



**Генеральная Ассамблея**

Distr.: General  
 14 June 2022  
 Russian  
 Original: English/Spanish

**Комиссия Организации Объединенных Наций**

**по праву международной торговли**

**Пятьдесят пятая сессия**

Нью-Йорк, 27 июня — 15 июля 2022 года

**Проект типового закона об использовании  
 и трансграничном признании управления  
 идентификационными данными и удостоверительных  
 услуг**

**Подборка замечаний правительств и международных  
 организаций**

Содержание

	<i>Стр.</i>
II. Подборка замечаний .....	2
F. Ассоциация банкиров по финансам и торговле .....	2
G. Многонациональное Государство Боливия .....	4
H. Исламская Республика Иран .....	5
I. Болгария .....	10
J. Сингапур .....	10



## II. Подборка замечаний

### F. Ассоциация банкиров по финансам и торговле

[Подлинный текст на английском языке]  
[27 мая 2022 года]

1. Ассоциация банкиров по финансам и торговле (АБФТ) выражает признательность за возможность представить замечания по проекту типового закона об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг.
2. АБФТ — международная ассоциация отрасли финансовых услуг, членами которой являются различные финансовые и ФинТех структуры по всему миру. АБФТ служит международной площадкой для анализа, обсуждения и информационно-просветительской работы в сфере международных финансовых услуг; почти 300 членов Ассоциации играют инициативную роль в выработке единой позиции в целях обеспечения безопасного и эффективного функционирования мировой финансовой системы. Члены АБФТ считают цифровизацию финансирования международной торговли ключевым приоритетом для отрасли, а управление идентификационными данными (УИД) является принципиально важным элементом для продвижения этого процесса вперед.
3. Развитие УИД необходимо для многих аспектов банковского обслуживания международных операций, включая финансирование торговли, финансирование производственно-сбытовых цепей и проведение платежей, а также для таких областей соблюдения нормативных требований, как «Знай своего клиента» (ЗСК) и «Борьба с отмыванием денег» (БОД). В этой связи АБФТ полностью одобряет усилия ЮНСИТРАЛ по разработке проекта типового закона.
4. В сфере глобального транзакционного бизнеса существует несколько направлений деятельности, целью которых является создание полностью цифровой экосистемы для этого бизнеса. Цифровизация открывает большие перспективы. Однако ее темпы на сегодняшний день нельзя назвать удовлетворительными. Очевидно, что она не произойдет резко, как «Большой взрыв», но будет внедряться поступательно, посредством взаимодополняющих инициатив.
5. Для перехода на цифровые технологии в повседневной деятельности участники рынка нуждаются в четких правилах. В этой связи Международная торговая палата, Азиатский банк развития и правительство Сингапура разработали Инициативу по цифровым стандартам (ИЦС)<sup>1</sup>, которая призвана способствовать решению вопросов, связанных со стандартами и функциональной совместимостью платформ, а также развивать отношения со сферой ФинТех. Что касается правовой поддержки, то в рамках ИЦС была разработана дорожная карта для принятия мер, стимулирующих правительства к введению в действие конкретных законодательных норм для регулирования цифрового бизнеса в соответствии с Типовым законом ЮНСИТРАЛ об электронных передаваемых записях<sup>2</sup> (ТЗЭПЗ). АБФТ участвует в работе по принятию ТЗЭПЗ в странах по всему миру. Помимо разработки нормативно-правовой базы представители отрасли работают над стандартами для обеспечения функциональной совместимости. В августе 2020 года АБФТ опубликовала документ «Передовая отраслевая практика в области обработки платежных обязательств на основе технологии распределенного реестра»<sup>3</sup>, который представляет собой отраслевое руководство по обработке совместимых платежных обязательств на основе технологии распределенного реестра.

<sup>1</sup> ICC Digital Standards Initiative, March 2020.

<sup>2</sup> Типовой закон ЮНСИТРАЛ об электронных передаваемых записях (ТЗЭПЗ), июль 2017 года.

<sup>3</sup> BAFT: DLPC May 2020.

6. Проект типового закона в его нынешнем виде обеспечивает общую основу для управления идентификационными данными и предоставления удостоверительных услуг; при этом в нем намеренно не дается даже минимальных предписаний. В нем четко сказано: «Как и ранее принятые тексты ЮНСИТРАЛ, проект типового закона основан на принципах автономии сторон, технологической нейтральности, функциональной эквивалентности и недискриминации в отношении использования электронных средств, с учетом корректировок. Принцип автономии сторон позволяет сторонам договора выбирать применимые правила в пределах, установленных императивными нормами права. Он основан на признании того факта, что именно стороны договора могут наилучшим образом определить наиболее подходящие правила для конкретной сделки».

7. Проект типового закона предполагает, что к услугам по управлению идентификационными данными будут предъявляться требования по надежности, как это предусмотрено статьей 10, однако в нем не прописано, как именно следует подходить к разработке «системы уровней доверия». Проект типового закона подтверждает, что международный аспект принципиально важен для использования услуг УИД и удостоверительных услуг, а также, в более общем плане, электронных услуг. Однако в тексте признается существование двух препятствий: i) технической несовместимости, ведущей к отсутствию функциональной совместимости; ii) юридических барьеров для трансграничного признания.

8. Для преодоления этих двух препятствий АБФТ предлагает включить в проект типового закона прямую ссылку на значительный объем работы, проделанный Всемирным фондом для юридического идентификатора (ВФЮИ)<sup>4</sup> по созданию электронного юридического идентификатора (ЭЮИ). Всемирная система юридических идентификаторов — это одобренная регулирующими органами система, которая обеспечивает признанный на глобальном уровне и пользующийся доверием электронный механизм идентификации юридических лиц. Идентификатор юридического лица (ИЮЛ) — это глобальный стандарт (ISO 17442), объединяющий основные данные, которые позволяют четко и однозначно идентифицировать юридическое лицо. Некоммерческий фонд ВФЮИ был учрежден в 2011 году в Швейцарии Советом по финансовой стабильности по рекомендации Группы двадцати. Его деятельность контролируют 65 регулирующих органов и 19 наблюдателей из более чем 50 стран, которые входят в Комитет по надзору и регулированию.

9. Общедоступный массив данных ИЮЛ можно рассматривать как глобальный справочный ресурс, который значительно повышает прозрачность на мировом рынке. ИЮЛ является разноплановым общественным благом, которое следует использовать для обеспечения технической совместимости на национальном и международном уровне.

10. Проект типового закона направлен на унификацию правил посредством законодательной работы. Такой подход приведет к появлению множества национальных технических стандартов, параллельное существование которых будет означать отсутствие функциональной совместимости и отвлечение ресурсов на обработку разнородных данных. Использование разнообразных идентификаторов и лежащих в их основе национальных технических стандартов затруднит надежную, последовательную и сопоставимую идентификацию сторон в электронных транзакциях. Таким образом, несмотря на то, что ЮНСИТРАЛ желает избежать каких-либо технологических предпочтений и сохранить нейтральный подход, Комиссии, возможно, следует рассмотреть возможность включения ИЮЛ в проект текста в качестве базового идентификатора для облегчения идентификации и проверки юридических лиц при трансграничных операциях. Глобальная система ИЮЛ — не технология, которую можно выбрать. Это общественное благо, предложенное Группой двадцати и созданное Советом по финансовой стабильности (СФС).

<sup>4</sup> GLEIF ([www.gleif.org](http://www.gleif.org)).

11. Учитывая, что справочные данные ИЮЛ уже включают местный регистрационный номер лица, адрес, время последнего обновления данных, а также информацию о том, какие поля данных были актуализированы, они могут способствовать обеспечению единообразия данных об организациях в глобальном масштабе.

12. В тексте проекта типового закона уже признается, что единообразные нормы могут повысить эффективность путем содействия принятию результатов использования УИД и удостоверительных услуг в разных системах; снизить операционные издержки путем упрощения задачи соблюдения нормативных требований; повысить правовую предсказуемость и определенность в отношении электронных сделок на основе единого подхода к рассмотрению вопросов, в том числе с помощью механизмов трансграничного признания; и способствовать преодолению отставания в сфере цифровых технологий за счет повышения доступности общих решений.

13. В случае если подходы будут различаться, статья 27 предусматривает, что совместными усилиями можно согласовать общие определения технических стандартов, включая уровни доверия и уровни надежности. Однако разнонаправленные национальные интересы могут привести к возникновению задержек, а в худшем случае помешать достижению соглашения о необходимых технических стандартах и других основополагающих принципах обеспечения качества данных. Если ЮНСИТРАЛ поддержит ИЮЛ в качестве основного сервиса для идентификации юридических лиц, это позволит ускорить процесс внедрения трансграничной электронной идентификации и задействовать систему, которая была создана регулирующими органами для устранения недостатков национальных/региональных/частных механизмов идентификации. ИЮЛ — проверенная и отлаженная система, которая обеспечивает совместимость и техническую нейтральность.

14. Цифровая трансформация в глобальном транзакционном банковском бизнесе позволяет снизить затраты, повысить эффективность и улучшить регуляторный контроль, в то же время обеспечивая снижение риска и расширяя возможности для сотрудничества между заинтересованными сторонами в глобальной экономике. Разработка и адаптация систем УИД является важнейшим первым шагом в процессе цифровизации. ИЮЛ является единственным глобальным стандартом идентификации юридических лиц, поэтому АБФТ выступает за его включение в текст проекта типового закона.

## **G. Многонациональное Государство Боливия**

[Подлинный текст на испанском языке]

[27 мая 2022 года]

Следующие комментарии и замечания по проекту типового закона представлены Управлением по регулированию телекоммуникаций и транспорта Многонационального Государства Боливия.

*Статья 6. Обязанности поставщиков услуг по управлению идентификационными данными*

Комментарий/замечание:

Рекомендуется считать обязательством обеспечение доступности в онлайн-режиме и корректной работы системы проверки электронных идентификационных данных или электронной подписи, которая позволяет удостоверить личность подписавшего лица и действительность всей последовательности действий уполномоченного удостоверяющего органа в стране происхождения.

### *Статья 16. Электронные подписи*

Комментарий/замечание:

Рекомендуется рассмотреть вопрос о создании механизма для обнаружения любых изменений, внесенных в сообщение данных, и обеспечения его подлинности и целостности, а также невозможности отказа пользователей системы от своих действий.

### *Статья 17. Электронные печати*

Комментарий/замечание:

Подлинность и целостность сообщения данных, невозможность отказа от связанных с ним действий, а также его юридическая и доказательная сила должны обеспечиваться в соответствии с законодательством страны, в которой находится поставщик услуг по управлению идентификационными данными.

## **Н. Исламская Республика Иран**

[Подлинный текст на английском языке]  
[30 мая 2022 года]

### **1. Сфера применения**

#### **Использование и трансграничное признание управления идентификационными данными и достоверительных услуг**

1. **Проблема:** перед ЮНСИТРАЛ поставлены задачи по согласованию и модернизации права международной торговли, а перед Рабочей группой IV — по устранению барьеров, затрудняющих международную электронную торговлю, и в этом контексте Исламская Республика Иран считает, что сфера применения типового закона чрезмерно широка и должна быть ограничена только международным взаимодействием и обстоятельствами, включающими иностранный элемент. Иными словами, мы исходим из того, что в случаях, когда услуги УИД и достоверительные услуги используются внутри одной страны, и все участники соответствующих процессов также находятся в одной и той же стране, и какие бы то ни было иностранные элементы отсутствуют, такие вопросы должны регулироваться национальным законодательством этой страны.

#### **Предлагаемое решение**

2. Рекомендуется ограничить сферу применения типового закона трансграничным использованием и признанием услуг УИД и достоверительных услуг и прояснить, что данный документ не ставит целью вмешательство в созданные в государствах-членах национальные структуры, связанные с УИД и достоверительными услугами, и не будет превалировать над национальным законодательством, регулирующим внутренние дела стран. В то же время отмечаем, что у принимающих типовой закон юрисдикционных систем может оставаться возможность распространить действие этого документа на внутренние дела государства, но только если они этого пожелают.

#### **Услуги, связанные с торговлей**

3. **Проблема:** что касается термина «услуги, связанные с торговлей» в статье 2, полагаем, что, несмотря на разъяснение в пункте 95 пояснительной записки, этот термин все еще слишком расплывчат и может толковаться шире, чем предусмотрено в типовом законе, а также может ошибочно охватывать все работающие в стране системы в области УИД и достоверительных услуг, в том числе не связанные с торговлей.

### Предлагаемое решение

4. В типовом законе рекомендуется сосредоточиться на ситуациях, возникающих в коммерческой деятельности. Тем не менее, в пояснительной записке можно уточнить, что «ничто в типовом законе не препятствует принимающему государству распространить его применение, чтобы охватить использование и трансграничное признание УИД и удостоверительных услуг в контексте услуг, связанных с торговлей».

## 2. Защита суверенитета и публичного порядка государств

5. **Проблема:** наша делегация выражает обеспокоенность в связи с имплицитными последствиями этого типового закона для суверенитета государств, чьи граждане или предприятия являются пользователями трансграничных услуг УИД и удостоверительных услуг. Чтобы лучше понять нашу озабоченность, предлагаем взглянуть на реалии рынка с точки зрения развивающихся стран: во всех соответствующих отраслях таких стран доминируют глобальные цифровые корпорации из нескольких лидирующих в этой области стран, которые предоставляют свои услуги пользователям по всему миру. Кроме того, привлечение поставщиков цифровых услуг к оказанию услуг по управлению идентификационными данными, если ранее правительство не поручало им эту задачу, и особенно если собираемые ими атрибуты тесно связаны с базовой идентификацией личности, не только может быть нерациональным и привести к недостоверным результатам, но и в силу исключительной компетенции государств в отношении управления идентификационными данными своих граждан на протяжении всего жизненного цикла может привести к вмешательству в их суверенные функции. Это также чревато потерей данных, технологий и цифрового суверенитета развивающихся стран, а также потерей защиты, предоставляемой гражданам императивными законодательными нормами. Пагубные последствия такой практики станут еще более очевидными, если учесть подчиненное положение развивающихся стран и мощное давление, которому они подвергаются на глобальных торговых площадках с целью заставить их принять модель глобальной цифровой экономики, навязываемую горсткой стран, в которых сосредоточено большинство гигантских цифровых корпораций. С учетом сказанного Исламская Республика Иран твердо убеждена, что если развивающиеся страны хотят извлечь пользу из работы международных организаций, то сначала они должны быть в состоянии защитить свой суверенитет и публичный порядок. В этом контексте мы считаем, что в положениях типового закона об использовании и трансграничном признании УИД и удостоверительных услуг не хватает четких формулировок относительно защиты суверенитета государств, равенства и невмешательства в вопросы, которые относятся исключительно к их внутренней юрисдикции.

6. Не менее важным является сохранение публичного порядка принимающих закон государств. В настоящее время трансграничные потоки данных и доступ иностранных поставщиков услуг к данным граждан и предприятий других стран становятся одной из основных проблем публичного порядка многих развивающихся государств. В отличие от предыдущих текстов ЮНСИТРАЛ (например, статей 6, 7, 8, 11, 12, 15 и 17 Типового закона об электронной торговле), в данном типовом законе не предусмотрена процедура ограничения сферы действия документа или действия любой из его статей, если это необходимо, в частности, с учетом публичного порядка принимающих его государств. Поскольку применение данного типового закона может быть связано с различными аспектами публичного порядка, которые должны быть оставлены на усмотрение каждого отдельного государства, следует предусмотреть определенную степень гибкости, позволяющую судам принимающего типовой закон государства или органам, ответственным за его применение, отказывать ему в юридической силе или аннулировать правовые последствия, возникающие в результате использования иностранных услуг УИД или удостоверительных услуг, на основании ряда обязательных причин, включая публичный порядок.

### Предлагаемые решения

7. В тексте следует четко указать, что типовой закон должен применяться с соблюдением принципов суверенитета государств, равенства и невмешательства в их внутренние дела. Кроме того, данный документ не должен наделять иностранных поставщиков услуг УИД и удостоверительных услуг полномочиями по выполнению функций, которые относятся к национальному суверенитету и находятся исключительно в компетенции государств в соответствии с их внутренним законодательством. Желательно, чтобы это было прописано в разделе F пояснительной записки в качестве общего принципа и ключевой концепции.

8. Чтобы учесть озабоченность, связанную с публичным порядком, и поддержать позицию, последовательно занимаемую ЮНСИТРАЛ в ее документах, считаем целесообразным рассмотреть следующие три варианта.

Первый: включить в типовой закон положения, которые позволят принимающим его юрисдикционным системам исключить применение или действие определенных статей этого документа в ситуациях, когда это противоречит их публичному порядку (в ряде предыдущих текстов ЮНСИТРАЛ такие положения присутствуют).

Второй: допустить определенную гибкость в формулировках некоторых статей, убрав категоричность относительно сферы их применения. Например, добавить в формулировку подпункта 3 статей 10 и 22 следующие слова: «при определении надежности этого метода, если только судебный орган не сочтет необходимым иное, не принимаются во внимание...». В этом же ключе подпункт 4 статей 11 и 23 может быть изменен следующим образом: «при назначении услуги по управлению идентификационными данными / удостоверительной услуги, если только [лицо, орган или ведомство, будь то публичное или частное, указанное принимающей юрисдикционной системой в качестве компетентного] не сочтет необходимым иное, не принимаются во внимание...». Кроме того, замена в тексте на английском языке “shall” на “may” в статьях 25 и 26 не только сделает их формулировки более гибкими с учетом озабоченности по поводу публичного порядка, но и в свете отсутствия ясности относительно признанных международных стандартов в статьях 25(2) и 26(2), представляется логичной.

Третий: если два вышеупомянутых варианта невозможны, было бы полезно предусмотреть в типовом законе в качестве общего правила исключение на основании публичного порядка и оставить частности на усмотрение каждой принимающей юрисдикционной системы.

### 3. Приоритет императивных правовых норм

9. **Проблема:** в настоящее время поставщики услуг УИД/удостоверительных услуг предлагают их гражданам и предприятиям, находящимся в других государствах. Хотя такое положение дел неизбежно и нормально в условиях глобальной электронной торговли, следует принять меры предосторожности для обеспечения соблюдения поставщиками услуг соответствующих приоритетных правовых норм, отступление от которых не допускается.

10. Исламская Республика Иран осознает тот факт, что данный документ не влияет на применение любого обязательного закона в контексте его положений, а также учитывает, что типовой закон не вмешивается в действие норм международного частного права. Тем не менее, мы твердо убеждены, что в проект документа необходимо включить конкретное положение, наделяющее приоритетом императивные правовые нормы страны, в которой услуги УИД или удостоверительные услуги предоставляются или используются. Для такого подхода есть несколько причин. Первая причина связана с доступом поставщиков услуг к данным граждан, предприятий и организаций рассматриваемой страны. Принимая во внимание, что данные являются ценным ресурсом, который в случае экстерриториального оказания услуг может попасть в руки иностранных поставщиков, мы считаем, что владельцы данных будут в лучшем положении, если в

отношении данных будет действовать режим защиты и императивные правовые нормы страны, где услуга предоставляется или используется. Вторая причина связана с отсутствием в международном частном праве четкой нормы, которая бы определяла применимое право и императивные правила защиты пользователей услуг электронной торговли. Хотя, как представляется, существует общий консенсус относительно применимого законодательства для защиты потребителей в потребительских договорах, может возникнуть двусмысленность в отношении защиты пользователей в договорах с поставщиками цифровых услуг, которые могут не подпадать под действие закона о защите прав потребителей. Третья причина — неравенство пользователей и поставщиков услуг согласно условиям договоров. Пользователи часто находятся в невыгодном положении, когда речь идет о заключении договора в цифровой среде и согласии с операционными правилами, политикой и практикой. По нашему мнению, условия договоров между пользователями и поставщиками услуг в большинстве случаев не являются предметом переговоров и обычно содержат положения о применимом праве или выборе суда, которые более благоприятны для поставщиков услуг и невыгодны пользователям. Отсутствие в типовом законе какой-либо ссылки на применение законодательства страны, в которой услуга предоставляется или используется, оставит пользователей без необходимой защиты, на которую они имеют право.

### **Предлагаемые решения**

11. Поиск адекватных гарантий и решений для реагирования на вышеупомянутые проблемы требует более широкого международного сотрудничества и политического диалога при активном участии развивающихся стран, которые в большинстве случаев являются получателями трансграничных услуг. Тем не менее, хотели бы предложить следующее.

- «Соответствие операционных правил, политики и практики поставщика услуг УИД / удостоверительных услуг императивным правовым нормам территории, на которой услуга предоставляется или используется» должно быть обязательством поставщиков таких услуг в статьях 6 и 14, а также аспектом, который необходимо учитывать как при определении надежности метода (*ex post*) в статьях 10(2) и 22(2), так и при назначении надежных услуг (*ex ante*) в статьях 11(2)(а) и 23(2)(а), а также должно в обычном порядке применяться для придания юридической силы при трансграничном оказании услуг в статьях 25 и 26.
- С целью придания силы императивным правовым нормам территории, где услуга предоставляется или используется, возникнет необходимость в наложении дополнительных обязательств на поставщиков услуг в статьях 6 и 14, что может быть более подробно изложено в пунктах 113 и 175 пояснительной записки. Например, сотрудничество поставщиков услуг с правоохранительными органами страны, в которой предоставляется или используется услуга (например, в вопросах защиты данных или в ситуациях, которые могут привести к деликтной или уголовной ответственности, включая предупреждение, расследование, выявление преступлений и уголовное преследование виновных) и, с этой целью, открытие представительства или назначение представителя в этой стране, изменение условий предоставления услуг и политики поставщиков услуг в соответствии с императивными правовыми нормами в месте предоставления или использования услуг и т. д. Мы считаем, что нарушение этих обязательств должно служить основанием для привлечения к ответственности поставщиков услуг УИД / удостоверительных услуг согласно статьям 12 и 24.
- Выполнение вышеупомянутых обязательств может способствовать достижению цели взаимного признания, предусмотренной в статьях 25 и 26. Поэтому было бы крайне желательно, чтобы принимающие типовой закон юрисдикционные системы предоставили информацию о своих императивных правовых нормах в рамках обмена информацией, предусмотренного в

статье 27. Такая информация дала бы возможность иностранным поставщикам услуг, которые хотят предлагать свои услуги экстерриториально, заранее внести изменения в условия и политику предоставления услуг с учетом соответствующих нормативных актов. Более подробно условия такого сотрудничества могут быть изложены в пункте 234 пояснительной записки.

#### 4. Добровольное использование услуг УИД и удостоверительных услуг

12. **Проблема:** Исламская Республика Иран выражает озабоченность в отношении статьи 3(2) типового закона, которая гласит, что вывод о согласии лица может быть сделан на основании его поведения. Хотя в предыдущих текстах ЮНСИТРАЛ такое правило использовалось, мы убеждены, что это несправедливо по отношению к людям, плохо разбирающимся в технологиях, которые могут и не знать о том, что, подписываясь на услугу или используя определенное программное обеспечение для электронной торговли, они разрешают использовать услугу УИД или удостоверительную услугу, используемую этим программным обеспечением. Более того, такое положение дел может привести к дальнейшим негативным последствиям, поскольку поставщики услуг обычно обращаются с пользователями по принципу «бери что дают», а последние часто дают согласие на заключение цифровых контрактов «вслепую», не ознакомившись с предлагаемыми условиями, хотя в них могут быть прописаны ситуации, в которых пользователь может считаться выразившим согласие на те или иные действия. Мы хотели бы обратить внимание Комиссии на тот факт, что хотя европейские потребители защищены от несправедливых стандартных условий договора в силу Директивы о несправедливых условиях в договорах с потребителями (93/13/ЕЕС), нам кажется, что в странах других регионов проработанных законодательных норм по этому вопросу нет.

#### Предлагаемое решение

13. Хотели бы предложить некоторую гибкость в отношении вывода о согласии лица на использование услуги УИД/удостоверительной услуги по его поведению и подчеркнуть, что такое подразумеваемое согласие должно определяться более четким и предсказуемым образом. Соответственно, государствам-членам было бы полезно обсудить этот вопрос более подробно и найти решения, которые позволят более грамотно подойти к выполнению этого требования применительно к договорам в цифровой среде. Полагаем, что подразумеваемое согласие сторон могло бы иметь форму презумпции с возможностью отозвать его на более поздней стадии.

#### 5. Электронное архивирование

14. **Проблема:** мы помним о том, что типовым законом не затрагивает законодательство, регулирующее конфиденциальность и защиту данных. Тем не менее, поскольку эта область права имеет самое непосредственное отношение к электронному архивированию, мы считаем, что в статье 19 необходимо подчеркнуть, что при электронном архивировании необходимо соблюдать императивные правовые нормы в отношении конфиденциальности и защиты данных. Что касается императивных правовых норм, действующих в этой сфере, то следует обратить внимание на функции трансграничных поставщиков услуг УИД/удостоверительных услуг и важность для них данных граждан, предприятий и организаций других стран. В свете того, что передача таких данных через границы представляет собой серьезную проблему уровня государственной политики и может лишить пользователей защиты данных, на которую они имеют право, мы считаем, что в данном типовом законе должно быть предусмотрено придание юридической силы закону о защите данных той страны, где услуга предоставляется или используется. Исламская Республика Иран хотела бы привлечь внимание Комиссии к тому факту, что, хотя в Европе субъекты данных защищены Общим регламентом защиты персональных данных Европейского союза, в других странах, особенно в странах третьего мира, могут отсутствовать

аналогичные правовые нормы широкого охвата, которые были бы обязательными для иностранных поставщиков услуг и могли бы принудить их соблюдать закон о защите данных той территории, где предоставляются или используются их услуги.

### **Предлагаемые решения**

15. Четко прописать в статье 19, что «при хранении документов, записей или информации согласно статье 19 должны соблюдаться гарантии, предусмотренные законодательством о конфиденциальности и защите данных». Для решения второй упомянутой выше проблемы мы предлагаем добавить пункт о том, что электронное архивирование не лишает пользователей трансграничных услуг УИД / удостоверительных услуг защиты данных, на которую они имеют право в том месте, где услуга предлагается или используется.

### **6. Добавления**

16. Для того чтобы подготовить более полный во многих отношениях текст, следует рассмотреть вопрос о добавлении в текст типового закона ряда недостающих элементов. Например, можно добавить определения понятий «уровень доверия», «уровень надежности» и «полагающаяся сторона» в статью 1, описать права и обязанности полагающейся стороны, а также более явно и комплексно изложить права пользователей.

## **I. Болгария**

[Подлинный текст на английском языке]  
[8 июня 2022 года]

1. Болгарское национальное законодательство и законодательство Европейского союза (ЕС) об электронной идентификации и удостоверительных (сертификационных) услугах основано на Регламенте № 910/2014 Европейского союза об электронной идентификации и удостоверительных услугах на внутреннем рынке и удостоверительных услугах для электронных операций, отменяющем Директиву ЕС 1999/93. Полномочия Комиссии по регулированию установлены в статье 32 Закона об электронной документации и электронных сертификационных услугах, согласно которой Комиссия является национальным надзорным органом в области электронных сертификационных услуг, ответственным за соблюдение положений указанного Регламента ЕС.

2. Регламент ЕС № 910/2014 устанавливает общую нормативно-правовую основу для использования сертификационных услуг в государствах — членах ЕС, а признание сертификационных услуг, поставщик которых находится в государстве за пределами ЕС, регулируется статьей 14 Регламента. Такие услуги могут признаваться при наличии соответствующего соглашения между ЕС и соответствующим третьим государством или международной организацией в соответствии со статьей 218 Договора о функционировании Европейского союза.

3. Учитывая вышеизложенное, болгарская Комиссия по регулированию считает, что представленный проект типового закона, подготовленный ЮНСИТРАЛ, соответствует основным целям и принципам, изложенным в Регламенте ЕС № 910/2014.

## Ж. Сингапур

[Подлинный текст на английском языке]  
[13 июня 2022 года]

1. Сингапур выражает признательность Рабочей группе IV за работу над проектом типового закона об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг.

2. Мы хотели бы обратить внимание Комиссии на следующие три аспекта проекта Типового закона (документ A/CN.9/1112), которые заслуживают тщательного рассмотрения.

а) Первый касается необходимости:

i) более четкого установления взаимосвязи между статьей 9 и статьей 10(1) (в отношении услуг УИД), включив в статью 9 слова «в соответствии со статьей 10(1)», с тем чтобы соответствующая фраза в статье 9 была сформулирована следующим образом: *«если с этой целью для электронной идентификации лица используется какой-либо метод в соответствии со статьей 10(1)»; и*

ii) более четкого установления взаимосвязи между каждой из статей с 16 по 21 и статьей 22(1) (в отношении удостоверительных услуг) путем включения слов «в соответствии со статьей 22(1)» в каждую из статей с 16 по 21 таким образом, чтобы соответствующие фразы в этих статьях гласили: *«если используется какой-либо метод в соответствии со статьей 22(1)...».*

(Подробнее этот вопрос рассматривается в пп. 3 и 4 ниже.)

б) Второй аспект касается важности сохранения «защитных оговорок», содержащихся в статье 10(1)(b) (в отношении надежности услуг по управлению идентификационными данными) и статье 22(1)(b) (в отношении надежности удостоверительных услуг). Эти защитные оговорки, которые зеркально отражают положения статьи 9(3)(b)(ii) Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах 2007 года (КЭС)<sup>5</sup> и статьи 12(b) Типового закона ЮНСИТРАЛ об электронных передаваемых записях 2017 года (ТЗЭПЗ), направлены на то, чтобы избежать безосновательных юридических претензий (т. е. что использованный метод не был «надежным для цели» *в теории*): они предусматривают, что метод удовлетворяет требованиям статьи 9 или статей 16–21, если имеется фактическое подтверждение того, что он выполнил функцию, описанную в статье 9, или соответствующие функции, описанные в статьях 16–21 (т. е. продемонстрировал *фактическую* надежность), при этом факт выполнения функции может учитываться сам по себе или вместе с дополнительными доказательствами. По нашему мнению, статьи 10(1)(b) и 22(1)(b) служат важнейшими гарантиями против таких безосновательных претензий и должны быть сохранены в прежнем виде. Кроме того, удаление (или перемещение) статей 10(1)(b) и 22(1)(b) приведет к тому, что проект типового закона перестанет соответствовать КЭС и ТЗЭПЗ. В этом случае Комиссии необходимо будет: а) выработать позицию относительно того, какие меры государствам — участникам КЭС и государствам, принявшим ТЗЭПЗ, необходимо принять для устранения такого несоответствия; б) принять решение о том, будет ли Комиссия продолжать рекомендовать КЭС и ТЗЭПЗ (с несовместимыми положениями) государствам, которые рассматривают возможность присоединения к КЭС или введения в действие ТЗЭПЗ. Мы предлагаем внести изменения в пункты 142 и 143 проекта пояснительной записки, чтобы более точно описать цель и действие статьи 10(1)(b) проекта типового закона.

<sup>5</sup> Подобно тому, как статья 10(1) устанавливает требования к надежности метода, используемого для электронной идентификации, статья 9(3)(b) КЭС устанавливает требования к надежности метода, используемого для создания электронной подписи.

(Подробнее этот вопрос рассматривается в пп. 5–16 ниже.)

с) Третий аспект касается фразы «*по меньшей мере эквивалентный уровень надежности*» в статьях 25 и 26. По нашему мнению, требовать точной эквивалентности по надежности в качестве условия для взаимного признания иностранной услуги по управлению идентификационными данными или удостоверительной услуги нецелесообразно. Уровни надежности не могут быть определены с абсолютной точностью, а требование точной эквивалентности неизбежно вызовет трудности практического характера при трансграничном признании. Фраза «*по существу эквивалентный или более высокий уровень надежности*»<sup>6</sup> была бы более уместна в многостороннем контексте.

(Подробнее этот вопрос рассматривается в пп. 17–19 ниже.)

## I. Связь между статьей 9 и статьей 10(1) и связь между статьями 16–21 и статьей 22(1)

3. Структура проекта типового закона имеет следующие особенности.

а) Статья 9 устанавливает правило функциональной эквивалентности для идентификации лица с использованием услуг по управлению идентификационными данными, а статья 10(1) устанавливает требования к надежности, которым должен соответствовать метод идентификации, указанный в статье 9.

б) Аналогичным образом статьи 16–21 устанавливают правила функциональной эквивалентности для электронных подписей (статья 16), электронных печатей (статья 17), электронных отметок времени (статья 18), электронного архивирования (статья 19), услуг электронной регистрации доставки (статья 20) и аутентификации веб-сайтов (статья 21), а статья 22(1) устанавливает требования к надежности, которым должен соответствовать каждый из методов, упомянутых в статьях 16–21.

4. По нашему мнению, связь между статьей 9 и статьей 10(1), а также между каждой из статей 16–21 и статьей 22(1) необходимо сделать более явной путем добавления слов «*в соответствии со статьей 10(1)*» сразу после слов «*какой-либо метод*» в статье 9 и добавления слов «*в соответствии со статьей 22(1)*» сразу после слов «*какой-либо метод*» в каждой из статей с 16 по 21. Это позволит прояснить, что требование соблюдается, если для выполнения функций используется метод в соответствии со статьей 10(1) или статьей 22(1), и таким образом исключить предположения о том, что достаточно *любого* метода. Пересмотренные варианты этих статей приведены в **Дополнении** ниже.

## II. Статьи 10(1)(b) и 22(1)(b)

### A. Предотвращение безосновательных юридических претензий

5. Статья 10(1) проекта типового закона предусматривает следующее.

#### *Статья 10. Требования к надежности удостоверительных услуг*

1. Для целей статьи 9 упомянутый в ней метод:

а) должен быть надежным для цели, для которой используется услуга по управлению идентификационными данными; или

б) должен быть проверенным на практике в части способности выполнять функцию, о которой говорится в статье 9.

6. Статья 22(1) проекта типового закона, которая имеет аналогичную структуру, гласит:

<sup>6</sup> Такая формулировка была рассмотрена на шестьдесят третьей сессии Рабочей группы.

Статья 22. Требования к надежности удостоверительных услуг

1. Для целей статей 16–21 упомянутый в них метод:

- а) должен быть надежным для цели, для которой используется удостоверительная услуга; или
- б) должен быть проверенным на практике в части способности выполнять функции, о которых говорится в соответствующей статье.

7. Защитные оговорки, которые упоминались выше, содержатся в статьях 10(1)(b) и 22(1)(b). Они являются зеркальным отражением статьи 9(3)(b)(ii) КЭС и статьи 12(b) ТЗЭПЗ и служат той же цели: они призваны не допустить предъявление безосновательных юридических претензий в связи с пригодностью метода.

а) Статья 9(3) КЭС, которая содержит правило функциональной эквивалентности для электронных подписей, гласит следующее:

3. В случаях, когда законодательство требует, чтобы сообщение или договор были подписаны стороной, или предусматривает наступление определенных последствий в случае отсутствия подписи, это требование считается выполненным в отношении электронного сообщения, если:

- а) использован какой-либо способ для идентификации этой стороны и указания намерения этой стороны в отношении информации, содержащейся в электронном сообщении; и
- б) использованный способ:
  - i) либо является настолько надежным, насколько это соответствует цели, для которой электронное сообщение было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности;
  - ii) либо, как это фактически продемонстрировано на основании самого способа или с помощью дополнительных доказательств, позволил выполнить функции, описанные в подпункте (а) выше.

Статья 9(3)(b)(ii) КЭС призвана предотвратить безосновательное оспаривание действительности электронной подписи — не потому, что предполагаемый автор подписи не подписывал документ или что подписанный им документ был изменен, а лишь потому, что использованный способ проставления подписи не был настолько надежным, *насколько это соответствует* обстоятельствам (т. е. обеспечить надежность в данных обстоятельствах было в принципе/теории невозможно)<sup>7</sup>. Статья 9(3)(b)(ii) позволяет исключить такие безосновательные

<sup>7</sup> Это подробно объясняется в пункте 164 Пояснительной записки к КЭС (воспроизводится ниже):

«164. Вместе с тем ЮНСИТРАЛ сочла, что Конвенция не должна позволять сторонам ссылаться на “критерий надежности” для отказа от своей подписи в тех случаях, когда могут быть доказаны как действительная личность соответствующей стороны, так и ее фактическое намерение. Требование о том, чтобы электронная подпись была “настолько надежной, насколько это соответствует...” не должно давать суду или какому-либо другому лицу или органу, занимающемуся установлением фактов, основание лишать весь договор юридической силы из-за *недостаточно* надежной электронной подписи, если по поводу идентификации подписавшего лица или факта проставления подписи не возникает никакого спора (т. е. если подлинность электронной подписи сомнению не подвергается). Такой результат был бы особенно неблагоприятным, поскольку в подобном случае сторона сделки, для которой требуется подпись, могла бы попытаться уклониться от выполнения своих обязательств путем отрицания того, что ее подпись (или подпись другой стороны) имеет силу — не потому, что предполагаемый автор подписи не подписывал документ или что подписанный им документ был изменен, а лишь потому, что использованный способ проставления подписи не был *«настолько надежным, насколько это соответствует»* обстоятельствам. Во избежание таких ситуаций в пункте 3(b)(ii) действительной признается подпись, проставленная любым способом — независимо от его надежности в принципе, — если было фактически продемонстрировано, что этот способ позволил

юридические претензии, поскольку предусматривает, что если использованный метод выполнил функции, описанные в статье 9(3)(а), то он является надежным *в действительности*.

б) Статья 12(б) ТЗЭПЗ содержит аналогичную защитную оговорку, которая служит той же цели<sup>8</sup>.

8. Прежде всего следует отметить, что фраза *«настолько надежный, насколько это соответствует обстоятельствам»* используется в статьях 10(1)(а) и 22(1)(а), поскольку *соответствие* надежности метода *обстоятельствам* зависит от цели, для которой используется соответствующая услуга, с учетом всех значимых обстоятельств, в том числе упомянутых в статьях 10(2) и 22(2). Особенно значимым обстоятельством может считаться любое соглашение между сторонами относительно используемого метода. Другими словами, соответствие обстоятельствам надежности метода, используемого в конкретной сделке, зависит от обстоятельств этой сделки, а в статьях 10(1)(а) и 22(1)(а) говорится об относительном, а не абсолютном уровне надежности.

9. Как и статья 9(3)(b)(ii) КЭС и статья 12(б) ТЗЭПЗ, статьи 10(1)(б) и 22(1)(б) проекта типового закона призваны предотвратить безосновательные юридические претензии, ставящие под вопрос соответствие обстоятельствам надежности используемого метода (*надежности в теории*): в них предусматривается, что использованный метод удовлетворяет требованиям статьи 9 или статей 16–21, если имеется фактическое подтверждение того, что он выполнил функцию, описанную в статье 9 (т. е. подтверждение *фактической надежности*), при этом факт выполнения функции может учитываться сам по себе или вместе с дополнительными доказательствами.

10. Исключение статей 10(1)(б) и 22(1)(б) открыло бы возможности для предъявления безосновательных юридических претензий. Считаем это нежелательным.

а) Если исключить из проекта типового закона статью 10(1)(б), оппортунистически настроенные субъекты (например, сторона в сделке с использованием электронной идентификации, желающая уклониться от своих обязательств, либо третья сторона, которая может получить выгоду от признания электронной идентификации недействительной) могут получить стимул для оспаривания действительности проведенной идентификации — не на том основании, что идентификация не проводилась, а на том (недостоверном) основании, что использованный метод электронной идентификации не был *«настолько надежным, насколько это соответствует»* обстоятельствам.

---

идентифицировать подписавшую сторону и указать намерение этой стороны в отношении информации, содержащейся в электронном сообщении».

[Важное выделено жирным шрифтом].

<sup>8</sup> Подробное объяснение содержится в пунктах 136 и 137 Пояснительной записки к ТЗЭПЗ (воспроизводятся ниже):

«136. В подпункте (б) предусматривается “защитительная оговорка” с целью **недопущения необоснованных тяжб путем утверждения методов, которые фактически выполнили свою функцию, независимо от какой бы то ни было оценки их надежности**. Он касается выполнения этой функции в конкретном случае, в отношении которого возник спор, и не преследует цели прогнозирования надежности на основе предыдущих случаев применения этого метода. Это положение может действовать в отношении любой из функций, выполняемых с помощью использования электронных передаваемых записей. Аналогичный механизм предусмотрен в подпункте 3(б)(ii) статьи 9 Конвенции об электронных сообщениях, касающейся функциональной эквивалентности электронных подписей.

137. На практике тот факт, что используемый метод позволил выполнить эту функцию посредством его использования, *будет предотвращать любое обсуждение оценки его надежности согласно подпункту (а)*».

[Важное выделено жирным шрифтом].

б) Аналогичные соображения применимы и в контексте удостоверительных услуг. На примере электронных подписей мы видим, что без статьи 22(1)(b) сторона сделки, в которой использовалась электронная подпись, может попытаться уклониться от своих обязательств, заявив о недействительности ее собственной подписи или подписи контрагента — и не на основании того, что намеревавшееся подписать лицо не поставило свою подпись или что подписанный документ был изменен, а на том (недостоверном) основании, что использованный метод подписи не был *«настолько надежным, насколько это соответствует»* обстоятельствам. Любая третья сторона, заинтересованная в признании сделки недействительной, также может предпринять попытку отменить ее.

11. Можно утверждать, что статей 10(1)(a) и 22(1)(a) самих по себе достаточно, чтобы избежать описанных выше нежелательных событий, потому что суд или какое-либо другое лицо или орган, занимающийся установлением фактов, может отклонить безосновательную юридическую претензию, постановив *ex post*, что метод, использованный в сделке, был *«настолько надежным, насколько это соответствует обстоятельствам»* для цели, для которой использовалась услуга, как указано в статье 9 (идентификация) или статьях 16–21 (удостоверительные услуги). Однако этому подходу присущи две проблемы. Первая заключается в том, что даже если безосновательная юридическая претензия в конечном счете не увенчается успехом, подобные судебные разбирательства не нужны добросовестным участникам электронной торговли. Они нежелательны.

12. Вторая и более важная проблема, связанная с исключением защитных оговорок из статей 10(1)(b) и 22(1)(b), которое подвергает риску безосновательного оспаривания все электронные сделки, осуществляемые в соответствии с внутренним законодательством страны, принявшей типовой закон, в которых используется электронная идентификация (статья 9), электронные подписи (статья 16), электронные печати (статья 17), электронные метки времени (статья 18), электронное архивирование (статья 19), услуги электронной регистрации доставки (статья 20) или аутентификация веб-сайта (статья 21), заключается в том, что такое исключение приводит к возникновению неопределенности в деловых транзакциях, осуществляемых по обоюдному согласию. Приведем показательный пример.

а) Предположим, что в 2023 году (когда типовой закон будет принят в качестве внутреннего законодательства в некоторых юрисдикционных системах) две стороны договорятся подписать контракт с помощью цифровой подписи, использующей алгоритм хеширования SHA2-256, который генерирует 256-битный хеш-код.

б) Факт подписания сторонами контракта не оспаривается. Также никто не заявляет, что контракт был каким-либо образом изменен.

с) Однако без защитной оговорки сторона А (которая, например, теперь хотела бы расторгнуть контракт, подписанный со стороной В, поскольку он оказался для нее невыгоден) может оспорить подлинность цифровых подписей, использованных для подписания контракта, утверждая, что алгоритм хеширования не был *«настолько надежным, насколько это соответствует обстоятельствам»*, поскольку вместо алгоритма SHA2-256, который не является достаточно надежным, следовало использовать SHA3-512.

Создавать возможности для таких манипуляций нежелательно. На наш взгляд, хотя стандарт *«настолько надежный, насколько это соответствует обстоятельствам»* является достаточно гибким, необходимо устранить риск оспаривания в суде на основании несоответствия использованного метода обстоятельствам в теории. С деловой точки зрения нецелесообразно полагаться лишь на формулировку *«настолько надежно, насколько это соответствует обстоятельствам»*. Как предприятия (такие, например, как сторона В в примере выше) могут быть уверены в том, что электронные сделки, которые они заключат в 2023 году, не будут уязвимы для безосновательных юридических претензий в

будущем? Защитные оговорки, содержащиеся в статьях 10(1)(b) и 22(1)(b) проекта типового закона, призваны дать им такую уверенность.

## **В. Приведение проекта типового закона в соответствие с КЭС и ТЗЭПЗ**

13. Сохранение статей 10(1)(b) и 22(1)(b) в прежней форме также позволит обеспечить согласованность проекта типового закона с КЭС — самым современным документом ЮНСИТРАЛ по электронным сделкам. Крайне важно, чтобы проект типового закона не противоречил статье 9(3)(b)(ii) КЭС. Многие государства, в том числе Сингапур, являются участниками КЭС и поэтому не могут принимать законы, противоречащие КЭС. Существуют также государства, которые не являются участниками КЭС, но приняли законодательные акты об электронных сделках на основе КЭС, включая защитную оговорку<sup>9</sup>. Исключение статей 10(1)(b) и 22(1)(b) (особенно статьи 22(1)(b)) приведет к тому, что проект типового закона войдет в противоречие с положениями статьи 9(3)(b)(ii) КЭС. Это также будет предметом озабоченности для будущих государств — участников КЭС.

14. Государства, принявшие или намеревающиеся принять ТЗЭПЗ в качестве национального законодательства, также будут обеспокоены исключением статей 10(1)(b) и 22(1)(b) из проекта типового закона, поскольку в результате проект типового закона перестанет соответствовать ТЗЭПЗ.

15. В случае если статьи 10(1)(b) и 22(1)(b) не будут сохранены в прежней форме, Комиссии необходимо будет а) выработать позицию относительно того, какие меры государствам — участникам КЭС и государствам, принявшим ТЗЭПЗ, необходимо принять для устранения такого несоответствия; б) принять решение о том, будет ли Комиссия продолжать рекомендовать КЭС и ТЗЭПЗ (с несовместимыми положениями) государствам, которые рассматривают возможность присоединения к КЭС или введения в действие ТЗЭПЗ.

## **С. Поправки к проекту пояснительной записки для уточнения цели статей 10(1)(b) и 22(1)(b)**

16. Для обеспечения правильного понимания цели защитной оговорки в статьях 10(1)(b) и 22(1)(b) пункты 142 и 143 проекта пояснительной записки предлагается изложить в следующей редакции:

142. Пункт 1(b) содержит положение, призванное не допустить отказа от услуги УИД, если она фактически выполнила свою функцию. От нее отказываются, когда субъект заявляет о невыполненном ею действии. Для того чтобы предусмотренный в пункте 1(b) механизм действовал, метод, независимо от того, **соответствует ли его надежность обстоятельствам надежный он** или нет, должен фактически выполнить функцию идентификации, т. е. связать требующее идентификации лицо с идентификационными учетными данными. Это положение основано на статье 9(3)(b)(ii) КЭС.

<sup>9</sup> Например, раздел 10(b)(ii) Закона об электронных транзакциях Австралии 1999 года дублирует статью 9(3)(b)(ii) КЭС. Раздел 10(b)(ii) австралийского закона гласит: Если в соответствии с законодательством Содружества требуется подпись лица, то это требование считается выполненным в отношении электронного сообщения, если:

- а) для всех случаев — использован какой-либо способ идентификации этого лица и подтверждения его намерений в отношении передаваемой информации; и
- б) для всех случаев — использованный метод:
  - i) является достаточно надежным для той цели, с которой данное электронное сообщение было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности; либо
  - ii) **как это фактически продемонстрировано на основании самого способа или с помощью дополнительных доказательств, позволило выполнить функции, описанные в пункте (а) выше...**

[Важное выделено жирным шрифтом].

Типовой закон в целом требует избрания надежных методов, и пункт 1(b) не преследует цели способствовать использованию ненадежных методов или признавать законным их использование. Скорее, в нем признается, что с технической точки зрения функция (в случае статьи 9 — идентификация) и надежность являются двумя независимыми атрибутами, и **полагается предусматривается**, что согласно Типовому закону метод должен быть надежным для цели, для которой используется услуга УИД, либо может быть доказано, что с его помощью идентификация была ~~может быть осуществлена~~ фактически ~~или с помощью надежного метода проведена~~. Другими словами, **доказательство достижения цели** идентификации на практике снимает необходимость подтверждения **соответствия** надежности использованного метода **обстоятельствам**.

### III. Статьи 25 и 26

17. Статьи 25 и 26 содержат положения, способствующие трансграничному признанию управления идентификационными данными и удостоверительных услуг соответственно. В качестве условия для взаимного признания электронной идентификации и результата использования удостоверительной услуги, предоставляемой за пределами принимающей юрисдикционной системы, в соответствии с положениями статей 25 и 26 проекта типового закона в настоящее время требуется, чтобы метод, используемый при предоставлении таких услуг, обеспечивал *«по меньшей мере эквивалентный уровень надежности»*.

18. По нашему мнению, устанавливать пороговое значение *«по меньшей мере эквивалентного уровня надежности»* неверно, поскольку такое требование действует только в одном направлении и не может быть выполнено в многостороннем контексте, когда много различных государств принимают один и тот же типовой закон. Кроме того, уровень надежности используемого метода, который зависит от многих юридических, технических и процедурных факторов, определяется с помощью качественных, а не количественных критериев. Это означает, что государству, добивающемуся взаимного признания своих услуг (государство А), будет очень сложно добиться того, чтобы уровень надежности его услуг в точности соответствовал уровню надежности согласно законодательству признающего государства (государство В). Это создает дополнительные проблемы. Предлагаем Комиссии рассмотреть следующий гипотетический сценарий.

а) Предположим, что государство А желает, чтобы его услуга по управлению идентификационными данными с уровнем надежности/доверия «степень 1» была признана в государстве В. Уровень надежности/доверия «степень 1» услуги государства А по существу эквивалентен самому высокому уровню надежности/доверия услуги государства В (уровень «высокий»). Но поскольку законодательство государства В требует, чтобы уровень надежности/доверия услуги, предлагаемой для взаимного признания, был точно таким же или выше, услуга управления идентификационными данными государства А не может быть взаимно признана в государстве В, если только государство А не изменит свои правовые и технические нормы таким образом, чтобы уровень надежности/доверия его услуги «степени 1» был точно таким же или выше, чем уровня «высокий» в государстве В.

б) В результате таких изменений весьма вероятно, что повышенный уровень надежности/доверия услуги «степени 1» государства А будет выше, чем уровень надежности/доверия «высокий» государства В (поскольку надежность нельзя измерить точно, государство А, скорее всего, обеспечит более высокий уровень надежности своей «степени 1», чтобы обеспечить успешное трансграничное признание).

с) В результате внесенных государством А изменений услуга управления идентификацией «степени 1» государства А будет иметь *«уровень надежности, по меньшей мере, эквивалентный»* «высокому» уровню в государстве В, и это позволит признать надежность услуги управления идентификационными

данными «высокой» в государстве В. Однако с другой стороны это означает, что услуга управления идентификационными данными «высокого» уровня надежности/доверия государства В не сможет быть взаимно признана в соответствии с законодательством государства А как эквивалент «степени 1», поскольку «высокий» уровень государства В теперь будет считаться более низким уровнем надежности/доверия по сравнению со «степенью 1» государства А (несмотря на то, что они могут быть по существу эквивалентными).

19. Такое положение дел нежелательно и делает трансграничное признание на взаимной основе практически невозможным. Трансграничное признание на многосторонней основе среди множества юрисдикций станет невыполнимой задачей. В данных обстоятельствах было бы целесообразнее использовать в статьях 25 и 26 формулировку «*по существу эквивалентный или более высокий уровень надежности*». Формулировка «*по существу эквивалентный или более высокий уровень надежности*» позволит осуществлять взаимное трансграничное признание между двумя юрисдикционными системами, не требуя точной эквивалентности. Таким образом, услуги «степени 1» государства А и услуги «высокого уровня» государства В будут подлежать взаимному признанию при условии, что обе услуги имеют по существу эквивалентный уровень надежности/доверия.

## Дополнение

### *Статья 9. Идентификация лица с помощью систем управления идентификационными данными*

С учетом пункта 3 статьи 2 в тех случаях, когда закон требует идентифицировать лицо для конкретной цели или предусматривает последствия за отсутствие идентификации, в контексте услуг по управлению идентификационными данными это требование выполняется, **если в соответствии со статьей 10(1)** с этой целью для электронной идентификации лица используется какой-либо метод.

### *Статья 16. Электронные подписи*

В тех случаях, когда законодательство требует наличия подписи какого-либо лица или предусматривает последствия в случае отсутствия подписи, это требование выполняется в отношении сообщения данных, если **в соответствии со статьей 22(1)** используется какой-либо метод: [...]

### *Статья 17. Электронные печати*

В тех случаях, когда законодательство требует от юридического лица представления печати или предусматривает последствия в случае отсутствия печати, это требование выполняется в отношении сообщения данных, **если в соответствии со статьей 22(1)** используется какой-либо метод: [...]

### *Статья 18. Электронные отметки времени*

В тех случаях, когда законодательство требует, чтобы те или иные документы, записи, информация или данные были связаны со временем и датой, или предусматривает последствия в случае отсутствия отметки времени и даты, это требование выполняется в отношении электронного сообщения, **если в соответствии со статьей 22(1)** используется какой-либо метод: [...]

---

*Статья 19. Электронное архивирование*

В тех случаях, когда законодательство требует, чтобы те или иные документы, записи или информация были сохранены, или предусматривает последствия в случае, если они не были сохранены, это требование выполняется в отношении сообщения данных, **если в соответствии со статьей 22(1)** используется какой-либо метод:

*Статья 20. Услуги электронной регистрации доставки*

В тех случаях, когда законодательство требует доставки документа, записи или информации с помощью заказного почтового отправления или аналогичной услуги или предусматривает последствия в случае недоставки, это требование выполняется в отношении сообщения данных, **если в соответствии со статьей 22(1)** используется какой-либо метод: [...]

*Статья 21. Аутентификация веб-сайтов*

В тех случаях, когда законодательство требует аутентификации веб-сайта или предусматривает последствия в отсутствие аутентификации веб-сайта, это требование выполняется, **если в соответствии со статьей 22(1)** используется какой-либо метод: [...]

---