном применении Протокола ICCA - Нью-Йоркская коллегия адвокатов - CPR либо эквивалентных стандартов, что позволит уже в краткосрочной перспективе, не дожидаясь законодательных изменений, повысить уровень защищённости арбитражных разбирательств и укрепить доверие иностранных участников оборота к национальной арбитражной инфраструктуре.

Заключение. Проведённое исследование показывает, что Протокол ICCA – Нью-Йоркская коллегия адвокатов - CPR и Руководство IBA по кибербезопасности, не обладая формальной юридической силой, образуют развитую систему рекомендательных стандартов, оказывающих реальное влияние на формирование практики должной осмотрительности в международном коммерческом арбитраже. Действующее законодательство Республики Узбекистан содержит отдельные нормативные элементы, функционально созвучные положениям указанных протоколов, однако не обеспечивает их системной привязки к арбитражному разбирательству. Гражданско-правовая рецепция соответствующих международных подходов возможна по трём взаимодополняющим каналам договорному, нормотворческому и правоприменительному и должна осуществляться с учётом гибкой, риск-ориентированной методологии, заложенной в самих международных протоколах. Реализация предложенных мер будет способствовать повышению конкурентоспособности Республики Узбекистан как площадки для проведения международного коммерческого арбитража и приведению национального

регулирования в соответствие с современными международными стандартами информационной безопасности.

Список литературы:

1. Гражданский кодекс Республики Узбекистан (часть первая утверждена Законом РУз от 21 декабря 1995 года № 163-I, часть вторая – Законом РУз от 29 августа 1996 года № 256-I; с изм. и доп. по состоянию на 25 декабря 2025 года). https://lex.uz/acts/111181 (Civil Code of the Republic of Uzbekistan, Part One approved by Law No. 163-I of 21 December 1995, Part Two by Law No. 256-I of 29 August 1996, with amendments as of 25 December 2025.)

2. Закон Республики Узбекистан «О международном коммерческом арбитраже» от 16 февраля 2021 года № ЗРУ-674. https://lex.uz/docs/5294087 (Law of the Republic of Uzbekistan «On International Commercial Arbitration» No. ZRU-674 of 16 February 2021.)

3. Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764. https://lex.uz/docs/6997403 (Law of the Republic of Uzbekistan «On Cybersecurity» No. ZRU-764 of 15 April 2022.)

4. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547 (с изм. и доп., в том числе от 26 марта 2026 года № ЗРУ-1125). https://lex.uz/docs/4396428 (Law of the Republic of Uzbekistan «On Personal Data» No. ZRU-547 of 2 July 2019, with amendments including ZRU-1125 of 26 March 2026.)

5. Постановление Кабинета Министров Республики Узбекистан «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных» от 5 октября 2022 года № 570. https://lex.uz/docs/6225469 (Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 570 of 5 October 2022 «On the Approval of Certain Regulatory Legal Acts in the Field of Personal Data Processing».)

6. Закон Республики Узбекистан «Об электронной цифровой подписи» от 12 октября 2022 года № ЗРУ-793 (вступил в силу 14 января 2023 года). https://lex.uz/docs/6234906 (Law of the Republic of Uzbekistan «On Electronic Digital Signature» No. ZRU-793 of 12 October 2022, entered into force 14 January 2023.)

7. Постановление Президента Республики Узбекистан «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» от 31 мая 2023 года № ПП-167. https://lex.uz/docs/6479197 (Presidential Decree of the Republic of Uzbekistan No. PP-167 of 31 May 2023 «On Additional Measures to Improve the Cybersecurity System for Critical Information Infrastructure Facilities of the Republic of Uzbekistan».)

8. Постановление Президента Республики Узбекистан «О мерах, направленных на дальнейшее усиление деятельности

по борьбе с преступлениями, совершаемыми с помощью информационных технологий» от 30 апреля 2025 года № ПП-153. https://lex.uz/docs/7511168 (Presidential Decree of the Republic of Uzbekistan No. PP-153 of 30 April 2025 «On Measures Aimed at Further Strengthening Activities to Combat Crimes Committed Using Information Technologies».)

9. ICCA, New York City Bar Association, CPR Dispute Resolution Services. Protocol on Cybersecurity in International Arbitration (2022 Edition). https://cdn.arbitration-icca.org/s3fs-public/document/media_document/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_print_version.pdf (ICCA, New York City Bar Association, CPR Dispute Resolution Services. Protocol on Cybersecurity in International Arbitration (2022 Edition).)

10. International Bar Association. IBA Rules on the Taking of Evidence in International Arbitration (2020 revision), Article 2.2(e). https://www.ibanet.org (International Bar Association. IBA Rules on the Taking of Evidence in International Arbitration (2020 revision), Article 2.2(e).)

11. International Bar Association. IBA Cybersecurity Guidelines. London: IBA, 2018. https://www.ibanet.org/LPRU/Cybersecurity (International Bar Association. IBA Cybersecurity Guidelines. London: IBA, 2018.)

12. Abdul Rahman D.S. The Role of Arbitral Institutions in Cybersecurity and Data Protection in International Arbitration. Kluwer Arbitration Blog, 24 November 2020. https://legalblogs.wolterskluwer.com/arbitration-blog/the-role-of-arbitral-institutions-in-cybersecurity-and-data-protection-in-international-arbitration/ (Abdul Rahman D.S. The Role of Arbitral Institutions in Cybersecurity and Data Protection in International Arbitration. Kluwer Arbitration Blog, 24 November 2020.)

13. UNCITRAL Model Law on International Commercial Arbitration (1985), with amendments as adopted in 2006. New York: United Nations, 2008. (UNCITRAL Model Law on International Commercial Arbitration (1985), with amendments as adopted in 2006. New York: United Nations, 2008.)

14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union, L 119/1. (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119/1.)